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

January 17, 2022

TABLE OF CONTENT

Contents

INTRODUCTION 1
Network Details 2
Scope of Test 4
TABLE OF FIGURES AND TABLES 5
1. Contingency Policy 6
2. Penetration Testing Framework and Tools 7
3. Attacks and Tests 8
3.1 Information Gathering Using Whois 8
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 19
3.8 Cookies Collection 20
3.9 Security Scan Using Nikto 20
4. Solutions for Threat Discovered 22
4.1 SQL injection Remedies and protection 22
4.2 XSS Remedies and protection 22
5. Forensic methodology 23
6. Forensic Report 26
CONCLUSION 28
References 29

INTRODUCTION

Penetration testing is the science of simulated authorized cyberattacks on a website or a company's technology by a penetration tester to test the security of the website. Penetration testing falls under the category of ethical hacking and security testing, or we can say that penetration testing, security auditing, security testing, ethical hacking are the same branches of the studies performed by a white hat hacker. The main objective of penetration testing is to present the profile of a company on the website from the eyes of a hacker but not with the deeds of a hacker definition tester points out every possible vulnerability that can be exploited by a hacker and once the company about it. During the penetration testing, a certified ethical hacker tries to exploit the vulnerabilities present in the system or the website of a company and shows the company what might have happened if the real hacker tried to manipulate or bridge the system of the company and warns them about the result and outcomes for their breaches. Many infrastructures are there that are being used for the base assessment of the penetration testing like OWASP.

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 the experienced and advanced hackers in order to better utilize the framework for the betterment of a website and pointing out the vulnerabilities. Now the biggest question that arises is why would a company hire an ethical hacker to crack into a system and exploit its vulnerability? In fact, this has a simple answer that the biggest objective of the ethical hacker is to uncover, identify and fix the vulnerabilities present in a website so that it would be unexploitable or unreachable and hard to penetrate by a real hacker if the time comes to that.

Without performing a pentest, a company can be left with an unknown number of entry points that can be used by any hacker to infiltrate the organization and submit their specific information and sensitive contents. There are two different perspectives from which a pentest can be approved and those are internal and external testing approaches. In an external test, a tester or an exploit does not have any inside information to the targeted systems, this is also known as the black box for anonymous tests. The internet is constantly being scanned through various bored attackers to find out the vulnerabilities and hackers are consistently keen to exploit those bugs and take advantage of them. So, an external vulnerability is more likely to be exploited and exposed to various numbers of hackers. Thus, an external black box test is necessary to conduct for a website. While in the internal attack, it can help some lead on the company’s data, it may be an account of

the company's current user or some leaked information that is utilized as a vulnerability by a hacker.

Presentation tests can also have an impact on the performance of a website but there are various steps that are being taken during the course of any test performance and the sustainability of the business operations and stability of the technical environment. For this reason, various contingency policies are used by the IT sectors to mitigate the risk and the potential impact of the penetration test.

In this assignment, black box testing is performed on the website Helios Pharma wire using various third-party applications on the Linux distribution environment Kali Linux searches, burp suite. The aim of the test is to analyze any external vulnerabilities that can be accessed via any worldwide network IP. Later in the assignment, the potential threats and the level of threats are pointed out along with the ways and the estimated cost of removing the vulnerabilities from the system.

The following pen test was carried out on 15 January 2022.

The testing team includes a single individual pen tester.

Network Details

Operating system details: Tester has used a Linux based operating system Kali Linux.

Major Software Applications:

i. Burp Suite
ii. Nmap

System Configuration:

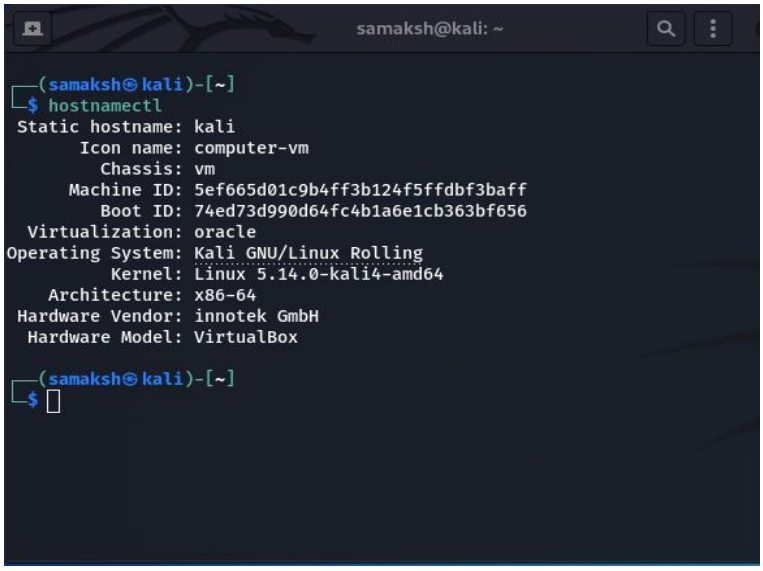
The Linux operating system is installed inside a virtual box.

The specifications of the virtual machine are:

