



INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

# **6COSC019C.2 Cyber Security Coursework**

## **Report**

Gayana Jayawardena

w1761099 / 2019411

**Module Leader:** Saman Hettiarachchi

**Date:** 09<sup>th</sup> May 2023

## Table of Contents

<b>List of Figures.....</b>	<b>3</b>
<b>Part A - Information Gathering .....</b>	<b>4</b>
<b>1 OSINT Activities .....</b>	<b>4</b>
<b>2 Reconnaissance.....</b>	<b>10</b>
<b>3 Port Scanning and Enumeration .....</b>	<b>12</b>
<b>Part B - Server-side exploits.....</b>	<b>13</b>
<b>1 Data tampering.....</b>	<b>13</b>
<b>3 XSS Scripting .....</b>	<b>17</b>
<b>4 OWASP vulnerable machine contains several other vulnerabilities that can be exploited ..</b>	<b>19</b>
<b>Part C -Client-side exploits .....</b>	<b>21</b>
<b>1) Man in the Middle Attack (MiTM).....</b>	<b>21</b>
<b>2 Social engineering attack.....</b>	<b>23</b>
<b>Part D - Denial of Service attacks.....</b>	<b>25</b>
<b>1 DoS the web server.....</b>	<b>25</b>
<b>Part E - Recommendations to protect the scenario company server .....</b>	<b>27</b>
<b>Reference .....</b>	<b>31</b>

## List of Figures

Figure 1-Harvester .....	4
Figure 2-harvester Info .....	5
Figure 3-Nmap.....	5
Figure 4-Port Scanning .....	6
Figure 5-spiderfoot .....	7
Figure 6-Spiderfoot Info .....	8
Figure 7-Spiderfoot Scan.....	8
Figure 8-Spiderfoot Graph .....	9
Figure 9-Robot.txt file .....	10
Figure 10-Jotto Game Interface .....	10
Figure 11-Jotto game answers.....	11
Figure 12-DirtBuster Results .....	11
Figure 13-Tcp Ports .....	12
Figure 14-Tamper Data .....	13
Figure 15-Tamper data Details.....	13
Figure 16-Tamper data Info .....	14
Figure 17-SQL injection 1 .....	15
Figure 18-SQL injection output .....	16
Figure 19-XSS Output.....	17
Figure 20-XSS successful message .....	18
Figure 21-Owasp command execution .....	19
Figure 22-Owasp Output.....	19
Figure 23-Ettercap host list adding .....	21
Figure 24-Adding target IP addresses .....	22
Figure 25-Verification of Ettercap filter .....	22
Figure 26-SEToolkit interface .....	23
Figure 27-Peruggia Login page.....	24
Figure 28-Wireshark ping Output .....	25
Figure 29-Checking Firewall status .....	29
Figure 30-adding firewall to port .....	29
Figure 31-sending traffic to port.....	30

# Scenario

A mid-sized transportation business with a fleet of trucks contacted my organization to perform a vulnerability assessment. The business keeps track of the whereabouts and condition of each fleet car using a GPS monitoring device. The system keeps track of private data such as delivery schedules, driver information, and vehicle whereabouts. GPS monitoring technology is used by staff members with various jobs and access levels. About fifty drivers use mobile or in-vehicle devices for navigation and updates, while three administrators are in charge of system maintenance and configuration, eight dispatchers keep an eye on the fleet and oversee driver assignments. The database stores the staff login information. The safety of the company's GPS tracking technology, which ensures the safety of the vehicle and the driver, is its top priority.

## Part A - Information Gathering

### 1 OSINT Activities

#### EXAMPLE 01 – using the harvester

```
(kali@kali)-[~]
$ theHarvester -d cwscenario.site -b all
*****
*                                     *
* [TheHarvester]                    *
* [TheHarvester]                    *
* [TheHarvester]                    *
* [TheHarvester]                    *
* [TheHarvester]                    *
* theHarvester 4.2.0                 *
* Coded by Christian Martorella      *
* Edge-Security Research             *
* cmartorella@edge-security.com      *
*                                     *
*****

[*] Target: cwscenario.site

[!] Missing API key for binaryedge.
[!] Missing API key for Censys ID and/or Secret.
[!] Missing API key for fullhunt.
```

Figure 1-Harvester

An effective open-source intelligence (OSINT) tool for learning more about a target domain is called TheHarvester. It makes it possible to look up email addresses, subdomains, hosts,

and other relevant data from a variety of places, including search engines, social media networks, and open databases.

```
[*] Searching Otx.
[*] Searching Rapiddns.
An exception has occurred: Cannot connect to host www.threatcrowd.org:443 ssl
:True [SSLCertVerificationError: (1, "[SSL: CERTIFICATE_VERIFY_FAILED] certifi
cate verify failed: Hostname mismatch, certificate is not valid for 'www.thr
eatcrowd.org'. (_ssl.c:992)")]
string indices must be integers, not 'str'
[*] Searching Threatcrowd.
[*] Searching Threatminer.
[*] Searching Urlscan.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected
mimetype: text/html; charset=utf-8', url=URL('https://sonar.omnisint.io/all/
cwscenario.site?page=1')
[*] Searching Omnisint.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected
mimetype: text/html; charset=utf-8', url=URL('https://api.sublist3r.com/sear
ch.php?domain=cwscenario.site')
[*] Searching Sublist3r.

[*] ASNS found: 1
AS8560

[*] Interesting Urls found: 1
https://cwscenario.site/

[*] LinkedIn Links found: 0

[*] IPs found: 3
50.87.192.155
217.160.0.219
2001:8d8:100f:f000::2b6

[*] No emails found.

[*] Hosts found: 10
autodiscover.cwscenario.site:195.20.225.174
cpanel.cwscenario.site
cpcalendars.cwscenario.site
cpcontacts.cwscenario.site
mail.cwscenario.site
webdisk.cwscenario.site
webmail.cwscenario.site
www.cwscenario.site:217.160.0.219
```

Figure 2-harvester Info

## Example 02 -using nmap

```
(kali㉿kali)-[~]
$ nmap -sT 217.160.0.219
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 01:14 +0530
Nmap scan report for 217-160-0-219.elastic-ssl.ui-r.com (217.160.0.219)
Host is up (0.16s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Figure 3-Nmap

```
(root@kali)-[/home/kali]
# sudo nmap 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-04 00:34 +0530
Nmap scan report for 192.168.56.102
Host is up (0.0052s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
5001/tcp  open  complex-link
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 4.88 seconds
```

Figure 4-Port Scanning

OSINT is particularly helpful for penetration testing since it enables the testers to spot security flaws and areas where data may be accessible to intruders. OSINT may also be used to identify the open ports.

The server of the estate agency firm becomes open to attacks once the attackers get access to all of its details. When an attacker learns that the ports are open, they can take over the server. Giving the attackers the chance to gain access to the database that contains all of the user information and financial information for property owners.

### Example 03 -using the spiderfoot tool

```

(kali@kali)-[~]
$ spiderfoot -l 127.0.0.1:5001
/usr/lib/python3/dist-packages/ipwhois/whois.py:412:
SyntaxWarning: "is not" with a literal. Did you mea
n "!="?
    if count is not 0 and count < 4:
/usr/lib/python3/dist-packages/ipwhois/whois.py:548:
SyntaxWarning: "is not" with a literal. Did you mea
n "!="?
    asn_data['asn_registry'] is not 'arin'):
2023-05-15 16:28:04,678 [INFO] sf : Starting web ser
ver at 127.0.0.1:5001 ...
2023-05-15 16:28:04,688 [WARNING] sf :
*****
*****
Warning: passwd file contains no passwords. Authenti
cation disabled.
Please consider adding authentication to protect thi
s instance!
Refer to https://www.spiderfoot.net/documentation/#s
ecurity.
*****
*****

