

PENETRATION TESTING ON A LIVE WEBSITE AND RESEARCH INTO CYBER SECURITY INCIDENT AND DEFENSIVE TECHNIQUE CASE STUDY

SECURITY ANALYSIS, TECHNIQUES, AND PROCEDURES – Coursework

Aneena Elizabeth Saju (2105165)

Computer Network and Cyber Security, MSc

August 1, 2022

TABLE OF CONTENT

CONTENTS

INTRODUCTION	3
Network Details.....	4
Scope of Test.....	5
TABLE OF FIGURES AND TABLES	6
1. CONTINGENCY POLICY	7
2. PENETRATION TESTING FRAMEWORK AND TOOLS.....	8
3. ATTACKS AND TESTS.....	9
3.1 Information Gathering Using Whois.....	9
3.2 Nmap scan of Website.....	10
3.3 Spidering and Mapping site using Burp Suite.....	11
3.4 Probing Hidden Files With ZAP	13
3.5 Active Scanning Using ZAP	15
3.6 ZAP scanning and Vulnerability analysis	16
3.7 Web application Firewall Detection with WAFW00F	18
3.8 Cookies Collection	19
3.9 Security Scan Using Nikto	20
4. SOLUTIONS FOR THREATS DISCOVERED	21
4.1 SQL injection Remedies and protection.....	21
4.2 XSS Remedies and protection.....	21
5. FORENSIC METHODOLOGY	22
6. FORENSIC REPORT	25
CONCLUSION.....	27
REFERENCES	28

INTRODUCTION

A systematic process known as penetration testing, or PEN testing, is used to test an organization's computing infrastructure, which includes people, software, and hardware. To detect the weakness, this procedure involves analyzing the complete organization's computing system in search of vulnerabilities including system setup, software and hardware faults, and its operating process. [1]

A penetration test is used to pinpoint the dangers that could arise if an attacker gained access to the organization's networks and computing systems. The mitigation plan to close security flaws before the actual attack will be estimated with the aid of a PEN test. An organization's ability to mitigate financial and information loss that might have resulted from security breaches and damaged consumer trust is helped by conducting PEN tests. [1] Minimizing financial loss and ensuring compliance with industry regulations, consumers, and shareholders, protects organizations from failure and helps build trust, a positive corporate image, and justifies IT security investments. Due to the proactive nature of penetration testing, it gives unquestionable data that enables the firm to comply with auditing and compliance requirements. [2] Many infrastructures are there that are being used for the base assessment of the penetration testing like OWASP.

The non-profit organization OWASP is dedicated to enhancing software security [3]. The OWASP Security Knowledge Framework, in many programming languages, is an open-source web application that outlines secure coding concepts. OWASP-mission SKF's is to assist you in learning security by design, incorporating it into your software development, and creating secure by design applications. This is accomplished by OWASP-SKF through manageable software development projects that include checklists and labs for security verification training. [4]

These frameworks are the collective ideas and the methodologies of many of the most advanced hackers in the world that are up to date with the tools and techniques used by the hacker to manipulate and penetrate the system. These frameworks also provide various guidelines and the way of using them as suggested by experienced and advanced hackers to better utilize the framework for the betterment of a website and pointing out the vulnerabilities.

To hack own business or systems, an ethical hacker must be hired. An ethical hacker, sometimes known as a white-hat hacker, evaluates computer security by searching for weaknesses and vulnerabilities in the targets' defenses using the same skills and equipment as a malevolent hacker, but legally and ethically. [5]

Without doing a penetration test, a business may have an undetermined number of entry points that might be exploited by any hacker to enter the network and transmit critical data. The internal and external testing methodologies are the two perspectives from which a penetration test might be approved. An external test is also referred to as a "black box" test because neither the tester nor the exploit has access to the systems being tested. A variety of bored attackers are always scanning the internet for vulnerabilities, and hackers are continually eager to identify those problems and exploit them. Therefore, it is more likely that an external vulnerability will be exploited and disclosed to several hackers. As a result, a website must undergo an external black box test. An account of a current user of the firm or other leaked information that a hacker uses as a weakness can help some lead on the organization's data while it is being attacked internally.

Although many measures are taken throughout every test to ensure test performance, the sustainability of business operations, and the stability of the technical environment, penetration tests can nevertheless have an impact on how well a website performs. The IT industries employ several contingency plans as a result to lessen the risk and potential effects of the penetration test. This assignment involves doing black box testing on the Helios Pharma Wire website using a variety of third-party apps on the Linux distribution Kali Linux lookups, and burp suite. The test's objective is to identify any outside vulnerabilities that can be accessed via any IP address on a global network. Later in the assignment, it is pointed out what risks might arise, how serious they might be, and how much it might cost to fix the system's weaknesses.

The following pen test was carried out on 01 August 2022.

The testing team includes a single individual pen tester.

Network Details

Operating system details: A Linux-based operating system Kali Linux, is used.

Major Software Applications:

- i. Burp Suite
- ii. Nmap

System Configuration:

The Linux operating system is installed inside a virtual box.

The specifications of the virtual machine are:

RAM: 3077 Mb

Storage: 39.77 Gb

CPU cores: 4

Interconnectivity:

A mobile Wi-Fi device is used to connect to the wide area network (WAN) and the internet.

Scope of Test

Constraints and Imposed Limitations:

- i. Because the website is live, no denial-of-service attack is conducted on it.
- ii. No data on the website is altered.
- iii. Finding new vulnerabilities is not done by using existing ones as a platform.
- iv. No attempt is made to tamper with the website's service.
- v. The malicious software is not sent, stored, or uploaded over the website using any scripting.