RAM: 3077 Mb

Storage: 39.77 Gb

CPU cores: 4

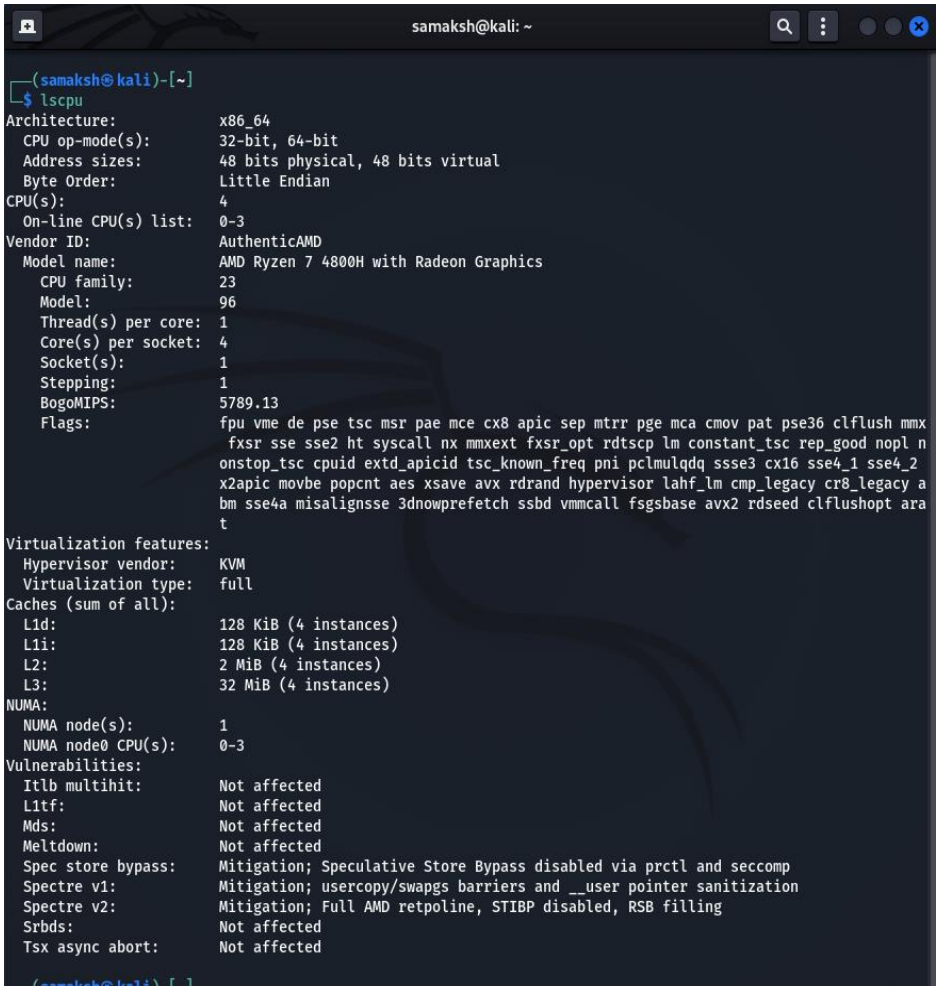


```
samaksh@kali: ~

┌──(samaksh㉿kali)-[~]
└─$ hostnamectl
 Static hostname: kali
       Icon name: computer-vm
         Chassis: vm
      Machine ID: 5ef665d01c9b4ff3b124f5ffdbf3baff
         Boot ID: 74ed73d990d64fc4b1a6e1cb363bf656
  Virtualization: oracle
Operating System: Kali GNU/Linux Rolling
          Kernel: Linux 5.14.0-kali4-amd64
    Architecture: x86-64
 Hardware Vendor: innotek GmbH
  Hardware Model: VirtualBox

┌──(samaksh㉿kali)-[~]
└─$
```

Figure 1: OS details



```
samaksh@kali: ~

┌──(samaksh㉿kali)-[~]
└─$ lscpu
Architecture:            x86_64
  CPU op-mode(s):        32-bit, 64-bit
  Address sizes:         48 bits physical, 48 bits virtual
  Byte Order:            Little Endian
CPU(s):                  4
  On-line CPU(s) list:   0-3
Vendor ID:               AuthenticAMD
  Model name:            AMD Ryzen 7 4800H with Radeon Graphics
    CPU family:          23
    Model:               96
    Thread(s) per core:  1
    Core(s) per socket:  4
    Socket(s):           1
    Stepping:            1
    BogoMIPS:            5789.13
    Flags:               fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx
                          fxsr sse sse2 ht syscall nx mmxext fxsr_opt rdtscp lm constant_tsc rep_good nopl n
                         onstop_tsc cpuid extd_apicid tsc_known_freq pni pclmulqdq ssse3 cx16 sse4_1 sse4_2
                         x2apic movbe popcnt aes xsave avx rdrand hypervisor lahf_lm cmp_legacy cr8_legacy a
                         bm sse4a misalignsse 3dnowprefetch ssbd vmmcall fsgsbase avx2 rdseed clflushopt ara
                         t
Virtualization features:
  Hypervisor vendor:     KVM
  Virtualization type:   full
Caches (sum of all):
  L1d:                   128 KiB (4 instances)
  L1i:                   128 KiB (4 instances)
  L2:                    2 MiB (4 instances)
  L3:                    32 MiB (4 instances)
NUMA:
  NUMA node(s):          1
  NUMA node0 CPU(s):     0-3
Vulnerabilities:
  Itlb multihit:         Not affected
  L1tf:                  Not affected
  Mds:                   Not affected
  Meltdown:              Not affected
  Spec store bypass:     Mitigation; Speculative Store Bypass disabled via prctl and seccomp
  Spectre v1:            Mitigation; usercopy/swapgs barriers and __user pointer sanitization
  Spectre v2:            Mitigation; Full AMD retpoline, STIBP disabled, RSB filling
  Srbds:                 Not affected
  Tsx async abort:       Not affected
```

Figure 2: CPU details

Interconnectivity:

Connection to the world wide web is achieved by a Wide Area Network (WAN) weather means of Wi-Fi 6 in the device and a router on the Wide Area Network (WAN).

Scope of Test

Constraints and Imposed Limitations:

i. A denial-of-service attack is not performed on the website as it is a live website.
ii. Any data website is not modified.
iii. Vulnerabilities are not used as a pivot to discover further vulnerabilities.
iv. There is no effort made in tampering with the service of the website.
v. No scripting is done to send, store and upload the malicious software via the website.

Purpose and Type of test:

A black box penetration test is conducted in order to analyze and point out the vulnerabilities in the site.