*****
*****
Use SpiderFoot by starting your web browser of choi
ce and
browse to http://127.0.0.1:5001/
*****
*****

http://127.0.0.1:5001/

```

Figure 5-spiderfoot

Users of the program may adjust and personalize the scanning and data collecting process using the web-based interface. It supports a number of modules and plugins that may be activated to collect particular kinds of data. SpiderFoot is a flexible tool for OSINT jobs since it facilitates interaction with various tools and frameworks.

Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Internet Name	7	7	2023-04-10 22:18:56
Co-Hosted Site	2	12	2023-04-10 22:17:23
DNS TXT Record	1	1	2023-04-10 22:17:17
Domain Name	1	10	2023-04-10 22:17:50
Email Gateway (DNS MX Records)	2	2	2023-04-10 22:17:17
HTTP Headers	31	31	2023-04-10 22:22:50
HTTP Status Code	2	31	2023-04-10 22:22:50
IP Address	1	2	2023-04-10 22:20:17
IPv6 Address	1	2	2023-04-10 22:18:57
Internet Name	3	28	2023-04-10 22:19:02
Internet Name - Unresolved	6	48	2023-04-10 22:19:07
Linked URL - External	8	8	2023-04-10 22:22:32
Linked URL - Internal	59	61	2023-04-10 22:22:50
Name Server (DNS NS Records)	4	4	2023-04-10 22:17:17
Raw DNS Records	4	4	2023-04-10 22:18:56
Raw Data from RIRs/APIs	3	3	2023-04-10 22:20:25
SSL Certificate - Raw Data	5	8	2023-04-10 22:17:17
Web Content	29	31	2023-04-10 22:22:50

Figure 6-Spiderfoot Info

<div> <div>cwscan1 <span>RUNNING</span></div> <div> <div>Summary</div> <div>Correlations</div> <div>Browse</div> <div>Graph</div> <div>Scan Settings</div> <div>Log</div> </div> <div> <div>🔄</div> <div>📊</div> <div>☰</div> <div>🖨️</div> <div>🔄</div> <div>⬇️</div> <div>Search...</div> <div>🔍</div> </div> </div>				
Browse / IP Address				
<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	195.20.225.174	autodiscover.cwscenario.site	sfp_dnsresolve	2023-04-10 22:24:49
<input type="checkbox"/>	217.160.0.219	cwscenario.site	sfp_dnsresolve	2023-04-10 22:17:50
<input type="checkbox"/>	217.160.0.219	www.cwscenario.site	sfp_dnsresolve	2023-04-10 22:20:17

Figure 7-Spiderfoot Scan



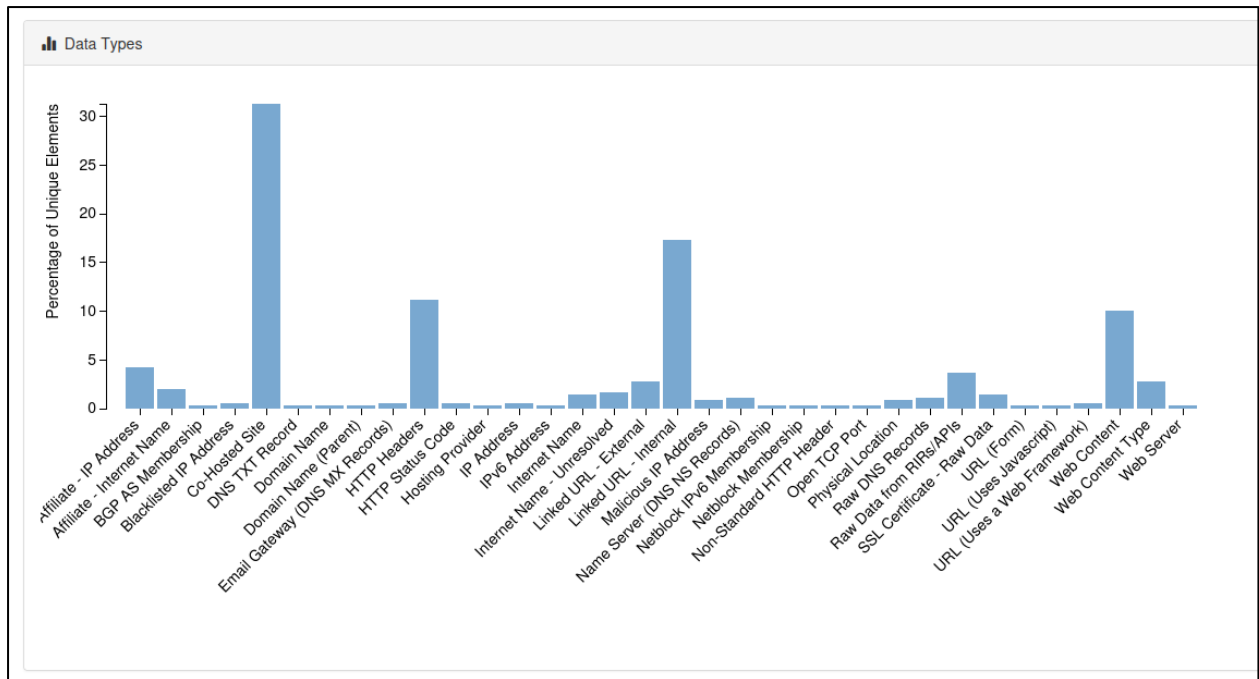


Figure 8-Spiderfoot Graph

**2)** Penetration testing requires the use of OSINT (Open-Source Intelligence), which provides important information from freely accessible sources. It facilitates data collection for penetration testers regarding the infrastructure, digital footprint, and possible vulnerabilities of the target. Target profiling, reconnaissance, attack surface mapping, exploitation planning, and social engineering are all made easier using OSINT. It is one of the initial tasks completed since it lays the groundwork for testing, forms the testing approach, and lowers the possibility of unpleasant surprises during the assessment. Penetration testers gather knowledge, spot possible flaws, and efficiently focus their efforts by performing OSINT early on.

**3)** The data gathered during the transportation industry's vulnerability assessment exposes serious threats to the security and privacy of sensitive data. Potential data breaches, insider threats, illegal system access, and poor password security are some of these concerns. These risks may lead to data abuse, operational interruptions, concerns for personal safety, and compromised confidentiality. To secure the system, stop unwanted access, and preserve the integrity and confidentiality of the data, the company must address these vulnerabilities and put in place the necessary security measures.

## 2 Reconnaissance

First, search for files and folders that aren't referenced on the website using the "robots.txt" file. This will enable us to gather useful data on the website's infrastructure.

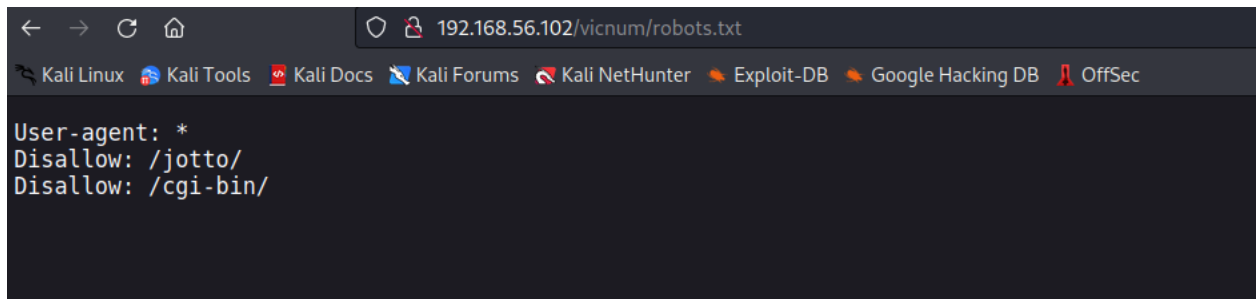


Figure 9-Robot.txt file

The "robots.txt" file gives search engines instructions on how to index a website's directories. The "jotto" and "cgi-bin" directories are not supported by all browsers, however users can browse them directly in any search engine.

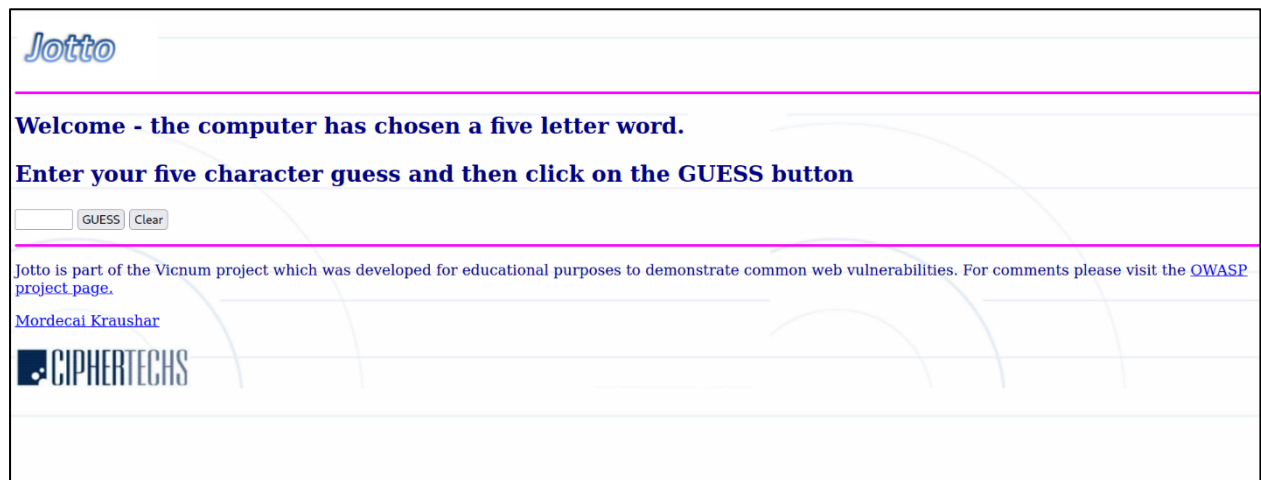


Figure 10-Jotto Game Interface

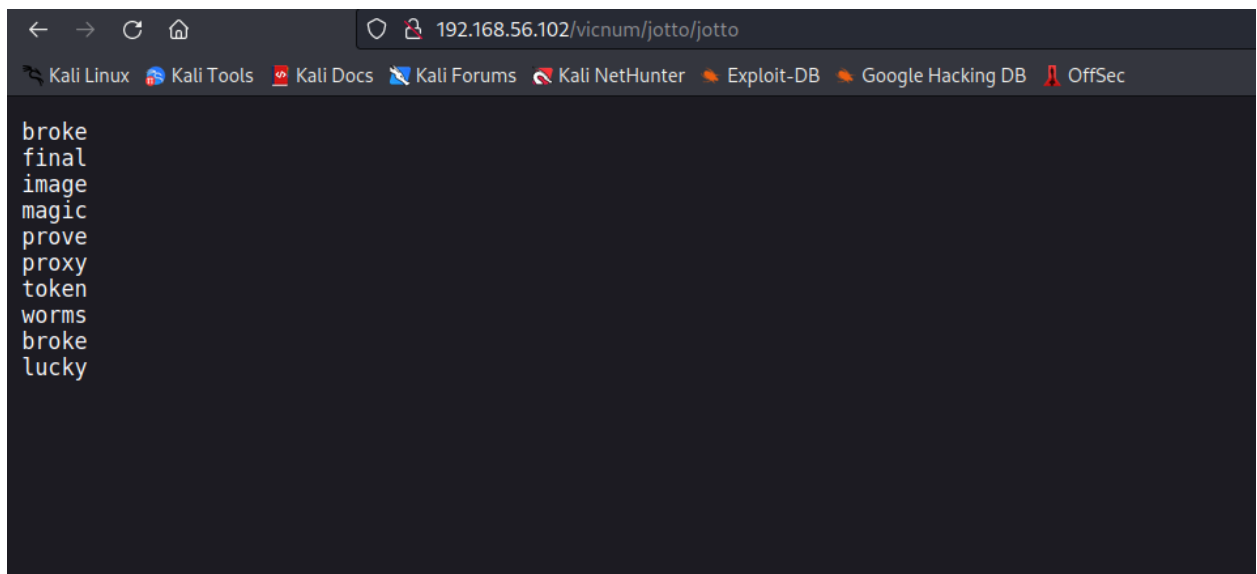


Figure 11-Jotto game answers

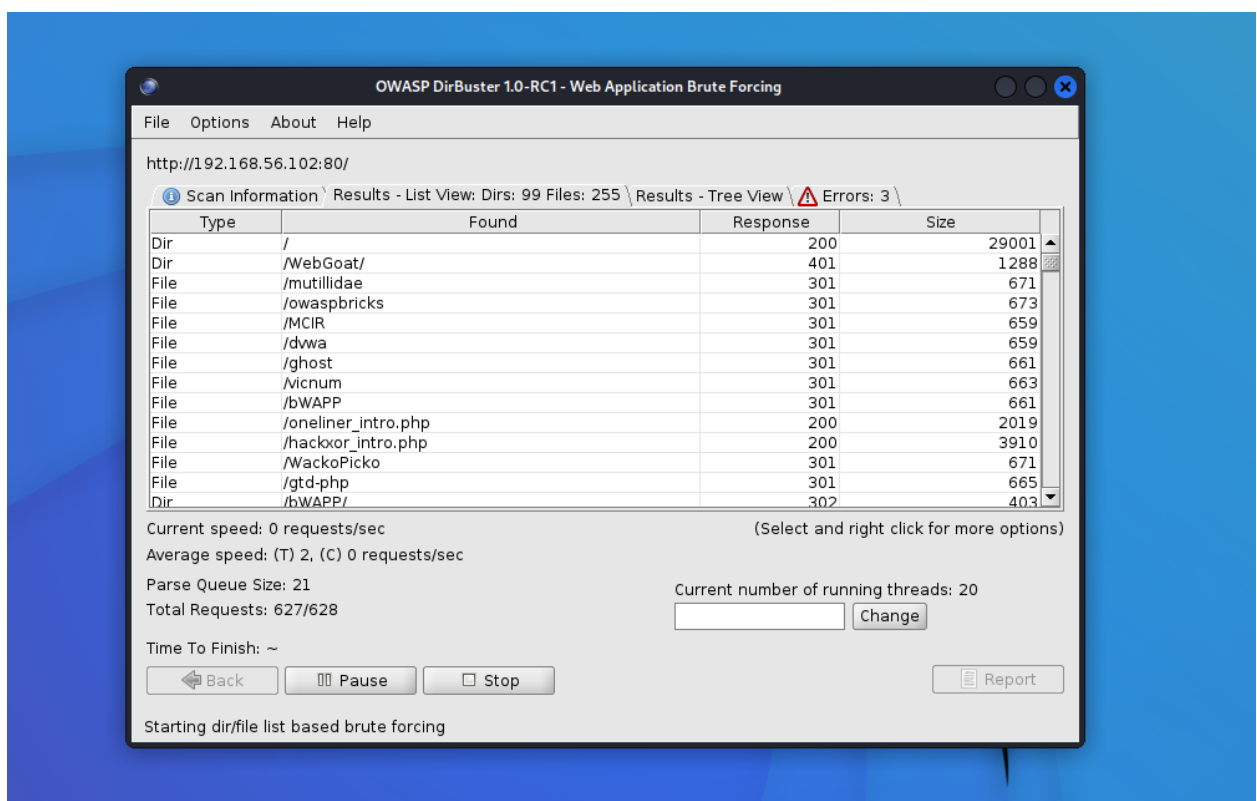


Figure 12-DirtBuster Results

According to the scenario, if an attacker used DirBuster against the server of the transportation buisness, they would be able to access several hidden files. As a result, the information or data contained in these files will likewise be accessible to these attackers.

### 3 Port Scanning and Enumeration

1.