Purpose and Type of test:

To examine and identify the site's vulnerabilities, a black box penetration test is performed.

TABLE OF FIGURES AND TABLES

Table 1: Table showing ports shown in Nmap	11
Table 2: Amount of alertness for each level of risk and confidence	17
Table 3: Number of alerts of each type with its risk level	18
Figure 1: Domain information shown in Whois	9
Figure 2: Raw Whois Data.....	10
Figure 3: Nmap result	11
Figure 4: Sitemap of the main directory on domain helios-pharma.com	12
Figure 5: Details about the asset folder shown in the sitemap.....	13
Figure 6: Detailed view of the main directory	13
Figure 7: Sitemap showing the hidden files in detail.....	14
Figure 8: Sitemap showing the main hidden files in the directory	15
Figure 9: Automatic scan main page	15
Figure 10: Automated scan results.....	16
Figure 11: WAFW00F results for domain helios-pharma.com	19
Figure 12: Cookies found on the domain helio-pharma.com	19

1. CONTINGENCY POLICY

A contingency plan is a strategy created to assist an organization in effectively responding to a large crisis, event, or condition that may or may not occur in the future. Because it can be utilized as a fallback strategy if desired outcomes are not achieved, a contingency plan is also known as a "Plan B" or backup plan. [6]

To identify the structural flaws and potential vulnerabilities of the website:

- i. The contingency needs are linked to the important company functions and missions.
- ii. Along with the recovery target, many metrics are presented, with varying restoration priorities.
- iii. Focuses on the designated tasks and duties for contingency situations.
- iv. When concessions are made on the side yet inside the domain, the missions and functions are kept in order.
- v. Since the testing is a black box, no source code information has been provided, and all the data has been acquired via external networks and web browsers.
- vi. In no circumstances is the information on the website altered, and no dangerous scripts are loaded onto the side.
- vii. No attempt is made to manipulate client interactions on the website to harm the company's bottom line.
- viii. Only scanning is carried out through third-party software, though the website's service is clear.
- ix. Beyond the parameters of this assignment, no other secured inspections of the site are performed.
- x. The penetration tester leaves no trace of the company's sensitive data.

The tester shall be held accountable for any non-disciplinary actions taken in any situation, even if this policy is not broken, and will accept the appropriate civil and criminal sanctions. Denial-of-service attacks are not covered under the agreement and won't be carried out by the penetration tester.

2. PENETRATION TESTING FRAMEWORK AND TOOLS

Penetration testers must first become familiar with the computer systems they will be trying to hack. Then, to detect vulnerabilities, they often employ a collection of software tools. Threats from social engineering hacking may also be present during penetration testing. Testers will attempt to get access to a system by duping a staff member into granting access. The organization is in charge of making the necessary modifications to either fix or mitigate the vulnerabilities after receiving the results of penetration testing. [7]

Penetration testing in online applications makes sure no security patches are covering the website, identifies risk vulnerabilities, and provides workable solutions for their eradication. There are common misconceptions about online application penetration testing, however, every individual website requires a different type of methodology.

- i. Information gathering - In this first step, information on the website's architecture, the web integration service, and other information that a tester requires as a guide to the website are generated.
- ii. The required equipment is set up to conduct experiments.
- iii. The existence of firewalls and other active security mechanisms is examined on the website.
- iv. Platform testing and configuration.
- v. Handling errors and checking test results.
- vi. Verifying the encryption-related security.
- vii. Business and client-side logic testing and verification.
- viii. Report generation solutions and advice.
- ix. Reset the vulnerabilities and clean them up.

3. ATTACKS AND TESTS

3.1 Information Gathering Using Whois

The information gathered when someone registers a domain name or modifies their DNS settings is stored in a public database called Whois. [8]

With the help of the online tool whois, you may learn more about a website's domain name, IP address, and other details. You can also learn more about the query that was submitted to the whois web server. In actuality, the information gathered by whois is accessible to the public and may be obtained without attempting to compromise the servers' or website's security.

The results of the Whois search for the website Heliospharma.com are shown in the figures below. By using the following command in the command line interface of any Linux distribution environment, we can immediately access the whois information gathering program from its website.

`whois <domain_name_of_target>`

Domain Profile	
Registrant	Whois Agent
Registrant Org	Domain Protection Services, Inc.
Registrant Country	us
Registrar	Name.com, Inc. IANA ID: 625 URL: http://www.name.com Whois Server: whois.name.com abuse@name.com (p) 17203101849
Registrar Status	clientTransferProhibited
Dates	636 days old Created on 2020-11-03 Expires on 2022-11-03 Updated on 2021-10-31
Name Servers	NS-1076.AWSDNS-06.ORG (has 54,630 domains) NS-1812.AWSDNS-34.CO.UK (has 311 domains) NS-416.AWSDNS-52.COM (has 1,229 domains) NS-873.AWSDNS-45.NET (has 25 domains)
Tech Contact	Whois Agent Domain Protection Services, Inc. PO Box 1769, Denver, CO, 80201, us (p) 17208009072 (f) 17209758725
IP Address	13.126.252.213 is hosted on a dedicated server
IP Location	🇮🇳 - Maharashtra - Mumbai - Amazon Data Services India
ASN	🇮🇳 AS16509 AMAZON-02, US (registered May 04, 2000)
Domain Status	Registered And Active Website
IP History	5 changes on 5 unique IP addresses over 2 years
Registrar History	1 registrar
Hosting History	2 changes on 3 unique name servers over 2 years