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 18

Table 3: Number of alerts of each type with its risk level 18

Figure 1: OS details 3

Figure 2: CPU details 3

Figure 3: Domain information shown in Whois 8

Figure 4: Administrative details shown in Whois 9

Figure 5: Raw Whois Data 9

Figure 6: Technical details shown in Whois 10

Figure 7: Registrant details shown in Whois 10

Figure 8: Nmap result 11

Figure 9: Sitemap of the main directory on domain helios-pharma.com 12

Figure 10: Details about the asset folder shown in sitemap 12

Figure 11: Detailed view of the main directory 13

Figure 12: Sitemap showing the hidden files in detail 14

Figure 13: Sitemap showing the main hidden files in the directory 15

Figure 14: Automatic scan main page 16

Figure 15: Automated scan results 16

Figure 16: WAFW00F results for domain helios-pharma.com 19

Figure 17: Cookies found on the domain helio-pharma.com 20

1. Contingency Policy

This policy is only applicable in the context of this assignment in which the black box penetration testing is being performed on the website. In order to determine the possible vulnerabilities and the weaknesses of the website structure:

i. Essential business functions and missions are identified and associated with the contingency requirements.
ii. Different metrics with the variable restoration priorities are provided along with the recovery objective.
iii. Addresses the contingency roles and the responsibilities that are assigned.
iv. The missions and the functions are orderly maintained in the case of compromises made at the side but within the domain.
v. Since the testing is black box, no information on the source code has been provided and the entire information is gathered from the outer networks and the web browsers.
vi. The information on the site is not altered in any cases nor any malicious scripts are loaded onto the side.
vii. No attack on the website is carried out to manipulate the company's customer interaction to cause them a business loss.
viii. The service of the website is understood, only scanning is done through third-party applications.
ix. No other secured inspections on the site are carried out beyond the scope of this assignment.
x. Company’s any vital data is untouched by the penetration tester.

This policy is not violated, in any case, the tester will hold responsible for any non-disciplinary actions taken in any circumstances and will accept the proper civil and criminal penalties. In the agreement, the denial-of-service attack is not included and will not be conducted by the penetration tester.

2. Penetration Testing Framework and Tools

In a web application, penetration testing ensures that there are no security patches over the website and identify the risk vulnerabilities and finds viable ways for their elimination. Every specific website demands a different type of methodology for penetration testing but, there is general mythology for web application penetration testing

i. Gathering information - information related to the architecture of the website, service of the web integration and other information which a tester needs as a guide to the website are generated in this first step.
ii. Necessary tools are installed for the purpose of experimentation.
iii. Website is checked for the presence of firewalls and other different active security protocols.
iv. Configuration and platform testing.
v. Handling error and verification of test data.
vi. Testing the protection related to encryption.
vii. Business and client-side logic verification and testing.
viii. Report generation remedies and suggestions.
ix. Cleanup and reset the vulnerabilities.

3. Attacks and Tests

3.1 Information Gathering Using Whois

Whois is an online tool that is used for gathering information about the website related to its domain name, internet protocol (IP) address, it also gets a wider range of information about the query sent from the whois web server. In fact, the information gathered by whois is publicly available and can be extracted with no efforts made to penetrate the structure of the website or servers.

Whois scanning results for the website Helios pharma.com are provided below in the figures.

We can directly access the whois information gathering tool from its website and can also use this whois tools in the command line interface of any Linux distribution environment by simply typing the command:

whois <domain_name_of_target>

Domain Information

Domain:	healios-pharma.com
Registrar:	Name.com, Inc.
Registered On:	2020-11-03
Expires On:	2022-11-03
Updated On:	2021-10-31
Status:	clientTransferProhibited
Name Servers:	ns-1076.awsdns-06.org ns-1812.awsdns-34.co.uk ns-416.awsdns-52.com ns-873.awsdns-45.net

Figure 3: Domain information shown in Whois

Administrative Contact

Name:	Whois Agent
Organization:	Domain Protection Services, Inc.
Street:	PO Box 1769
City:	Denver
State:	CO
Postal Code:	80201
Country:	US
Phone:	+1.7208009072
Fax:	+1.7209758725
Email:	https://www.name.com/contact-domain-whois/healios-pharma.com

Figure 4: Administrative details shown in Whois

Raw Whois Data

```
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#clientTrar
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.c
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
```

Figure 5: Raw Whois Data

Technical Contact

Name:	Whois Agent
Organization:	Domain Protection Services, Inc.
Street:	PO Box 1769
City:	Denver
State:	CO
Postal Code:	80201
Country:	US
Phone:	+1.7208009072
Fax:	+1.7209758725
Email:	https://www.name.com/contact-domain-whois/healios-pharma.com

Figure 6: Technical details shown in Whois

Registrant Contact

Name:	Whois Agent
Organization:	Domain Protection Services, Inc.
Street:	PO Box 1769
City:	Denver
State:	CO
Postal Code:	80201
Country:	US
Phone:	+1.7208009072
Fax:	+1.7209758725
Email:	https://www.name.com/contact-domain-whois/healios-pharma.com

Figure 7: Registrant details shown in Whois

3.2 Nmap scan of Website

Nmap is frequently used by experts in the cyber security field to audit the security and expiration of the network of a website as this is an open-source tool. And Nmap generally expands to 'network mapper' for its literal understanding. It is also available on both the online and the command line interface. For online network mapping the website using Nmap we just have to go to the site ‘nmap.online’. Although in this project Nmap scan is done through the command line interface of Kali Linux by just simply typing the command.