```
(kali㉿kali)-[~]
└─$ nmap -p 1-1000 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 01:36 +0530
Nmap scan report for 192.168.56.102
Host is up (0.037s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 13.79 seconds
```

*Figure 13-Tcp Ports*

2 A communication endpoint in a computer system that is set up to listen for and receive incoming network data is referred to as a "open port." When a port is open, it indicates that the computer is prepared to engage in network communication with other devices through that specific port. In other terms, a computer system vulnerability that may be exploited by attackers is an open port.

3. Leaving open ports on a computer system poses significant security risks. Attackers can exploit these open ports to gain unauthorized access, launch brute force attacks, or exploit vulnerabilities in specific services. Malicious software can also enter through open ports, leading to data theft, system espionage, or ransomware attacks. Furthermore, open ports make the system vulnerable to denial of service (DoS) attacks, where overwhelming traffic can overload and crash the system. It is crucial to properly manage and secure open ports to mitigate these risks and protect the system from unauthorized access and potential damage.

## Part B - Server-side exploits

### 1 Data tampering

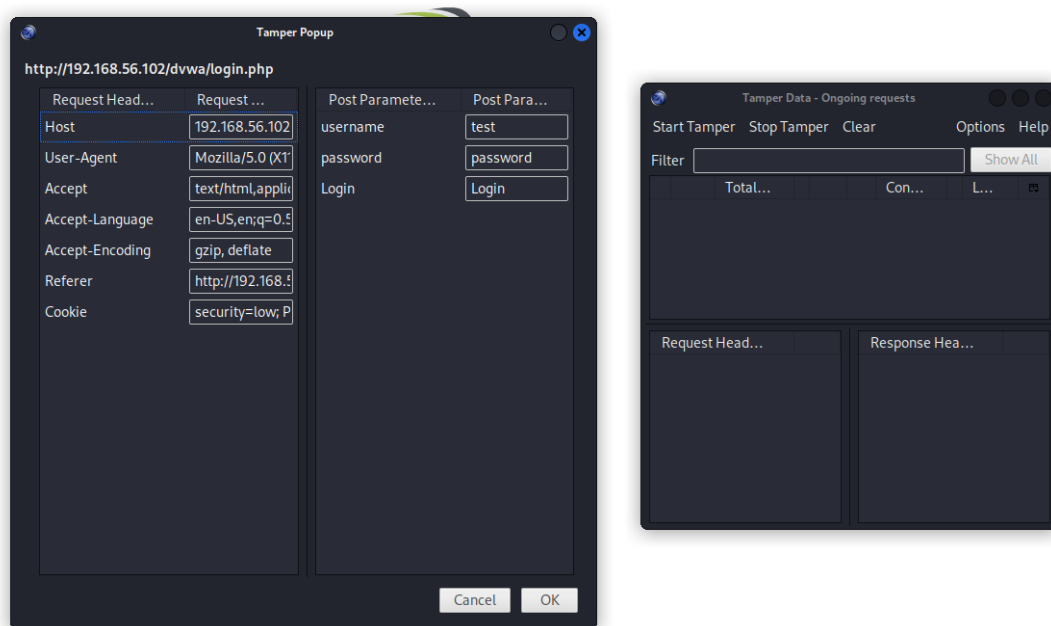


Figure 14-Tamper Data

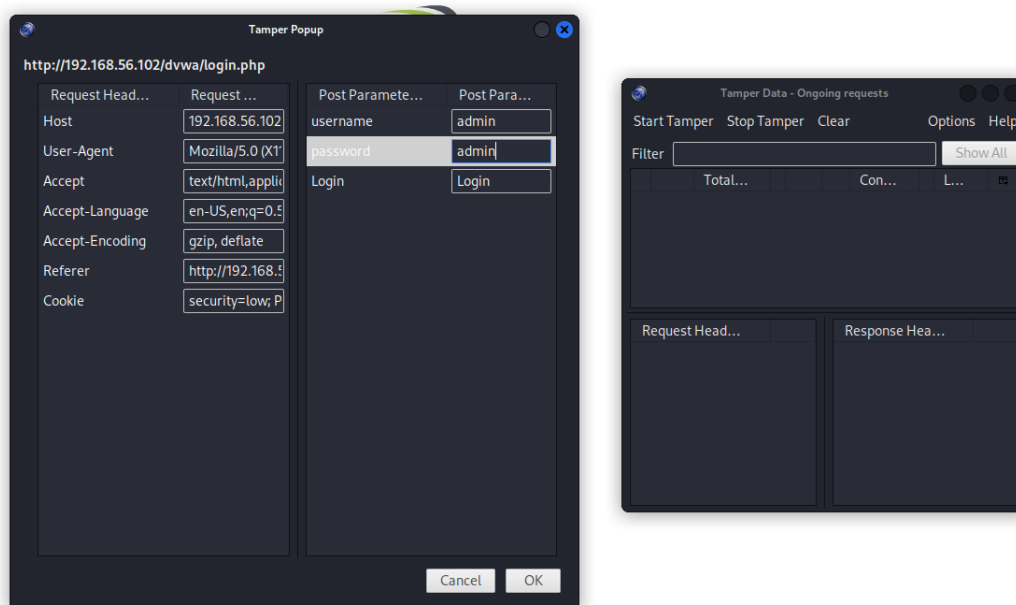


Figure 15-Tamper data Details

Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags
22:57:29.104	33 ms	33 ms	20	POST	302	text/html	http://192.168.56.102/dv...	LOAD_DOCUMENT_URI LOAD_INITI...
22:57:29.261	11 ms	154 ms	1660	GET	200	text/html	http://192.168.56.102/dv...	LOAD_DOCUMENT_URI LOAD_REP...
22:57:29.290	80 ms	80 ms	1094	GET	200	text/css	http://192.168.56.102/dv...	LOAD_NORMAL
22:57:29.291	81 ms	81 ms	413	GET	200	application/javascript	http://192.168.56.102/dv...	LOAD_NORMAL
22:57:29.292	80 ms	80 ms	6749	GET	200	image/png	http://192.168.56.102/dv...	LOAD_NORMAL
22:57:29.382	70 ms	70 ms	1406	GET	200	image/x-icon	http://192.168.56.102/dv...	LOAD_NORMAL
22:57:29.479	0 ms	0 ms	-1	GET	Loaded from cache	unknown	http://192.168.56.102/dv...	LOAD_FROM_CACHE VALIDATE_N...

Figure 16-Tamper data Info

The Web Parameter Tampering attack is based on changing application data, including user credentials and permissions, pricing and quantity of goods, etc., by manipulating parameters that are transferred between client and server. This information is often used to improve the operation and control of an application and is kept in cookies, hidden form fields, or URL Query Strings.(Web Parameter Tampering | OWASP Foundation, no date)

**2-** A security flaw known as a data tampering vulnerability allows an attacker to change data without authorization. This flaw enables an attacker to change or alter the data that the system is transmitting, storing, or processing, which can result in a number of security problems, including data loss, data theft, and system penetration.

The integrity principle of cybersecurity is broken by this kind of vulnerability. Integrity is the safeguarding of data against unlawful erasure or change. Attacks that tamper with data put the integrity of the information at risk because they provide attackers the ability to change the data in ways that the system's authorized users never intended. Serious repercussions, including monetary loss, reputational harm, and legal liability, may result from this.

Organizations should implement security measures including access controls, encryption, and integrity checks to make sure that only authorized individuals may edit the data and that any modifications made are identified and reported promptly in order to reduce the risk of data tampering. Regular security testing and assessments can also aid in locating and addressing any potential flaws in the system.

**3** Enterprises are at substantial risk from data tampering attacks because they can result in data alteration and its unfavorable effects. Every piece of data that a system transmits, stores, or processes is vulnerable to hacking, including private data, sensitive financial information, and confidential organizational information. Such assaults have the potential to cause

monetary loss, reputational harm, legal liability, and even possible personal injury to users of life-or-death services like transportation or medical equipment. Businesses should have robust security measures in place, such as access controls, data encryption, routine backups, and ongoing security testing, to reduce these risks. Another key factor in lowering the probability of data tampering attacks is employee education and training on cybersecurity best practices.