Figure 1: Domain information shown in Whois

Whois Record (last updated on 2022-08-01)

```
Domain Name: HEALIOS-PHARMA.COM
Registry Domain ID: 2570004120_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.name.com
Registrar URL: http://www.name.com
Updated Date: 2021-10-31T18:56:41Z
Creation Date: 2020-11-03T16:31:47Z
Registrar Registration Expiration Date: 2022-11-03T16:31:47Z
Registrar: Name.com, Inc.
Registrar IANA ID: 625
Reseller:
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Whois Agent
Registrant Organization: Domain Protection Services, Inc.
Registrant Street: PO Box 1769
Registrant City: Denver
Registrant State/Province: CO
Registrant Postal Code: 80201
Registrant Country: US
Registrant Phone: +1.7208009072
Registrant Fax: +1.7209758725
Registrant Email: https://www.name.com/contact-domain-whois/healios-pharma.com
Registry Admin ID: Not Available From Registry
Admin Name: Whois Agent
Admin Organization: Domain Protection Services, Inc.
Admin Street: PO Box 1769
Admin City: Denver
Admin State/Province: CO
Admin Postal Code: 80201
Admin Country: US
Admin Phone: +1.7208009072
Admin Fax: +1.7209758725
Admin Email: https://www.name.com/contact-domain-whois/healios-pharma.com
Registry Tech ID: Not Available From Registry
Tech Name: Whois Agent
Tech Organization: Domain Protection Services, Inc.
Tech Street: PO Box 1769
Tech City: Denver
Tech State/Province: CO
Tech Postal Code: 80201
Tech Country: US
Tech Phone: +1.7208009072
Tech Fax: +1.7209758725
Tech Email: https://www.name.com/contact-domain-whois/healios-pharma.com
Name Server: ns-1812.awsdns-34.co.uk
Name Server: ns-1076.awsdns-06.org
Name Server: ns-873.awsdns-45.net
Name Server: ns-416.awsdns-52.com
DNSSEC: unsigned
Registrar Abuse Contact Email: abuse@name.com
Registrar Abuse Contact Phone: +1.7203101849
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

For more information on Whois status codes, please visit https://icann.org/epp
```

Figure 2: Raw Whois Data

3.2 Nmap scan of Website

Nmap, which stands for Network Mapper, is a free and open-source application used for port scanning, vulnerability analysis, and, obviously, network mapping. The enormous developer and programmer community that contributes to Nmap's upkeep and updates has allowed it to maintain

its dominance. Its open source, flexible code base allows for customization to function in the majority of highly specialized or customized environments. [9]

We only need to visit the website 'map.online' to map a website' network using Nmap. Although in this project the Nmap scan is performed using Kali Linux's command line interface by just executing the command.

```
>>nmap-sS healios-pharma.com
```

Following are the result of the Nmap scan done on the website healios-pharma.com:

<u>Port</u>	<u>Protocol</u>	<u>State</u>	<u>Service</u>
21	TCP	Open	FTP
80	TCP	Open	HTTP
443	TCP	Open	HTTPS
554	TCP	Open	RTSP
1723	TCP	Open	PPTP

Table 1: Table showing ports shown in Nmap

```
(aneena@kali)-[~]
$ sudo nmap -sS healios-pharma.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 12:37 BST
Nmap scan report for healios-pharma.com (13.126.252.213)
Host is up (0.0073s latency).
rDNS record for 13.126.252.213: ec2-13-126-252-213.ap-south-1.compute.amazonaws.com
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp

Nmap done: 1 IP address (1 host up) scanned in 8.07 seconds
```

Figure 3: Nmap result

3.3 Spidering and Mapping site using Burp Suite

The technique of mechanically following every link on a web page to find both static and dynamic online resources of the web application is known as spidering, or web crawling. The mapping of an application is automated by Burp using the Spider tool. [10]

The goal of spidering is to determine the context and the area of the website that we want to search for its structure, web forms, and embedded links.

You can describe the pages, videos, and other resources on your site as well as the connections between them in a sitemap file. This file is examined by search engines like Google to improve the way they index your website. A sitemap not only gives useful information about these files but also lets Google know which pages and files you believe are crucial to your website. [11]

The sitemap for the domain heailospharma.com is shown in the picture below; it is made up of the main directory <http://heailospharma.com>, which contains the directories: assets, icons, and includes. The results show that the website has a straightforward tree structure. The website's CSS code, fonts needed to construct the website's exterior structure, images' illustrative images, and numerous graphical representations are all contained in the assets folder. The website's front-end javascript code is also included in the assets folder.

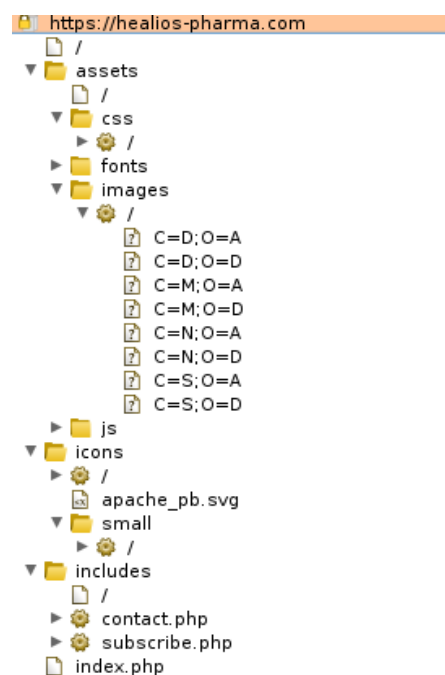


Figure 4: Sitemap of the main directory on domain helios-pharma.com

Name	Value
GET	/assets/css/?C=D;O=A HTTP/1.1
Host	healios-pharma.com
Accept-Encoding	gzip, deflate
Accept	*/*
Accept-Language	en
User-Agent	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection	close
Referer	https://healios-pharma.com/assets/css/
Cookie	PHPSESSID=435vm7sjk772h5oehgt0j1egrg