>>nmap-sS heaslios-pharma.com

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

Port	Protocol	State	Service
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

```
┌──(samaksh㉿kali)-[~]
└─$ sudo nmap -sS healios-pharma.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-16 16:46 IST
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 8: Nmap result

3.3 Spidering and Mapping site using Burp Suite

The purpose of Spidering is to identify the context and the scope in which we want to scan the website for its structure for the web forms and the embedded links on the website. In the Burp Suite's automatic spider link, it automatically performs the spidering and records all the links request and intercept sent to the website, also follows the link forms and requests from the web server and all the requests are recorded while performing spidering.

Sitemap depicts all the important information about its content and the issues of securities that have been discovered in the targeted application. The sitemap helps us view the requests and responses for every single item and details about every discovered issues. The sitemap for the site pharma.com is given in the figure below, the site consists of the main directory http://heailos pharma.com inside which it has folders: assets, icons, includes. The findings indicate that the website is of a simple tree structure. The assets folder contains the information of the CSS code of the website, fonts used in the development of website external structure, the images used in the

illustration, and various graphical representation. The assets folder also contains the front-end javascript code of the website.

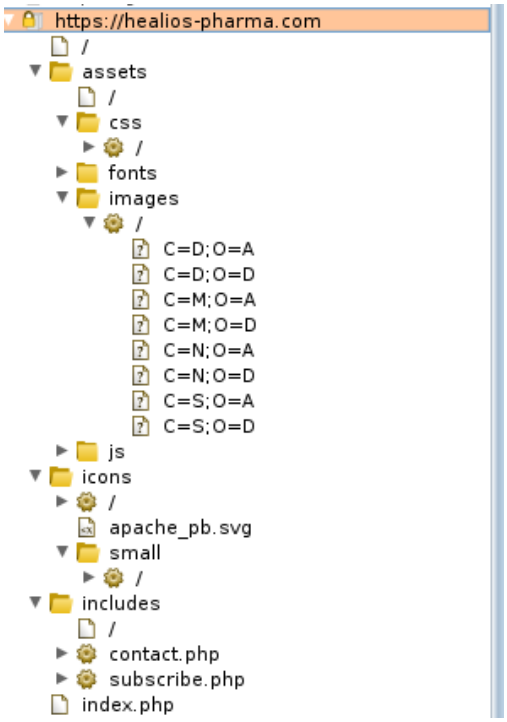


Figure 9: Sitemap of the main directory on domain helios-pharma.com

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 10: Details about the asset folder shown in sitemap

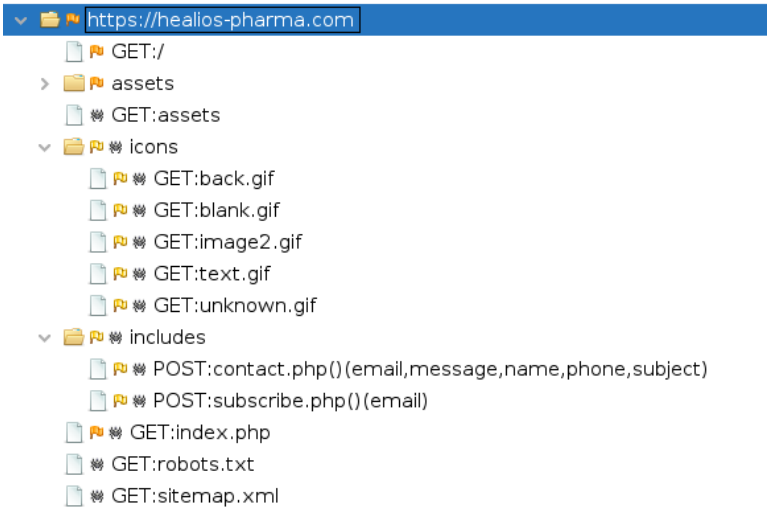


Figure 11: Detailed view of the main directory

3.4 Probing Hidden Files With ZAP

The Zed attack proxy from OWASP is a tool that is based on the graphical user interface and coded in Java. This tool allows us to test the web application security and perform forging proxying spidering and scanning on the web application in order to attack. Being a tool of Java, it can be run on almost every operating system which supports Java. Zap can capitalize on the Kali Linux distribution. We can set up a proxy via web browser and intercept the packet communication between the website and the server. The website with which we are communicating, in this case, is healiospharma.com is mapped on the ZAP interface at the left side now by right-clicking on the website from the options menu we can select the option for scanning it for hidden files. Hidden files are the files that are either left by the developer of a website or the junk files which may or may not influence the vulnerability of the website.

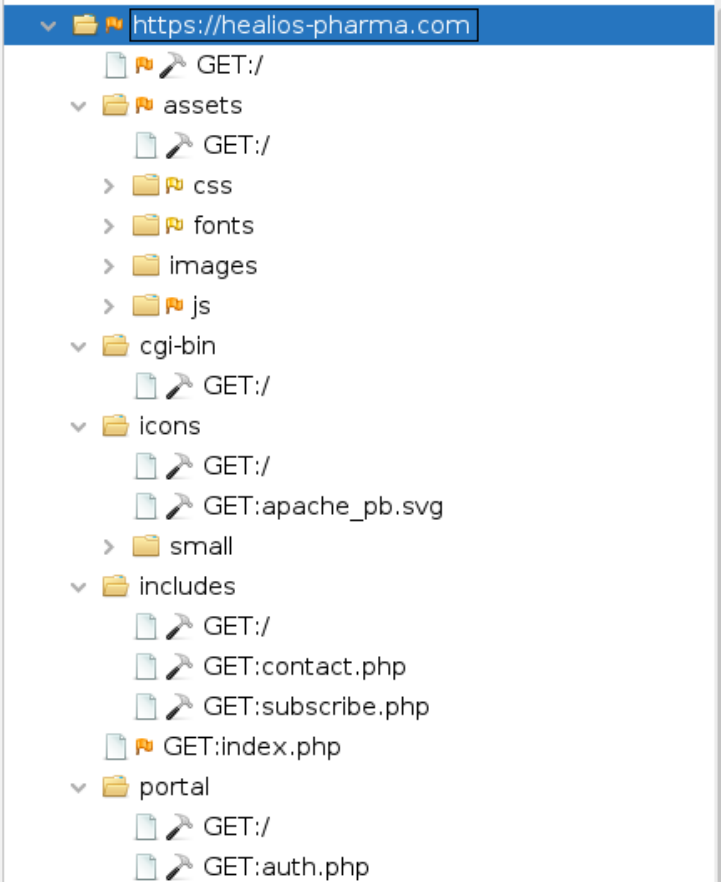


Figure 12: Sitemap showing the hidden files in detail

In order to jeopardize the network to a greater extent, it looks for the hidden files that can overload the network sometimes and take time for performing discovery for hidden files, but it is worth it. There are two folders found where the hidden files scan with zap in the main website folder *http://healios-pharma.com*. Those folders are cgi-bin and portal. These two folders are not included in the external structure of the website and are hidden from the main structure although the cgi-bin folder contains the single file, and the portal folder contains two files. Files and folder are as follow:

http://healios-pharma.com

assets

cgi-bin

> GET:/

Icons

Includes

portals

> ***GET:/***

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

The italic bolded are the names of hidden files and folders in the structure of the website.

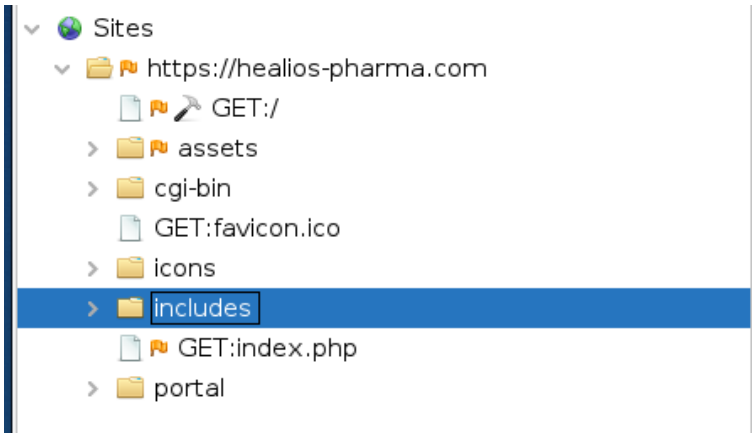


Figure 13: Sitemap showing the main hidden files in the directory

3.5 Active Scanning Using ZAP

Active scanning using ZAP is a way to find vulnerabilities in a website in an automated style. Using the tool active scan, the website is scanned for possible targets, vulnerabilities and it is only recommended against the written permission from the website holder for a website to be analyzed by the penetration tester.