## 2 SQL injection

- 1) The SQL Injection attack was another vulnerability found in the web application operating on the server computer and leveraged during penetration testing. SQL Union queries can be used to see sensitive data, such as login credentials.

The user credentials were extracted using Union Query, as seen in the image below;

SQL-query: 1' union select user, password FROM dvwa.users -- '

The screenshot shows the 'Vulnerability: SQL Injection' page of the DVWA. On the left is a navigation menu with links like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, Insecure CAPTCHA, File Inclusion, SQL Injection (highlighted), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, and About. The main content area has a 'User ID:' label with an input field and a 'Submit' button. Below the input field, the results of the SQL query are displayed in red text: 'ID: 1' union select user,password FROM dvwa.users -- ', 'First name: admin', and 'Surname: admin'. Under the 'More info' section, there are four links to external resources about SQL injection.

Vulnerability: SQL Injection	
User ID:	<input type="text"/>
<input type="button" value="Submit"/>	
ID: 1' union select user,password FROM dvwa.users -- ' First name: admin Surname: admin	
<b>More info</b>	
<a href="http://www.securiteam.com/securityreviews/5DP0N1P76E.html">http://www.securiteam.com/securityreviews/5DP0N1P76E.html</a> <a href="http://en.wikipedia.org/wiki/SQL_injection">http://en.wikipedia.org/wiki/SQL_injection</a> <a href="http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/">http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/</a> <a href="http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet">http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet</a>	

Figure 17-SQL injection 1

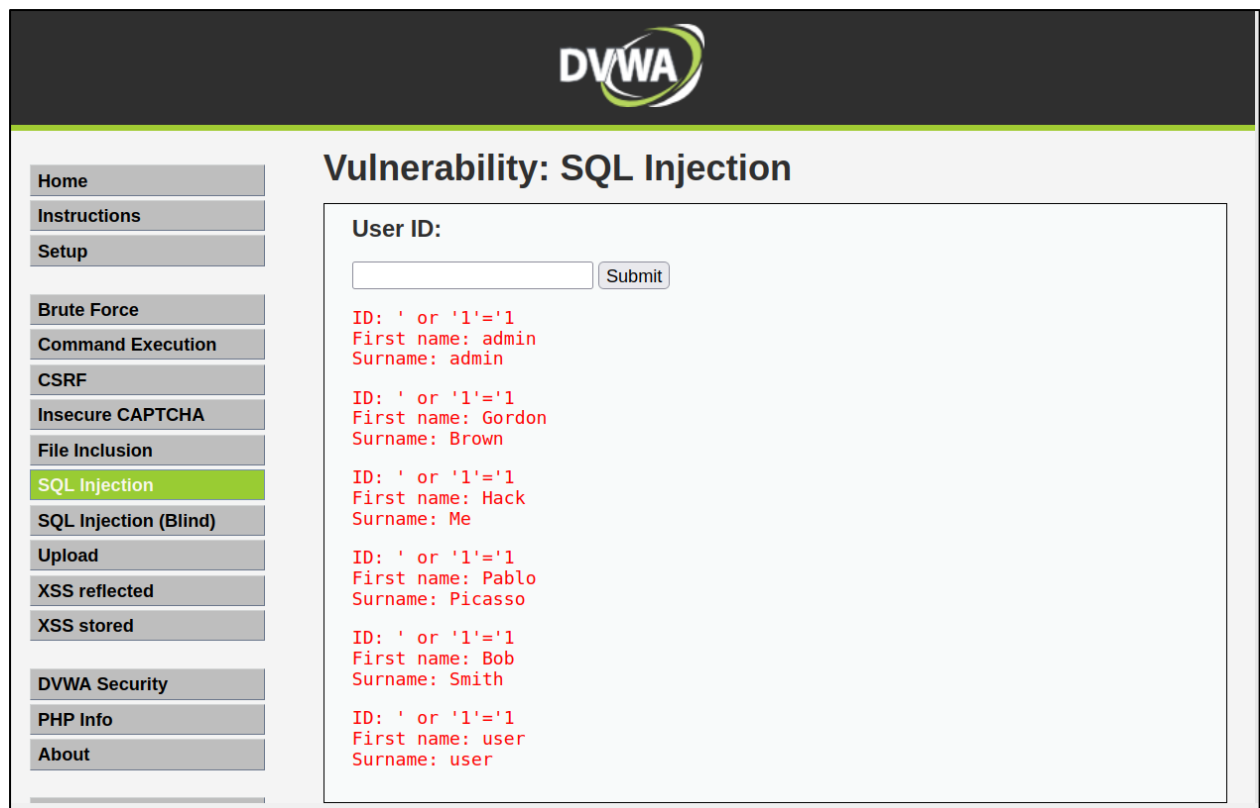


Figure 18-SQL injection output

The attacker can filter credentials via a SQL injection, as was demonstrated previously. Then, he or she can decrypt the encrypted passwords using a number of programs and tools.

The transportation business must make sure the GPS monitoring system is safe and that the necessary security measures are put in place to stop illegal access and data breaches. As described in the scenario, doing a vulnerability assessment is a crucial first step in identifying and reducing any security concerns related to the GPS monitoring system.

2) The confidentiality principle of computer security is broken by the SQL injection vulnerability. The confidentiality tenet makes sure that the information in the particular entity is kept secret and that only people with permission can access it.

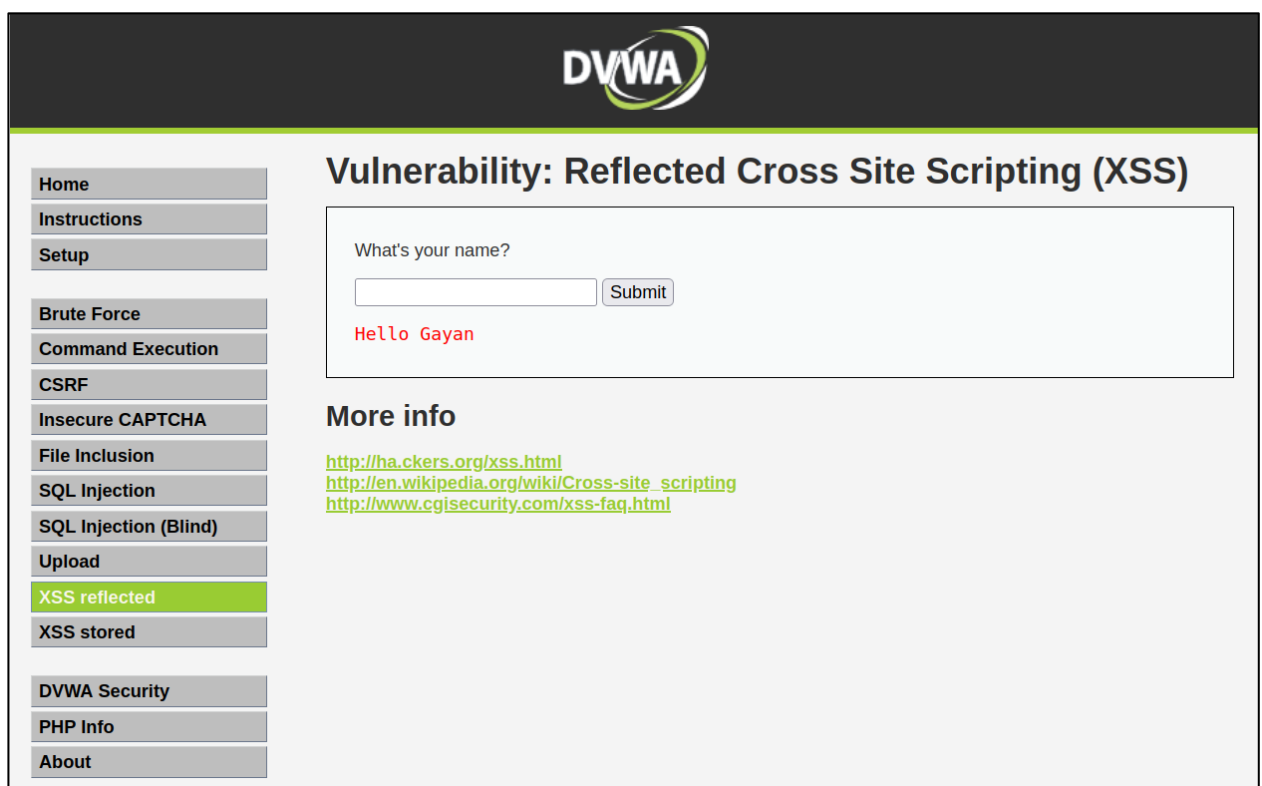
3) In the outlined scenario, intruders who take over the GPS tracking system and related databases can access private data including delivery schedules, driver information, car whereabouts, and staff login credentials. This puts the transportation industry at great danger. Attackers may use this information to gain illegal access, commit theft, intercept shipments, commit identity theft, engage in social engineering assaults, or even cause bodily harm to drivers or cars. The goals and skills of the attackers, who may be rivals, criminals, hacktivists, or data brokers, determine the hazard level. Any breach in the GPS monitoring



system poses a threat to operational continuity, financial losses, legal repercussions, and reputational harm given the company's emphasis on vehicle and driver safety.

### 3 XSS Scripting

- 1) In an injection attack known as cross-site scripting (XSS), a threat actor inserts data, such a malicious script, into material from reputable websites. The malicious code is subsequently supplied to a victim's browser along with dynamic content.(What is Cross-Site Scripting (XSS)? How to Prevent and Fix It, no date)



**DVWA**

**Vulnerability: Reflected Cross Site Scripting (XSS)**

What's your name?

Hello Gayan

**More info**

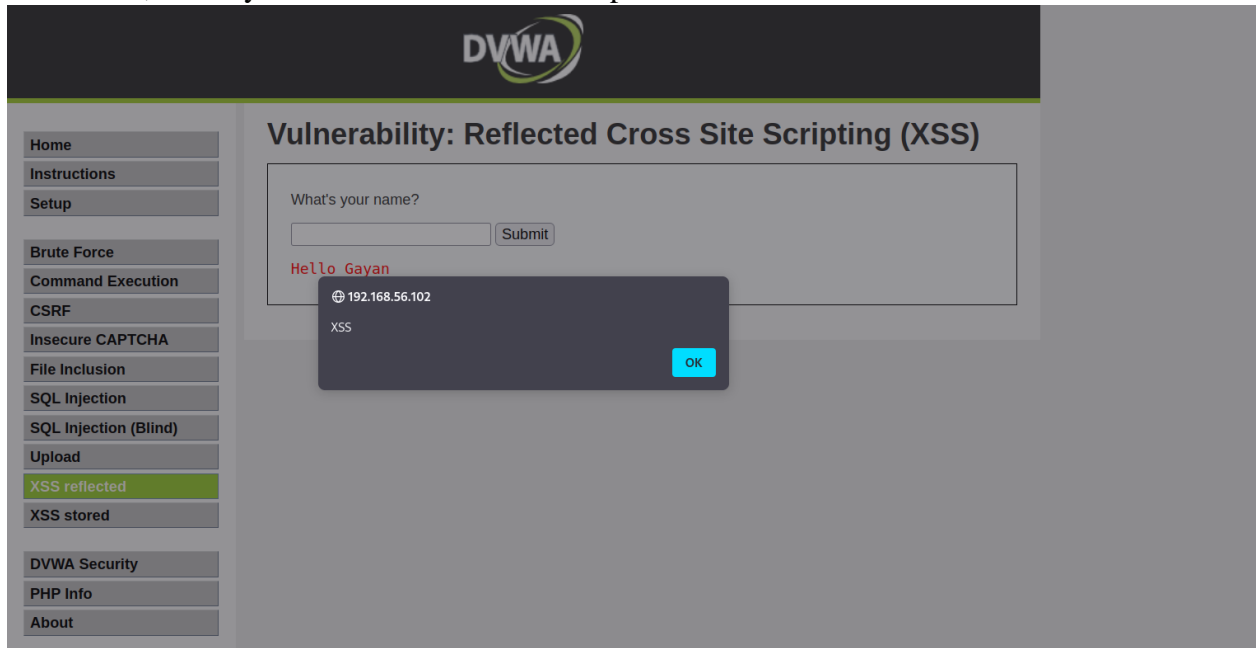