Figure 5: Details about the asset folder shown in the sitemap

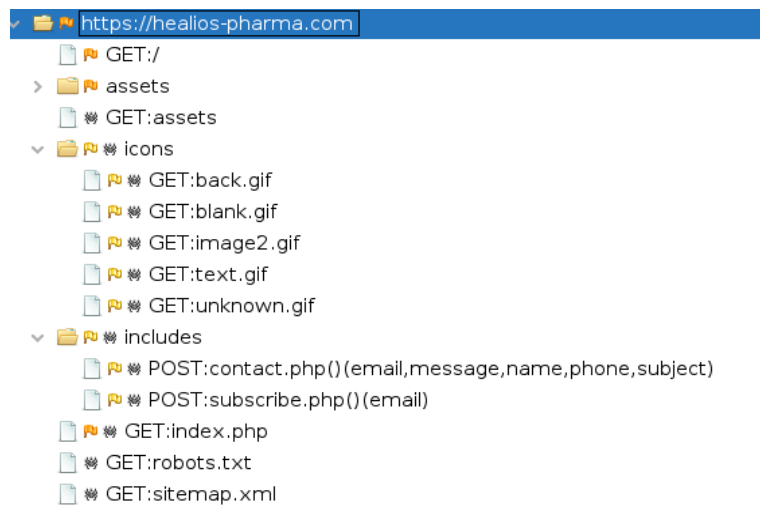


Figure 6: Detailed view of the main directory

3.4 Probing Hidden Files With ZAP

For testing online security, OWASP ZAP (Zed Attack Proxy) is an extremely flexible tool. It has a proxy, HTTP request sender, fuzzer, spider, passive and active vulnerability scanners, and some more intriguing features. [12]

It can be used on practically every operating system that supports Java because it is a Java tool. The packet communication between the website and the server can be intercepted by setting up a proxy using a web browser. In this instance, the website we are talking about is healiospharma.com, which is mapped on the ZAP interface's left side. By right clicking the website, we can choose the option to scan it for hidden files from the settings menu. Hidden files are either garbage files or files left behind by a website's developer that may or may not affect the website's vulnerability.

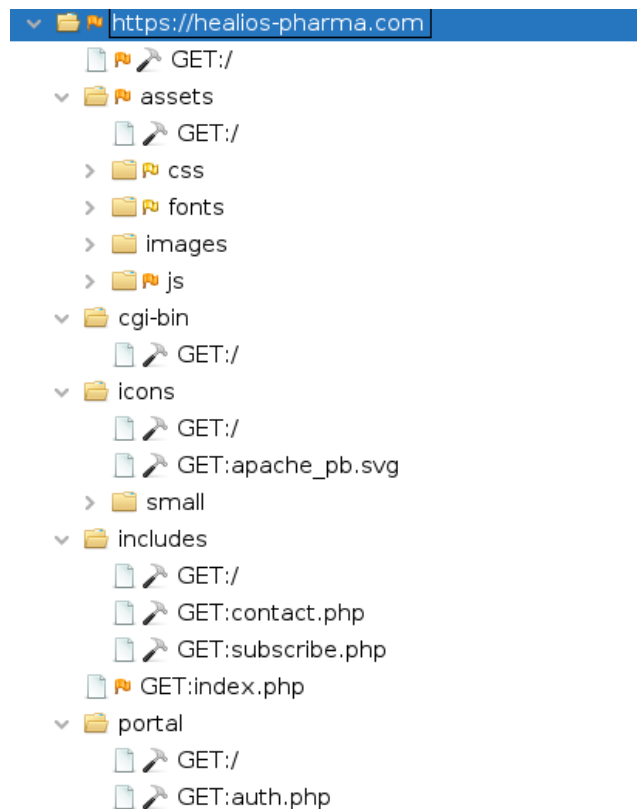


Figure 7: Sitemap showing the hidden files in detail

It searches for hidden files to put the network at more risk. This can occasionally overload the network and require some time for hidden file discovery, but it is worthwhile.

In the root folder of the main website, <http://healios-pharma.com>, two directories are located where the hidden files are scanned with zap. They are cgi-bin and portal, respectively. Even though the portal folder has two files, and the cgi-bin folder contains one file, these two folders are not part of the website's external structure and are concealed from the main structure. Following are the files and folders:

<http://healios-pharma.com>

assets

cgi-bin

> ***GET:/***

Icons

Includes

portals

> ***GET:/***

> ***GET:auth.php***

The names of hidden files and folders in the website's structure are in bold italics.

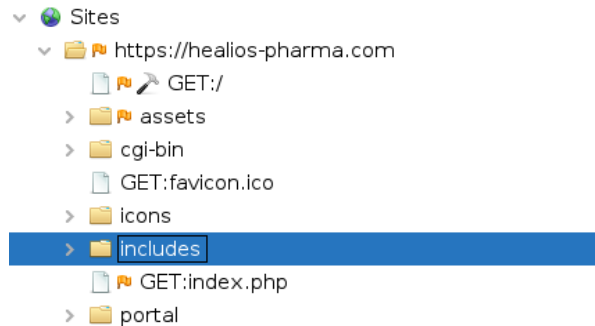


Figure 8: Sitemap showing the main hidden files in the directory

3.5 Active Scanning Using ZAP

The attempt to identify possible weaknesses by utilizing well-known attacks against the chosen targets is active scanning. Only if you have been given the authorization to test the application must you run an active scan. Active scanning can incorporate the method of fuzzing. Fuzzing involves submitting unexpected or faulty data to look for vulnerabilities. [13]

Any active or automatic vulnerability scanning will not discover logical flaws, such as faulty access control. To detect all types of vulnerabilities, manual penetration testing should always be done in addition to active scanning. [13]

The automatic scan is simple, we just must give the URL and the rest of the work is on the software. Besides, we can determine some of the tools it will use in the way like whether it must use the traditional spider or not.