Active scanning in ZAP does not give the whole detailed idea of every possible vulnerability and missing links on the website, it provides a brief automated and shortcut way to analyze the vulnerabilities. Logical vulnerabilities in the website, like a vulnerability of broken access control, are hard to be determined; in fact, they cannot be determined by an automated vulnerability scanning in ZAP. In this kind of vulnerability testing, manual penetration testing should be performed.

The automatic scan is simple, we just have to 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 has to use the traditional spider or not.

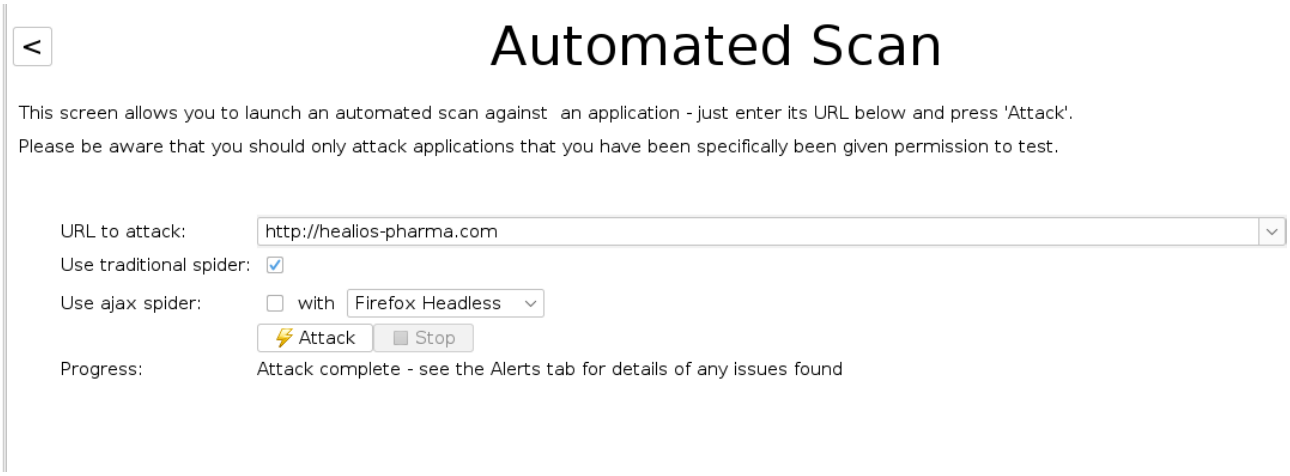
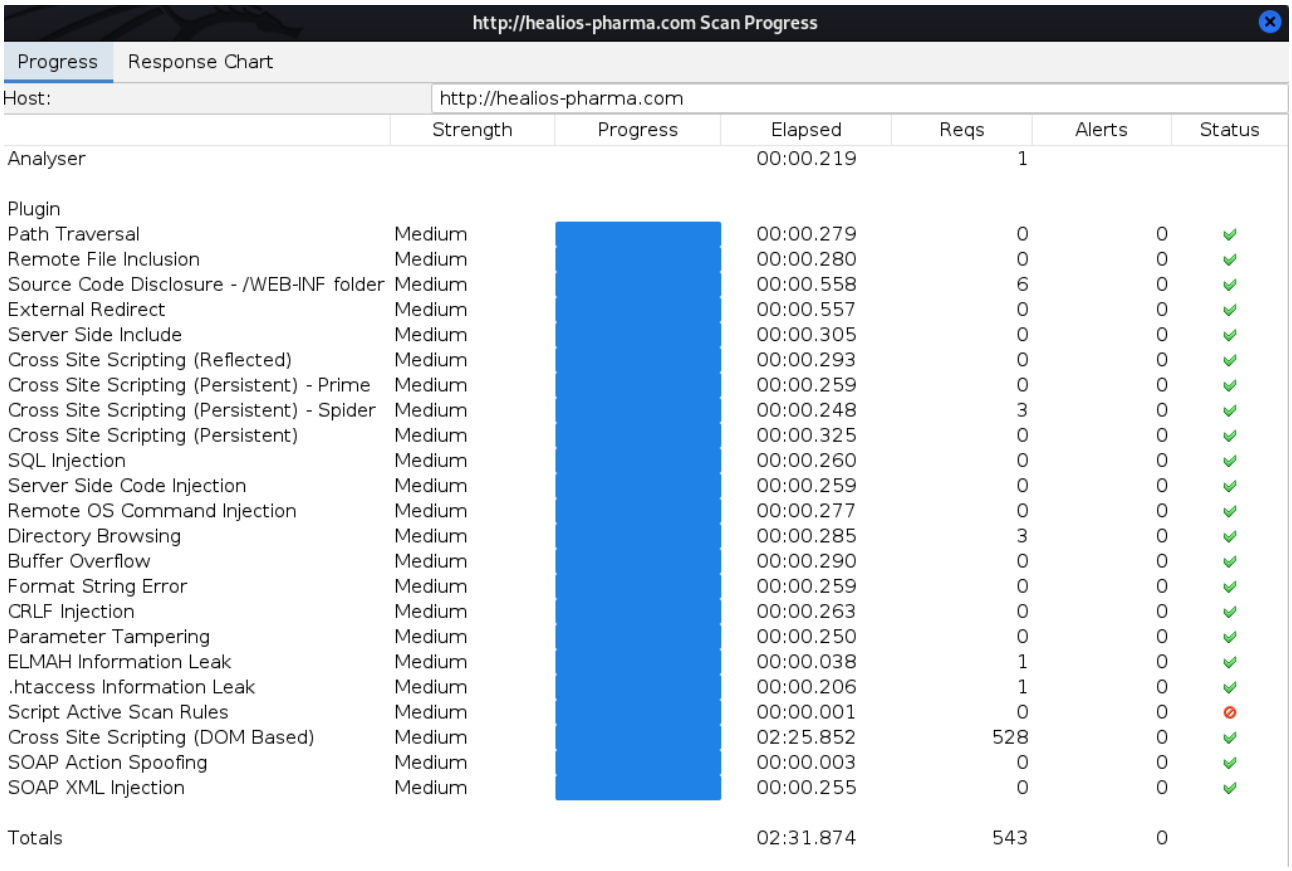


Figure 14: Automatic scan main page



http://healios-pharma.com Scan Progress

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 15: Automated scan results

3.6 ZAP scanning and Vulnerability analysis

Context of analysis: No specified contexts were selected, so all contexts were included by default by the software.

Sites: The following sites were included:

http://healios-pharma.com

https://healios-pharma.com

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

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

Alertness counts by risk and confidence measures:

The table below depicts the number of alerts for each level of risk and confidence included in the report. (The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		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

This table shows the number of alerts of each alert type, together with the alert type's risk level. (The percentages in brackets represent each count as a percentage, rounded to one decimal place of the total number of alerts included in this report.)

Alert type	Risk	Count
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 URL https://healios-pharma.com/ have an alert of medium security vulnerability and is suspected to be vulnerable toward script, set cookie and comment. The same goes for URL https://healios-pharma.com/index.php which is script, comment vulnerable.

3.7 Web application Firewall Detection with WAFW00F

Web applications use one of the strongest defenses against attacks and it is the firewall. A firewall is very effective against small and trivial attacks, in some cases, it has been seen that the presence of a firewall reduces the small and the trivial attacks of a website by about 20%, thus a wire of firewall is recommended for every website in every case. There are various private companies like Cloudflare which provide firewall security for websites.

WAFW00F being an industry-level tool that is encoded in Java takes the work of fingerprinting a website from the hand of a penetration tester and does it automatically. The result of web proof is pretty solid and determines the underlying firewall used by the website services. WAFW00F as told in the distribution of Linux and on any python systems, firewall detection can also be done by some script of any map, but the results given by web proof are very consistent and on the solid grounds of its firewall detection history.

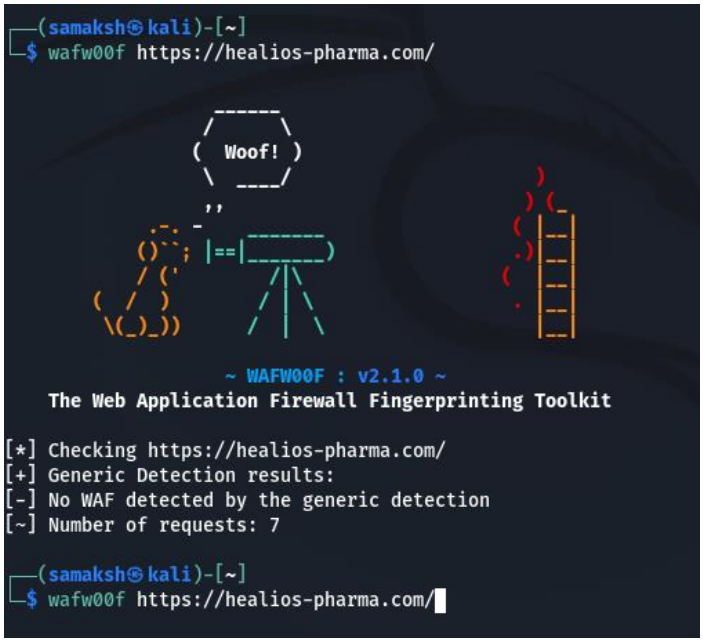


Figure 16: WAFW00F results for domain helios-pharma.com

For the website https://healios-pharma.com, WAFW00F detects the presence of no firewall.
No WAF detected by the generic detection
This can be very dangerous for the website; it can be susceptible to numerous attacks**.**

3.8 Cookies Collection

Cookies contain very sensitive information about the individuals who visit the websites, so it becomes the responsibility of web server holders to handle their cookies with very sensitive care.

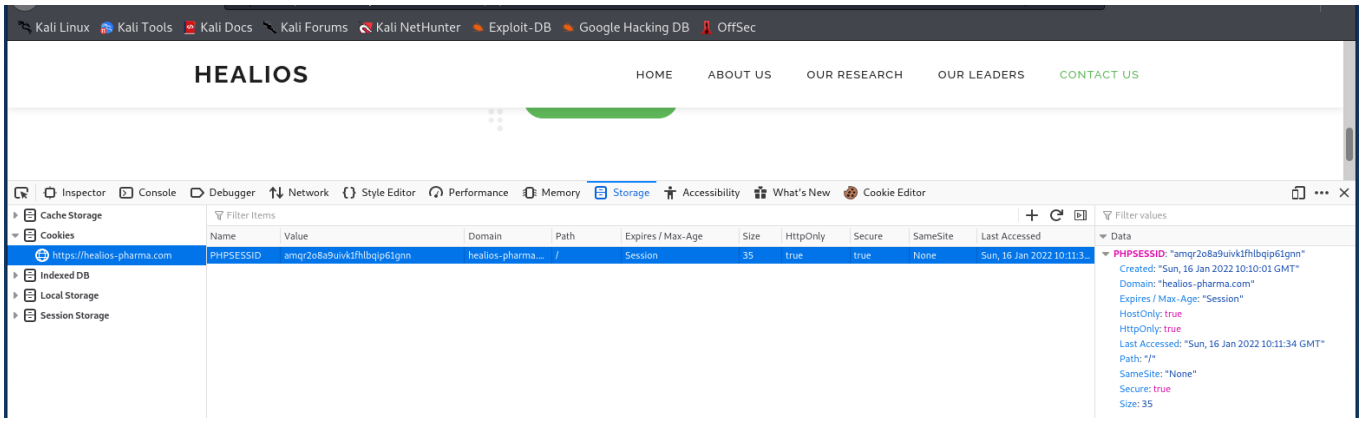


Figure 17: Cookies found on the domain helio-pharma.com

On the website, https://healios-pharma.com/ cookies are handled with care and the cookies protection is turned on. Although this is a very primitive way to trick website visitors to surrender their sensitive information, here it is not the case.

3.9 Security Scan Using Nikto