<http://hackers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

Home  
Instructions  
Setup  
Brute Force  
Command Execution  
CSRF  
Insecure CAPTCHA  
File Inclusion  
SQL Injection  
SQL Injection (Blind)  
Upload  
**XSS reflected**  
XSS stored  
DVWA Security  
PHP Info  
About

Figure 19-XSS Output

A script was fed into the form to obtain the response in order to demonstrate how the website may be exploited using a script. `alert('XSS');` is a script. The script mentioned above will trigger an alert box with the message "XSS." When the script was run in the browser, the alert box that displayed the message appeared as expected.

As a result, we may conclude that the form is open to XSS assaults.



*Figure 20-XSS successful message*

2) The confidentiality and integrity principles of cybersecurity are broken by XSS vulnerabilities. Because the attacker has access to private information that is intended to be kept confidential, confidentiality is broken. Integrity is compromised because the attacker can alter the web page's content to dupe the victim into taking activities they did not intend to.

To avoid XSS vulnerabilities, web application developers must include the proper security safeguards, such as input validation and output encoding. By updating their operating systems, web browsers, and security plugins that can identify and stop dangerous malware, web users may safeguard themselves online.

3) Sensitive information including vehicle positions, driver names, and delivery schedules may become public if a GPS tracking system is breached or has illegal access. Attackers may use this information for a range of nefarious activities, such as concentrating attacks on specific vehicles or drivers, theft, sabotage, or espionage. They can alter delivery timetables or vehicle routing to impede business operations. Hackers may obtain illegal access to the system, change data, or disable GPS tracking devices if employee login information is stolen, which might result in large financial losses. These possible risks pose a threat to the company's operations, reputation, and financial stability. Implementing security measures like access controls, encryption, recurring security audits, and employee education is essential to safeguarding the system.

## 4 OWASP vulnerable machine contains several other vulnerabilities that can be exploited

The screenshot shows the 'Vulnerability: Command Execution' page in DVWA. The left sidebar contains navigation links: Home, Instructions, Setup, Brute Force, Command Execution (highlighted), CSRF, Insecure CAPTCHA, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, and About. The main content area has a title 'Vulnerability: Command Execution' and a section 'Ping for FREE'. Below this is a form with the text 'Enter an IP address below:' and a 'submit' button. The output of the ping command is displayed in red text: 'PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data. From 192.168.56.102 icmp\_seq=1 Destination Host Unreachable. From 192.168.56.102 icmp\_seq=2 Destination Host Unreachable. From 192.168.56.102 icmp\_seq=3 Destination Host Unreachable. --- 192.168.56.101 ping statistics --- 3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2015ms, pipe 3. Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686 GNU/Linux'. Below the output is a 'More info' section with three links: <http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>, <http://www.ss64.com/bash/>, and <http://www.ss64.com/nt/>.

Figure 21-Owasp command execution

The screenshot shows the 'Vulnerability: Command Execution' page in DVWA. The left sidebar is identical to the previous screenshot. The main content area has a title 'Vulnerability: Command Execution' and a section 'Ping for FREE'. Below this is a form with the text 'Enter an IP address below:' and a 'submit' button. The output of the command is displayed in red text: 'uid=33(www-data) gid=33(www-data) groups=33(www-data) 20:54:28 up 39 min, 0 users, load average: 0.00, 0.00, 0.07 USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT'. Below the output is a 'More info' section with three links: <http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>, <http://www.ss64.com/bash/>, and <http://www.ss64.com/nt/>.

Figure 22-Owasp Output