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack:

Use traditional spider: ☒

Use ajax spider: ☐ with

Attack Stop

Progress: Attack complete - see the Alerts tab for details of any issues found

Figure 9: Automatic scan main page

Progress		Response Chart				
Host:		http://healios-pharma.com				
	Strength	Progress	Elapsed	Reqs	Alerts	Status
Analyser			00:00.219	1		
Plugin						
Path Traversal	Medium		00:00.279	0	0	✓
Remote File Inclusion	Medium		00:00.280	0	0	✓
Source Code Disclosure - /WEB-INF folder	Medium		00:00.558	6	0	✓
External Redirect	Medium		00:00.557	0	0	✓
Server Side Include	Medium		00:00.305	0	0	✓
Cross Site Scripting (Reflected)	Medium		00:00.293	0	0	✓
Cross Site Scripting (Persistent) - Prime	Medium		00:00.259	0	0	✓
Cross Site Scripting (Persistent) - Spider	Medium		00:00.248	3	0	✓
Cross Site Scripting (Persistent)	Medium		00:00.325	0	0	✓
SQL Injection	Medium		00:00.260	0	0	✓
Server Side Code Injection	Medium		00:00.259	0	0	✓
Remote OS Command Injection	Medium		00:00.277	0	0	✓
Directory Browsing	Medium		00:00.285	3	0	✓
Buffer Overflow	Medium		00:00.290	0	0	✓
Format String Error	Medium		00:00.259	0	0	✓
CRLF Injection	Medium		00:00.263	0	0	✓
Parameter Tampering	Medium		00:00.250	0	0	✓
ELMAH Information Leak	Medium		00:00.038	1	0	✓
.htaccess Information Leak	Medium		00:00.206	1	0	✓
Script Active Scan Rules	Medium		00:00.001	0	0	✗
Cross Site Scripting (DOM Based)	Medium		02:25.852	528	0	✓
SOAP Action Spoofing	Medium		00:00.003	0	0	✓
SOAP XML Injection	Medium		00:00.255	0	0	✓
Totals			02:31.874	543	0	

Figure 10: Automated scan results

3.6 ZAP scanning and Vulnerability analysis

Context of analysis: Since no contexts were chosen, the software included every context by default.

Sites: The following sites were included:

http://healios-pharma.com

https://healios-pharma.com

(If no sites were chosen, all sites were automatically added.)

For a site to have its data included in the report, it must also be located inside one of the mentioned contexts.

Risk levels:

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels:

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

By risk and confidence measures, alertness is valued:

The number of alerts for each level of risk and confidence in the report is shown in the table below. (The percentages in brackets, which are rounded to one decimal place, show the count as a proportion of the total number of alerts contained in the report.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	0 (0.0%)	78 (30.6%)	0 (0.0%)	78 (30.6%)
	Low	0 (0.0%)	0 (0.0%)	159 (62.4%)	0 (0.0%)	159 (62.4%)
	Informational	0 (0.0%)	0 (0.0%)	0 (0.0%)	18 (7.1%)	18 (7.1%)
	Total	0 (0.0%)	0 (0.0%)	237 (92.9%)	18 (7.1%)	255 (100%)

Table 2: Amount of alertness for each level of risk and confidence

Alert counts by alert type

The number of each alert type's alerts, as well as the danger level of each alert type, are displayed in this table. (The percentages in brackets show each count as a proportion of the total number of alerts included in this report, rounded to one decimal place.)

<u>Alert type</u>	<u>Risk</u>	<u>Count</u>
Application error disclosure	Medium	36 (14.1%)
Missing anti-clickjacking header	Medium	41 (16.1%)
Vulnerable JS library	Medium	1 (0.4%)
Absence of anti-CSRF tokens	Low	8 (3.1%)
Cookie without same site attribute	Low	3 (1.2%)

Incomplete or no cache-control header set	Low	37 (14.5%)
Server leaks information via "X-Powered-By" HTTP response header fields	Low	7 (2.7%)
X-content-type-options header missing	Low	104 (40.8%)
Information disclosure - suspicious comments	Informational	18 (7.1%)
Total		255

Table 3: Number of alerts of each type with its risk level

The website address <https://healios-pharma.com/> has been flagged as having a medium security vulnerability and is likely weak to script, cookie-setting, and commenting attacks. This also applies to the script and comment vulnerability of the URL <https://healios-pharma.com/index.php>

3.7 Web application Firewall Detection with WAFW00F

One of a web app's strongest protections is a web application firewall, although they can be vulnerable if an attacker is aware of the firewall version being utilized. A hacker may need to know the firewall a target is using to figure out how to get around it and what defenses the target has in place. The Wafw00f and Nmap programs also make it simple to fingerprint firewalls. Even while most web app firewalls, or WAFs, are rather effective at securing the services they shield, they occasionally get exposed when a vulnerability is found that may be exploited. It may be simple to decipher the rules of a firewall and find a way to circumvent them to gain entry if it hasn't been updated in a while. [14]

A well-known Python tool called WAFW00F eliminates the guesswork involved in identifying a website's firewall. A service that WAFW00F probes can reveal the underlying firewall that is being used. Nmap scripts can perform some of the same tasks, however, while testing WAFW00F consistently provided more thorough and precise findings. [14]

```

(aseena@kali)-[~]
$ wafw00f https://healios-pharma.com/

      ( Woof! )
    /      \
   /        \
  /          \
 /            \
/              \
(              )
(              )
(              )

~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://healios-pharma.com/
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7

```

Figure 11: WAFW00F results for domain helios-pharma.com

There is no firewall present for the website <https://healios-pharma.com>, according to WAFW00F. *No WAF was detected by the generic detection*
 This poses a serious risk to the website because it leaves it open to a variety of attacks.