Nikto is a tool and scanner which runs on Linux distribution. Due to it being open source, it can be used by anyone to scan any web servers for vulnerabilities (Nginx, IHS, Litespeed, OHS, Apache etc.). It is a perfect all capable scanning tool that can be deployed on any web server. It has a strong capability of scanning over 6700 files on any webserver to detect misconfigurations, weak spots and risky files.

Here are the results of a Nikto scan done to find out the suspected vulnerabilities and potential threats.

i. The anti-clickjacking X-Frame-Options header is not present.
ii. The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS.
iii. The site uses SSL, and the Strict-Transport-Security HTTP header is not defined.
iv. The site uses SSL, and the Expect-CT header is not present.
v. The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME-type.

vi. OpenSSL/1.0.2k-fips appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.

vii. Web Server returns a valid response with junk HTTP methods, this may cause false positives.

viii. OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST.

4. Solutions for Threat Discovered

4.1 SQL injection Remedies and protection

In SQL injection, a user from any untrusted IP tries to provoke the query in the database by entering the symbols and the special alphanumeric quotes as the input in the site of SQL database. In many cases SQL injection may lead to heavy data breaches in the company's database.

Proper client-side input validation and filtering the hazardous character out of the user input must be the forward step to avoid SQL injection; additional statements can be prepared and parameterized to be stored as the text in the input parameters of the website.

Sample code to validate the input of 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

Forensic methodology used to investigate and restore deleted files

Data forensics is based on the fact that, when we delete the pre-existing data and the data is transferred in the recycle bin only the pointer record of the data changes from pointing to the memory location to pointing to the recycle bin, and if we empty the recycle bin or use shift+delete it only deletes the pointer record of the data. The existing data is not lost until it is overwritten by another data. If this storage device is handled professionally the data can be easily restored.

The steps that are used in the security analysis techniques and procedures module to investigate and restore the deleted files are as follows:

Procedure development

Digital evidence can be delicate and highly sensitive. This evidence can be easily compromised if not properly handled and protected. Hence it is critical to follow strict guidelines and procedure for activities related to computer forensic investigation, these include detailed instruction about how to properly prepare a system for evidence retrieval, how to document these activities to help and ensure the authenticity of data and to recover potential digital evidence.

An integral part of the security analysis techniques and procedure module is the modification of a set of explicitly stated actions regarding what constitutes evidence, where to look for evidence and how to treat it once it has been retrieved. Before any investigation, proper steps must be taken to determine the details of the case at hand and obtain any permission needed prior to purchasing the case.

Evidence assessment

The assessment of potential evidence in cybercrime is a key component of the investigative process. Prior to conducting any investigation, the type of evidence sought (include specific platforms and data format) must be defined by the investigator and have a clear understanding of how to preserve pertinent data. The computer forensic investigator uses sophisticated methods to shift through hard drives, email, social networking sites and other digital archives to receive and access any information that can serve as viable evidence of the crime.

Evidence acquisition