1) In this example, a ping is sent to the IP address of a Kali Linux computer using the DVWA's Ping for FREE form. The result indicates that the server is utilizing an OS command to carry out the ping, which shows that OS instructions may be injected.

A straightforward script that executes the "uname -a" command and obtains the system information is injected into the input field to test this vulnerability. The presence of the

Command Injection vulnerability is confirmed by the output of the command being shown immediately after the output of the ping.

Attackers may use this flaw to run arbitrary commands on the target system with the same rights as the vulnerable application, which might result in system compromise, data theft, or other nefarious activities. In order to protect online applications from Command Injection vulnerabilities, it is crucial to adopt safe coding techniques like input validation and sanitization.

2) Several possible risks and weaknesses that the GPS tracking system may have include:

A GPS monitoring system's flaws pose serious threats to the security of your data. Password guessing or brute force attacks provide chances for unauthorized access when authentication methods are weak or passwords are easily guessed. Sensitive data is exposed to extraction or alteration if the database is not adequately protected against SQL Injection. Employee system access abuse can also result in breaches or illegal entrance. Without adequate access restrictions, unauthorized people might access critical information or take over the tracking system. The system is vulnerable to data breaches due to inadequate security measures, which provide hackers access to sensitive data they can use for bad intentions. To reduce these threats and safeguard sensitive information, it is essential to secure the GPS monitoring system with strong security measures.

These flaws undermine the principles of confidentiality, integrity, availability, and accountability in cyber security. The confidentiality and integrity precepts are violated by weak authentication methods and SQL injection attacks, while the accountability and availability tenets are violated by insider threats and unauthorized access. Data breaches are a violation of all four tenets since they jeopardize the confidentiality, integrity, and accessibility of the data. They may also have an effect on accountability if it is determined that the firm was careless in maintaining the data's security.

## Part C -Client-side exploits

### 1) Man in the Middle Attack (MiTM)

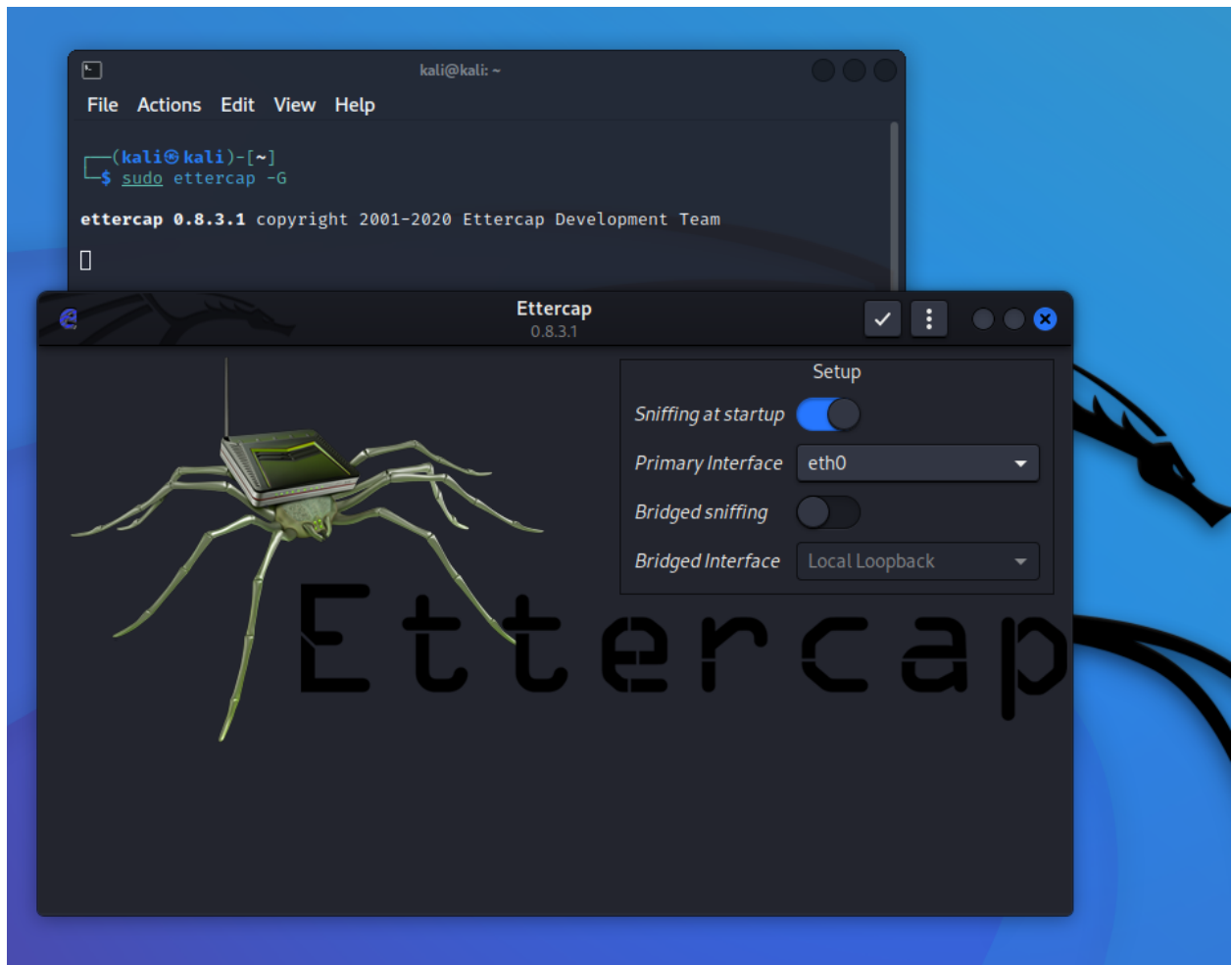


Figure 23-Ettercap host list adding

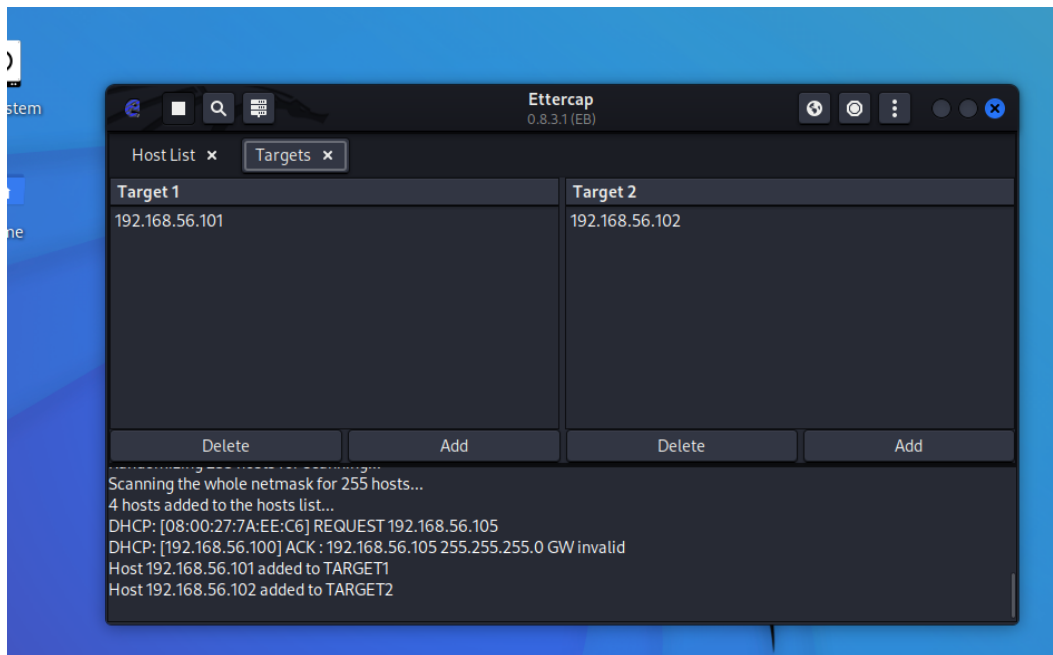


Figure 24-Adding target IP addresses

To show the APR poisoning the server machines IP address(192.168.56.102) and the client's machine's IP address(192.168.56.101) will be attacked with the attacker using Kali Linux.

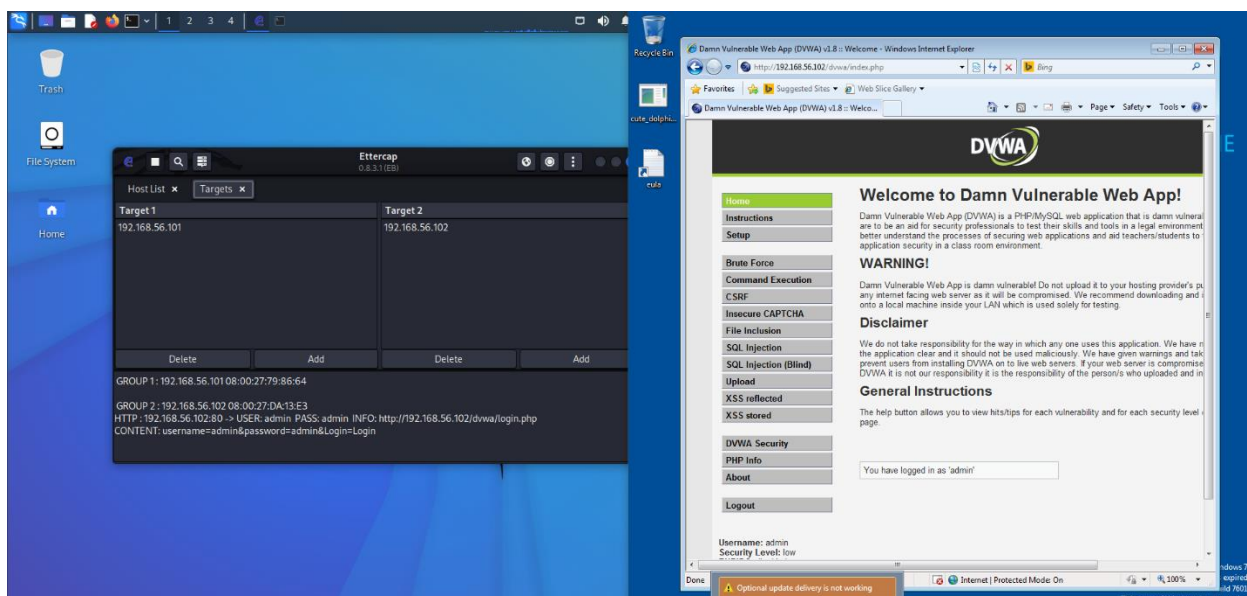


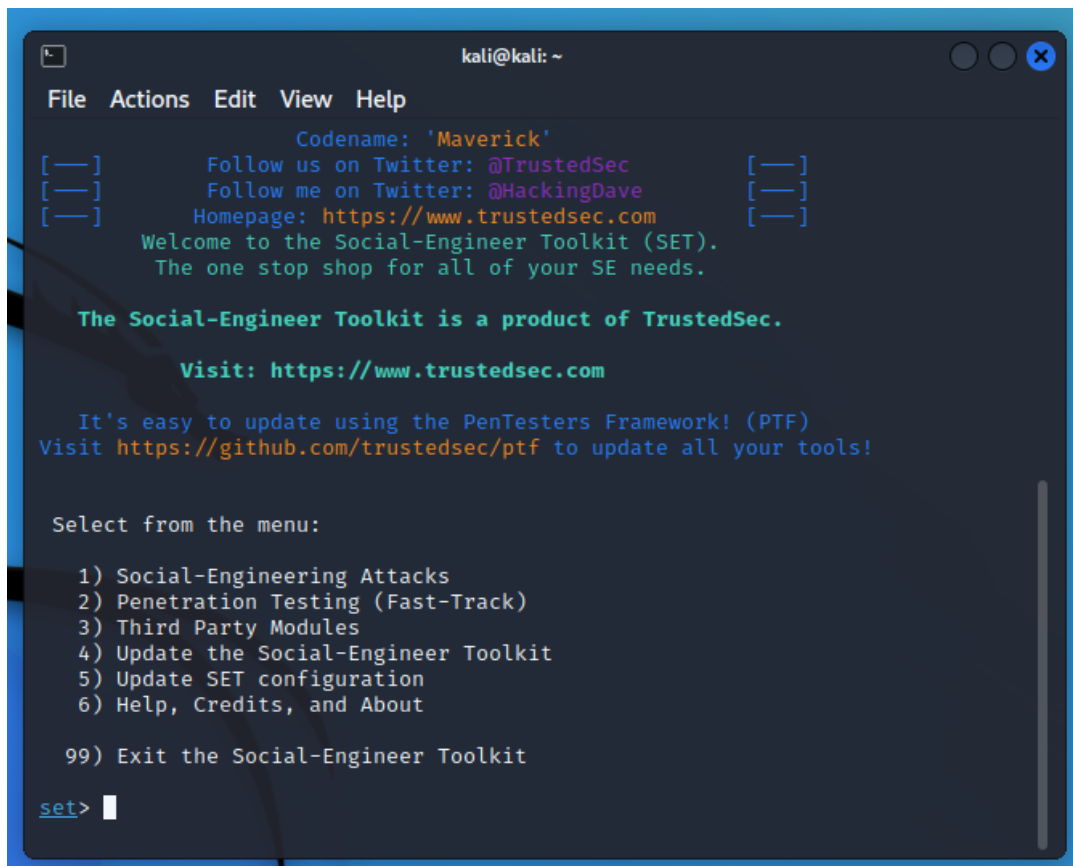
Figure 25-Verification of Ettercap filter

When a user enters sensitive data, such a username and password, Ettercap can tell. Gaining access to credentials like a login and password won't be sufficient for an attacker to conduct a penetration test.

2) A successful vulnerability assessment on the transportation company's GPS tracking system might provide an attacker access to private data including vehicle positions, driver identities, and delivery timetables. It is possible to plot and carry out physical assaults on the fleet or the drivers using this information, steal the cargo, pose as a driver, or sell the data to third parties for profit.

Additionally, attackers may gain unauthorized access to the GPS tracking system and potentially manipulate or disrupt the system if staff login credentials are compromised during the vulnerability assessment. This could result in serious operational disruptions and financial losses for the transportation company. Additionally, if the company's architecture includes other systems or networks that are connected to the GPS tracking system, an attacker may be able to change directions and get access to additional systems or networks that contain sensitive information, thus expanding the effect of the attack. A good vulnerability assessment can pose a number of dangers that could have a substantial impact on the transportation firm, its employees, and its clients.

## 2 Social engineering attack