3.8 Cookies Collection

Cookies are designed expressly to track, personalize, and save data about each user's session in Internet web browsers. Simply said, a "session" is the amount of time you spend on a website. To recognize you when you visit a new website, cookies are created. Your web browser receives a brief trickle of identification data from the web server, which houses the website's data. [15]

HEALIOS

HOMEABOUT USOUR RESEARCHOUR LEADERSCONTACT US

InspectorConsoleDebuggerNetworkStyle EditorPerformanceMemoryStorageAccessibilityWhat's NewCookie Editor

Cache Storage

Indexed DB

Local Storage

Session Storage

Filter Items

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSESSID	amqr2o8a9uivk1fhlbgp61gmn	healios-pharma...	/	Session	35	true	true	None	Sun, 16 Jan 2022 10:11:34

Filter values

PHPSESSID: "amqr2o8a9uivk1fhlbgp61gmn"

Created: "Sun, 16 Jan 2022 10:10:01 GMT"

Domain: "healios-pharma.com"

Expires / Max-Age: "Session"

HostOnly: true

HttpOnly: true

Last Accessed: "Sun, 16 Jan 2022 10:11:34 GMT"

Path: "/"

SameSite: "None"

Secure: true

Size: 35

Figure 12: Cookies found on the domain helio-pharma.com

Cookies on the website <https://healios-pharma.com/> are handled carefully, and cookie protection is enabled. Even though this is a very archaic technique, it is not used here to deceive website users into giving up their private information.

3.9 Security Scan Using Nikto

Nikto is a web application scanner and an open-source web server. Nikto can run extensive tests on web servers to check for a variety of security risks, including more than 6700 potentially harmful files and programs. Additionally, Nikto may check for version-specific issues and outdated web server software. [16]

It is open source, therefore anyone can use it to check any web servers for vulnerabilities (Nginx, IHS, Litespeed, OHS, Apache, etc.).

The findings of a Nikto scan to identify suspected vulnerabilities and potential threats are shown below.

- i. The X-Frame-Options header for anti-clickjacking is missing.
- ii. The header for X-XSS-Protection is not defined. The user agent may receive a hint from this header to help prevent some XSS attacks.
- iii. The Strict-Transport-Security HTTP header is not defined, and the website uses SSL.
- iv. SSL is being used by the website, and the Expect-CT header is missing.
- v. There is no X-Content-Type-Options header. This might enable the user agent to render the website's content differently depending on the MIME type.
- vi. It appears that OpenSSL/1.0.2k-fips is out-of-date (current is at least 1.1.1). Both OpenSSL 0.9.8zc and 1.0.0o are current.
- vii. The web server sends back a legitimate answer using shoddy HTTP methods, which may result in false positives.
- viii. OSVDB-877: The presence of the HTTP TRACE method indicates that the host may be XST vulnerable.

4. SOLUTIONS FOR THREATS DISCOVERED

4.1 SQL injection Remedies and protection

An injection attack known as SQL Injection enables the execution of malicious SQL commands. These commands manage a database server that sits in front of a web application. SQL Injection flaws allow attackers to get around application security safeguards. The full content of a SQL database can be retrieved by getting past authentication and authorization of a web page or online application. They can also add, alter, and delete records in the database using SQL Injection. [17] To prevent SQL injection, proper client-side input validation and character filtering are required; alternative statements can be generated and parameterized to be placed as text in the website's input parameters.

Sample code to validate the input of the user:

```
input = request.getParameter ("seqno");  
String charPattern = "[0-9a-zA-Z]";  
If (! input. matches (charPattern))  
{  
out.println ("Invalid Input");  
}
```

4.2 XSS Remedies and protection

There should be either the server side and the client side verification for the code and any introduction of hazardous characters like special symbols and carriage return, feedline & ; \$ % @ ' " \ ' " < > () + linefeed ,(comma sign) \] . (dot) and / must be avoided.

Sample code to validation encoding technique:

```
<input type="txt" mxlength="30" name="ecsChangePwdForm" size="40" readonly="true"  
value='<%=ESAPI.encoder().encodeForHTML(request.getParameter("userName"))%>'>
```

5. FORENSIC METHODOLOGY

The forensic methodology is used to investigate and restore deleted files.

Data forensics is based on the observation that when we delete pre-existing data, only the pointer record of the data changes from pointing to the memory location to pointing to the recycle bin, and that when we empty the recycle bin or use shift+delete, only the pointer record of the data is deleted. Until it is replaced by new data, the previous data is not lost. The data on this storage device can be easily restored if it is handled professionally.

Following are the actions are taken in the security analysis techniques and processes module to look into and recover the deleted files:

Collection of evidence

All the devices seized should be placed in an anti-static bag and sent to the forensics laboratory, so that the following steps can be performed.