The most critical path of successful forensic investigation could be a rigorous and detailed plan for acquiring evidence. Detailed documentation is needed after, during and prior to the acquisition process. The process for preserving evidence includes the physical removal of storage devices to retrieve sensitive data and ensure functionality and taking appropriate steps to copy and transfer evidence to the investigator system.

We should always follow the order of volatility before acquiring and evidence that means collecting the most volatile evidence first and least volatile evidence last. A computer that is running has critical data stored in its RAM (Random access memory) and data can be lost if the computer is turned off. It is very important to collect the content of the RAM before you turn off the computer and this is the first content to collect by the order of volatility. Once you collect the content of RAM then you can proceed to collect any evidence on hard drives, external devices in CD and other hard copy evidence. Every evidence should be labelled with a case number and an identifier so that you can identify individual devices.

Evidence examination

Proper procedure must be followed for retrieving, copying and storing evidence within an appropriate database. A variety of methods and approaches are used to analyze information and examine data from the designated archives. Analyzing software can be used to search massive archives of data for specific file types or keywords and retrieving files that have recently been deleted. The files and programs that have intentionally been encrypted or hidden can be particularly helpful in investigation.

Specific data like where and when specific files were created, uploaded or downloaded can be obtained by the file name. As file names point to the address of files, if the file is located on other servers or systems, it can be tracked through their file name. Now various cyber forensic tools are used to analyze the disk image and find out and recover any hidden or deleted data. Images and videos can also be analyzed using these tools and all the information like the device used to take it and the time of taking the photograph or video is found. During this phase the investigators work in close proximity with other law enforcing bodies to properly understand the case and collect all the evidence necessary.

Documenting and reporting

All the steps taken to conduct the investigation must be properly documented, including the specs of the hardware and software used, the methods used for testing system functionality of the system, retrieving the storage devices, making copies of the data, and activities done to examine and access the copied data. This ensures that proper procedure has been followed for the investigation, while staying within the boundaries of law. These documents can also be used to cross check the investigator so every detail given in the report must be completely true and relevant.

6. Forensic Report

Overview/case summary

Nera Star, an employee of Healios Pharmaceutical Company (HPC), was working on a human vaccine for Covid-19 treatment. Her research files had sensitive chemical formulae and mathematical codes that she had researched on for the past six years. She had a fight with the management for side-lining her while promoting Napel as Senior Scientist. In a fit of rage, she deleted all the critical research documents so that no one could access them.

Objective

This report is the summary of the processes and methods used to investigate and recover the deleted files containing chemical formulas and mathematical codes. If the data was not retrieved, the firm stood to lose USD 3 million in various contracts with the suppliers.

Evidence analyzed

Pursuant to the order, I inspected the data on the computer Nera was working with. Using widely accepted digital forensic techniques and procedures a bit for bit, forensic copies of the hard drive of the computer were made. By using the digital forensic copying process the entire contents of the hard disk, including the user-accessible files, deleted files, and unallocated space, which may contain deleted content was captured. As it had been a week since the computer was used by her there was no point searching the RAM of the computer.

Investigation steps