```
kali@kali: ~
File Actions Edit View Help
Codename: 'Maverick'
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 
```

Figure 26-SEToolkit interface



Figure 27-Peruggia Login page

The above-mentioned screen photos serve as an illustration of a social engineering attack made with the sudo setoolkit. The Apache server should be operational in order to conduct the aforementioned command. Social engineering assaults, website attack vectors, credential harvester attack strategies, and Site-clone have all been chosen. The first image above illustrates how to choose those alternatives. The URL for the Perugia login form that was originally provided to the terminal to clone the site is included in the second snapshot.

2) The repercussions can be dire if a hacker is successful in finding holes in a GPS monitoring device. By gaining access to real-time location information, they can alter or take advantage of the fleet's movements for illegal ends. Additionally, the hacker has access to priceless delivery timetables, which helps them plan and carry out their illicit acts with accuracy. Additionally, if the employee login database is breached, they can get usernames and passwords, giving them access to not just the GPS tracking system but also potentially other company systems. To avoid these negative effects, it is crucial to protect GPS monitoring systems and prioritize their security.



This kind of information can be extremely risky for the business since they may lead to monetary loss, reputational harm, and legal penalties. Attackers may utilize this data for a variety of nefarious activities, including theft, fraud, or cyberespionage. Furthermore, if hackers are able to access the GPS monitoring system, they may be able to take control of the vehicles and cause accidents or interfere with business activities. Therefore, it is imperative that the business take the required steps to safeguard their GPS monitoring system and guard against illegal access to important information.

## Part D - Denial of Service attacks

### 1 DoS the web server

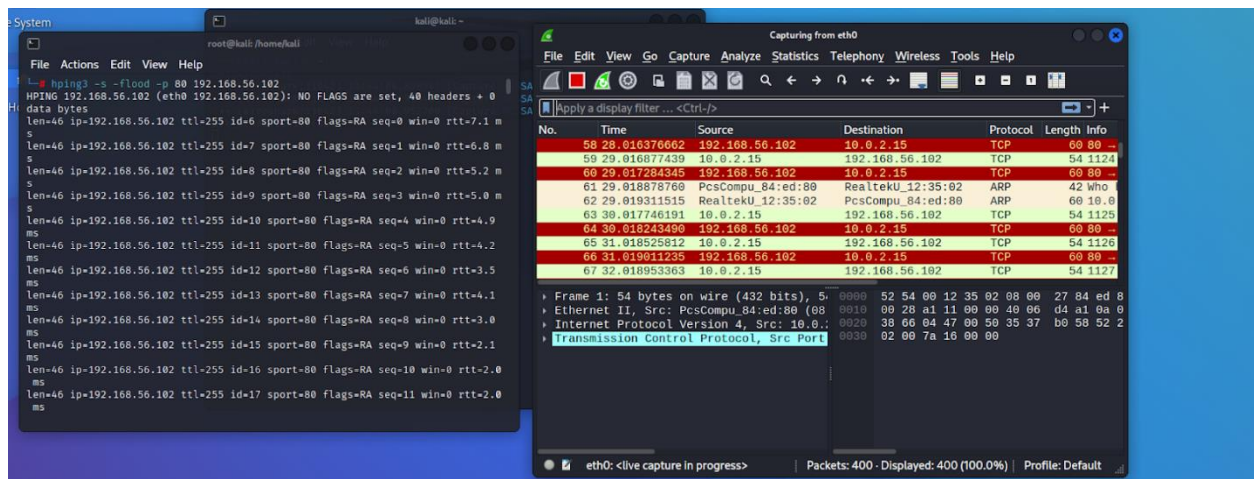


Figure 28-Wireshark ping Output

Increasing traffic keeps the server busy, which prevents it from accessing the online application. When the following code "hping3 -s -flood -p 80 192.168.56.102" is entered into the terminal, Wireshark detects excessive traffic. The code execution and high server traffic are shown in the following picture.

Since the server is receiving packets continually during this form of attack, the victim's workstation is unable to access any applications.

2) The availability tenet states that the data is accessible to authorized users at any time. A system needs working computer systems, security measures, and communication routes in

order to show availability. Extreme requirements in terms of availability are frequently present for systems classified as critical (power generation, medical equipment, safety systems). These systems must be resistant to cyberattacks and contain protections against hardware malfunctions, power outages, and other occurrences that can reduce system availability. (The three-pillar approach to cyber security: Data and information protection, no date)

As a result, the availability tenet is the primary cyber security principle that has been broken.

**3).** An attack on the transportation company's GPS monitoring system might have a big impact and lead to a variety of outcomes. Here are a few possible effects:

**Unauthorized access to sensitive data:** In the event of a system breach, attackers may have access to sensitive data kept in the database, such as the whereabouts of the vehicles, the identities of the drivers, and the delivery schedules. The privacy and security of the business and its clients may be jeopardized if this results in the disclosure of sensitive business information.

**Fleet operations might be compromised** if an attacker gained access to the GPS tracking system without authorization. They could then alter or obstruct the tracking and observation of vehicles. Fleet operations may be disrupted as a result, which might have an impact on delivery timetables, driver assignments, and general effectiveness. The business might experience delays, financial setbacks, and reputational damage as a result. **Identity theft and fraud:** If login credentials are stolen, attackers could pretend to be employees and commit fraud. They could change delivery schedules, tamper with driver assignments, or even utilize stolen identities for other nefarious ends. This might lead to monetary losses, legal troubles, and reputational harm for the business.

Legal repercussions and regulatory fines may be imposed on the firm for inadequately protecting sensitive information, depending on the specifics of the data breach and applicable industry standards. To protect oneself from legal ramifications, one must abide by data protection rules as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR).

## **Part E - Recommendations to protect the scenario company server**

1. To enhance the security of the transportation business's GPS tracking system, several measures should be implemented. Firstly, access controls should be properly implemented to restrict unauthorized access to sensitive information. This involves securing directories and files, enforcing strong passwords, and utilizing multi-factor authentication where possible. Additionally, secure communication protocols like HTTPS should be employed to encrypt data transmission and prevent eavesdropping. Disabling directory listings on the web server further mitigates information leakage. Regularly updating and patching software is essential to address known vulnerabilities. Lastly, implementing a web application firewall (WAF) aids in detecting and blocking malicious traffic, including reconnaissance attempts, thereby reducing the effectiveness of reconnaissance-based attacks. By implementing these measures, the transportation business can enhance the security and privacy of their GPS tracking technology.

(How to Protect Against Increased Reconnaissance | Fortinet Blog, no date)

2. Port knocking is an authentication technique to validate a user and open a TCP/IP port to incoming packets. A port knocking sequence consists of a specific number of closed port connection attempts to particular IP addresses. When the correct series of port “knocks” is received, the firewall opens the specific port(s) to the incoming connection request. In addition, port knocking processes commonly also determine if the requesting IP address is on an approved list. One significant benefit of port knocking is that to a hacker scanning a firewall, the service on the port will simply appear not to be available.(Port Knocking | Bugcrowd, no date)

3. It is advised to apply the least privilege principle and grant the bare minimum of access to the database user accounts that the application uses in order to increase the security of the GPS tracking system used by the transportation industry. As a result, possible SQL injection attacks are less damaging since access to particular columns and functions is restricted. Furthermore, it is essential to secure the database settings by turning on firewalls, encrypting vital information, and turning off extraneous functions. To successfully discover and fix SQL injection vulnerabilities, routine security testing should be carried out, including penetration testing and vulnerability assessments.(How to Protect Against SQL Injection Attacks | Information Security Office, no date)

**4.** To ensure robust input sanitization, implement a mechanism that removes or encodes characters that can be exploited for script injection, such as HTML tags and JavaScript event handlers. This sanitization should be performed both on the client-side and server-side to provide multiple layers of protection.

Additionally, implement context-specific output encoding to prevent script injection in different contexts where user-generated content is displayed. Apply appropriate encoding techniques for HTML, CSS, JavaScript, and URLs, depending on the context. Utilize libraries or frameworks that offer context-aware encoding functions to simplify this process and ensure accurate and secure output rendering.

(What is Cross Site Scripting? How to Protect against XSS Attacks, no date)

**5.** Implementing Encryption: Enable encryption for sensitive data transmission. This can be achieved through protocols like SSL/TLS, which encrypt the communication between the client and the server. Encryption ensures that data exchanged during the communication remains confidential and protected from interception by potential attackers.

**6.** Implement comprehensive employee training programs to raise awareness about social engineering attacks like phishing, pretexting, and baiting. Teach employees to recognize warning signs, verify requests, and safeguard sensitive information. Additionally, implement multi-factor authentication (MFA) to add an extra layer of security by requiring additional verification factors in addition to passwords. MFA reduces the risk of unauthorized access even if passwords are compromised.(8 Ways Organisations Prevent Social Engineering Attacks, no date)

**7.** Traffic Monitoring and Anomaly Detection: Implement real-time traffic monitoring systems that can detect abnormal patterns and behavior indicative of a DoS attack. By analyzing network traffic and application metrics, companies can identify sudden spikes in traffic, unusual request patterns, or excessive resource consumption, and respond promptly.(DoS Attack | What Is A Denial-of-Service Attack (DoS) | Mimecast, no date)

## 8. Intrusion Detection and Prevention systems

First, we must confirm that the server's firewall is turned on; if not, we must do so. To determine if the firewall is active or not, run the command "ufw status numbered" in this