Procedure development

Digital evidence can be very sensitive and delicate. If handled and protected improperly, this evidence can be easily corrupted. Therefore, it is essential to adhere to strict policies and procedures for activities related to computer forensic investigation. These include detailed instructions about how to correctly set up a system for evidence retrieval and how to document these activities to support and ensure the authenticity of data and to recover potentially useful digital evidence.

The adjustment of a set of explicitly stated actions about what constitutes evidence, where to look for evidence, and how to manage it once it has been retrieved is a crucial component of the security analysis techniques and procedure module. The right steps must be done to ascertain the specifics of the case at hand and secure the necessary approval before purchasing the case before doing any investigation.

Evidence assessment

An important step in the investigative process in cybercrime is the evaluation of potential evidence. The type of evidence sought (including specific platforms and data formats) and a clear knowledge of how to preserve relevant data must be established by the investigator before beginning any investigation. The computer forensic investigator uses cutting-edge techniques to

sift through hard drives, email, social networking sites, and other digital archives to gather and retrieve any data that might be useful as a crime's evidence.

Evidence acquisition

A thorough and well-thought-out plan for gathering evidence may be the most important factor in a successful forensic inquiry. There must be thorough documentation after, during, and before the acquisition process. To retrieve sensitive data and ensure functionality, storage devices must be physically removed as part of the preservation procedure. The entire system must also be copied and transferred properly.

Before gathering any evidence, we should always follow the order of volatility, which means gathering the most volatile evidence first and the least volatile evidence last. Critical data is kept in the RAM (random access memory) of an operating computer, and if the computer is shut off, data may be lost. Before turning off the computer, it's crucial to gather the RAM's contents, which should be collected in order of volatility. Once the RAM material has been gathered, you can move on to gather any hard disc, external device, CD, and other hard copy evidence. A case number and identification should be written on every piece of evidence so that you can recognize certain devices.

Evidence examination

For retrieving, copying, and saving evidence in the proper database, a proper method must be followed. Information and data from the chosen archives are analyzed and examined using a range of techniques and strategies. Large data archives may be searched for certain file kinds or keywords using analytical tools, and recently deleted files can also be retrieved. The files and programs that have been purposefully hidden or encrypted can be especially useful in investigations.

The file name can be used to find specific information, such as the location and time that particular files were produced, uploaded, or downloaded. If a file is located on another server or system, it can be tracked through that server's or system's file name because file names lead to the address of files. To analyze the disc image and discover and retrieve any concealed or erased data, a variety of cyber forensic techniques are now being deployed. These technologies may also be used

to examine images and videos, and all the information, including the camera used and the time it was taken, is discovered. The investigators collaborate closely with various law enforcement agencies during this phase to comprehend the case and gather all required evidence.

Documenting and reporting

The specifications of the hardware and software used, the techniques used to test the system's functionality, the processes are taken to retrieve the storage devices, create copies of the data, and the actions necessary to review and access the duplicated data all need to be adequately documented. This guarantees that the inquiry has been conducted according to the law and following the correct process. These records might be utilized to double-check the investigator, therefore every detail provided in the report needs to be accurate and pertinent.

6. FORENSIC REPORT

Overview/case summary

To treat Covid-19, Nera Star, an employee of Healios Pharmaceutical Company (HPC), was developing a human vaccination. She had spent the last six years researching sensitive mathematical codes and chemical formulas, which were contained in her study files. She fought with the management over their decision to ignore her and elevate Napel to the position of Senior Scientist. She destroyed all the important study records in a fit of wrath, making them inaccessible to anybody.

Objective

This report offers an overview of the procedures and techniques utilized to investigate and recover deleted files that contained mathematical and chemical equations. The company stood to lose USD 3 million in various contracts with the suppliers if the data wasn't recovered.

Evidence analyzed

I checked the information on the PC Nera was used by the directive. A forensic copy of the computer's hard drive was created using methods and techniques used in digital forensics that are widely accepted and replicated bit for bit. The whole contents of the hard disc, including the user-accessible data, deleted files, and unallocated space, which may hold deleted content, were copied using the digital forensic copying procedure. There was no use in examining the computer's RAM because it had been a week since she had used it.

Investigation steps

Using the program known as FTK imager, a bit-for-bit forensic duplicate of the hard disc was created. The FTK imager analyses the hard drive sector by sector and finds any hidden files and documents. The bit stream images were hashed using the MD5 algorithm. To prevent evidence loss, forensic investigations now employ the hard disc image rather than the actual disc, while the actual hard disc is safely stowed away. The data that is most pertinent to the investigation was extracted from the hard drive using Autopsy or the Sleuth Kit.

To find the data that was not backed up by the enterprise central backup machine while it was being built, we first created a timeline of all the files using the MACtime program uses the search for a particular file or set of data, and it is then used to list all the meta-data entries about the

material on the hard drive where the autopsy is being done. The metadata obtained was searched by using find tools for specific metadata entries. Our search area was significantly reduced in this way.

Now, using a hexadecimal editor to search for any relevant data stored in the targeted files, keywords, and other searches were conducted on them. The entire hard drive was run via undeleted utilities to check for any remaining deleted files. The entire hard drive was examined for any remnants of deleted data while being shown as a hexadecimal image. The remaining data is then recovered utilizing scavenging tools. The Covid-19 treatment vaccine's important information was manually checked in several non-searchable media categories, such as movies and images without text. HPC received all the data that can be salvaged (Healios Pharmaceutical Company).