The bit-for-bit forensic copy of the hard disk was made using the tool called FTK imager. The FTK imager performs sector by sector analysis of the hard disk and uncovers any hidden files and documents. MD5 hash of the bit stream images was generated. Now the image of the hard disk is used for any forensic investigation rather than the hard disk to avoid loss of evidence and the hard disk is locked away safely. Autopsy/the Sleuth Kit was used to analyze the hard disk and find out the data that is most relevant to the case.

First MACtime tool was used to create a timeline of all the files, as we needed to look for the data that was not backed up by the enterprise central backup machine while it was under construction. This narrows down the search area for the specific file or data, then it was used to list all the meta-data entries about the data in the hard disk on which autopsy is performed. The metadata obtained

was searched through using find tools for specific metadata entries. In this way our search area was greatly minimized.

Now keywords and other searches were performed on the targeted files by running a hexadecimal editor to find any relevant information stored in them. Undeleted utilities were run on the entire hard disk to see whether there are any deleted files left. The entire hard disk was viewed in hexadecimal image format and analyzed for portions of deleted data. Then the portion of data left is recovered using scavenger utilities. Certain unsearchable file types like videos and photographs with no text were manually checked for any relevant information regarding the covid-19 treatment vaccine. All the data that can be scavenged was handed over to HPC (Healios Pharmaceutical Company).

CONCLUSION

The website *https://healios-pharma.com/* is tested against a black box penetration test via several tools like Whois, Nmap, Burp Suite, Zed attack proxy (ZAP), WAFW00F and Nikto. All These are the linux based penetration testing tool as the whole penetration test was carried out on a linux distribution, Kali Linux.

The overall security of the website is not very strong, and the website is vulnerable to a lot of attacks. First and foremost being the absence of a firewall. A firewall is always a must for any commercial website. In my recommendations this website should have a Cloudflare firewall Protection. Cloudflare has a base plan for any business website starting from 200$/month and enterprises can have their costume plans. Vulnerabilities may take many weeks of routine penetration testing and code correction to fix the errors and vulnerabilities of the website. For a penetration working for website securities, it may cost up to $10,000 for the vulnerabilities and code correction.

The hardware of the server must be advanced in order to perform at the optimum levels all the time any outdated component in the server configuration must be immediately replaced.

References

[1] L. R. JohnsonIII, "Science DIrect," 2014. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/forensics-tool.

[2] L. E. D. Larry E. Daniel, "Science Direct," 2012. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/forensic-process.

[3] "Norwich University Online," 11 September 2017. [Online]. Available: https://online.norwich.edu/academic-programs/resources/5-steps-for-conducting-computer-forensics-investigations.

[4] None, "Rec Faces," 18 January 2021. [Online]. Available: https://recfaces.com/articles/digital-forensics.

[5] V. M. Antunes N, "Detecting SQL injection vulnerabilities in web services," in *The Fourth Latin-American Symposium Dependable Computing.*, 2009.

[6] 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.

[7] 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.

[8] O. J, "IBM," 2011. [Online]. Available: http://www.ibm.com/developerWorks.

[9] A. K. Ravneet Kaur, "Digital Forensics," *International Journal of Computer Applications*, vol. 50, no. 5, pp. 5-9, 2012.

[10] K. Orrey, "Vulnerability Assessment," [Online]. Available: http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html.

[11] R. D. S. Vijay, "Software testing help," 3 January 2022. [Online]. Available: https://www.softwaretestinghelp.com/penetration-testing-tools/.