CONCLUSION

A black box penetration test is performed on the website <https://healios-pharma.com> using several tools, including Whois, Nmap, Burp Suite, Zed attack proxy (ZAP), WAFW00F, and Nikto. All these penetration testing tools are based on Linux because Kali Linux was used to conduct the entire penetration test.

The website's overall security is not particularly good, making it open to several attacks. The lack of a firewall is the primary example. Any commercial website must always include a firewall. My suggestions state that Cloudflare firewall protection should be installed on this website. Any company website can use Cloudflare's base plan, which starts at \$200/month, and larger businesses can choose custom plans. The website's flaws and vulnerabilities may require numerous weeks of regular penetration testing and code rectification. It may cost up to \$10,000 for the vulnerabilities and code fixing in a penetration test for website security.

Any obsolete component in the server configuration must be changed right away for the server to operate at peak performance levels constantly.

REFERENCES

- [1] B. D. B. Hessa Mohammed Zaher Al Shebli, "A Study on Penetration Testing Process and Tools".
- [2] X. Y. B.-T. B. C. M. J. A. G. Bacudio, ".An overview of penetration Testing," *International Journal of Network Security & its application (IJNSA)*, vol. 3, no. 6, 2011.
- [3] B. K. K. & S. S. Ghazali, "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating,," *Information Technology Journal*, vol. 4, no. 4, p. 264, 2019.
- [4] R. t. C. Glenn ten Cate, "OWASP," [Online]. Available: <https://owasp.org/www-project-security-knowledge-framework/#:~:text=The%20OWASP%20Security%20Knowledge%20Framework,that%20are%20secure%20by%20design..> [Accessed 2022].
- [5] W. Dawson, "Why Do You Need To Hack Your Company?," 26 September 2019. [Online]. Available: <https://codersera.com/blog/why-do-you-need-to-hack-your-company/>. [Accessed 2022].
- [6] P. Kirvan, "Tech Target," 2022 May 2022. [Online]. Available: <https://www.techtarget.com/whatis/definition/contingency-plan>.
- [7] G. Jevtic, "phenonixNAP," 9 May 2019. [Online]. Available: <https://phoenixnap.com/blog/best-penetration-testing-tools>. [Accessed 2022].
- [8] N. Brownell, "Domain.com Blog," [Online]. Available: <https://www.domain.com/blog/what-is-whois-and-how-is-it-used/>. [Accessed 2022].
- [9] J. B. II, "NetworkWorld," 20 May 2022. [Online]. Available: <https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html>. [Accessed 2022].
- [10] A. Mahajan, Burp Suite Essentials, Packt, 2014.
- [11] G. LLC, "Google Search Central," [Online]. Available: <https://developers.google.com/search/docs/advanced/sitemaps/overview#:~:text=A%20sitemap%20is%20a%20file,crawl%20your%20site%20more%20efficiently..> [Accessed 2022].

- [12] G. Najera-Gutierrez, Kali Linux Web Penetration Testing Cookbook, Packt, 2016.
- [13] "Devopedia," 22 July 2020. [Online]. Available: <https://devopedia.org/owasp-zap#qst-ans-6>. [Accessed 2022].
- [14] Kody, "Wonder How to," 19 November 2019. [Online]. Available: <https://null-byte.wonderhowto.com/how-to/identify-web-application-firewalls-with-wafw00f-nmap-0198145/>. [Accessed 2022].
- [15] "Kasperasky," [Online]. Available: <https://www.kaspersky.com/resource-center/definitions/cookies>. [Accessed 2022].
- [16] M. Shivanandhan, "FreeCodeCamp," 14 July 2021. [Online]. Available: <https://www.freecodecamp.org/news/an-introduction-to-web-server-scanning-with-nikto/>. [Accessed 2022].
- [17] "Acunetix," [Online]. Available: <https://www.acunetix.com/websitesecurity/sql-injection/>. [Accessed 2022].
- [18] L. R. JohnsonIII, "Science Direct," 2014. [Online]. Available: <https://www.sciencedirect.com/topics/computer-science/forensics-tool>.
- [19] L. E. D. Larry E. Daniel, "Science Direct," 2012. [Online]. Available: <https://www.sciencedirect.com/topics/computer-science/forensic-process>.
- [20] "Norwich University Online," 11 September 2017. [Online]. Available: <https://online.norwich.edu/academic-programs/resources/5-steps-for-conducting-computer-forensics-investigations>.
- [21] None, "Rec Faces," 18 January 2021. [Online]. Available: <https://recfaces.com/articles/digital-forensics>.
- [22] V. M. Antunes N, "Detecting SQL injection vulnerabilities in web services," in *The Fourth Latin-American Symposium Dependable Computing.*, 2009.
- [23] L. S. M. L. H. K. J. K. S. C. N. G. P. J. G. Kwon O, "An automation of penetration testing for remote buffer vulnerabilities," *The proceedings of the International Conference on Information Networking* , vol. LNCS 3391, pp. 652-661, 2005.
- [24] d. A. B. T. M. E. Moraes R, "Mapping web-based applications failures to faults," in *In Proceedings of the First Latin-American Symposium on Dependable Computing.*, 2009.
- [25] O. J, "IBM," 2011. [Online]. Available: <http://www.ibm.com/developerWorks>.

- [26] A. K. Ravneet Kaur, "Digital Forensics," *International Journal of Computer Applications*, vol. 50, no. 5, pp. 5-9, 2012.
- [27] K. Orrey, "Vulnerability Assessment," [Online]. Available: <http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html>.
- [28] R. D. S. Vijay, "Software testing help," 3 January 2022. [Online]. Available: <https://www.softwaretestinghelp.com/penetration-testing-tools/>.