```
root@owaspbwa:~# ufw delete 1
Deleting:
  allow 80/tcp
Proceed with operation (y/n)? y
Rule deleted
root@owaspbwa:~# ufw status numbered
Status: active
root@owaspbwa:~# ufw deny 80/tcp
Rule added
root@owaspbwa:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:30:ea:c3
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe30:eac3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:55 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4704 (4.7 KB)  TX bytes:9002 (9.0 KB)
          Interrupt:9 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:184 errors:0 dropped:0 overruns:0 frame:0
          TX packets:184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:39721 (39.7 KB)  TX bytes:39721 (39.7 KB)

root@owaspbwa:~#
```

situation.

Figure 29-Checking Firewall status

The firewall has to be added to that particular port in order to protect the web application. This will be accomplished by using the command line "ufw allow 80/tcp".

```
root@owaspbwa:~# ufw status
Status: active

To Action From
--
80/tcp DENY Anywhere

root@owaspbwa:~# ufw allow 80/tcp
Rule updated
```

Figure 30-adding firewall to port

I used several command lines to generate network traffic to demonstrate that the iptables rules were in operation, but the network traffic was refused on the port, preventing the attacker from sending unauthorized traffic to the server.

```
root@owaspbwa:~# sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@owaspbwa:~# sudo iptables -A INPUT -s 192.168.56.102 -p tcp --destination -
port 80 -j DROP
```

*Figure 31-sending traffic to port*

The comparison between Iptables and Firewalls (ufw) is shown here.

Iptables	Firewalls(ufw)
It is brand-new and compatible with contemporary technology.	unable to work with the majority of modern technology.
Mechanism for kernel-level IP filtering	It is based on Iptables.
Simple to construct	modify Actions are constrained

#### Comparison of IDS and Ips

IDS	IPS
Tools for detection and observation	regulating system
unable to act alone	The ruleset is available for use by the system.
present should be someone present to observe the procedure.	doesn't require anyone

Put in place a thorough access control and authentication mechanism to safeguard critical information and stop unwanted access. It also incorporates user training, role-based access control, routine password changes, user authentication mechanisms, and monitoring tools. These steps will strengthen the GPS tracking system's security and eliminate any weaknesses that could exist.

## Reference

- 8 Ways Organisations Prevent Social Engineering Attacks. (no date). Available from <https://www.stickmancyber.com/cybersecurity-blog/8-ways-organisations-prevent-social-engineering-attacks> [Accessed 14 May 2023].
- Breda, F., Barbosa, H. and Morais, T. (2017). SOCIAL ENGINEERING AND CYBER SECURITY. *INTED2017 Proceedings*, 1, 4204–4211. Available from <https://doi.org/10.21125/INTED.2017.1008> [Accessed 10 May 2023].
- Conti, M., Dragoni, N. and Lesyk, V. (2016). A Survey of Man in the Middle Attacks. *IEEE Communications Surveys and Tutorials*, 18 (3), 2027–2051. Available from <https://doi.org/10.1109/COMST.2016.2548426> [Accessed 10 May 2023].
- Dokman, T. and Ivanjko, T. (2020). Open Source Intelligence (OSINT): issues and trends. *INFuture2019: Knowledge in the Digital Age*. Available from <https://doi.org/10.17234/INFUTURE.2019.23> [Accessed 10 May 2023].
- DoS Attack | What Is A Denial-of-Service Attack (DoS) | Mimecast. (no date). Available from <https://www.mimecast.com/blog/what-is-dos-attack-and-how-to-prevent-it/> [Accessed 14 May 2023].
- How to Protect Against Increased Reconnaissance | Fortinet Blog. (no date). Available from <https://www.fortinet.com/blog/industry-trends/be-prepared-for-the-increase-in-reconnaissance> [Accessed 14 May 2023].
- How to Protect Against SQL Injection Attacks | Information Security Office. (no date). Available from <https://security.berkeley.edu/education-awareness/how-protect-against-sql-injection-attacks> [Accessed 14 May 2023].
- Javeed, D. and MohammedBadamasi, U. (2020). Man in the Middle Attacks: Analysis, Motivation and Prevention. *International Journal of Computer Networks and Communications Security*, 8 (7), 52–58. Available from [https://doi.org/10.47277/IJCNCs/8\(7\)1](https://doi.org/10.47277/IJCNCs/8(7)1) [Accessed 10 May 2023].
- Mahmoud, S.K. et al. (2017). A comparative analysis of Cross Site Scripting (XSS) detecting and defensive techniques. *2017 IEEE 8th International Conference on Intelligent Computing and Information Systems, ICICIS 2017*, 2018-January, 36–42. Available from <https://doi.org/10.1109/INTELCIS.2017.8260024> [Accessed 10 May 2023].

Port Knocking | Bugcrowd. (no date). Available from <https://www.bugcrowd.com/glossary/port-knocking/> [Accessed 14 May 2023].

The three-pillar approach to cyber security: Data and information protection. (no date). Available from <https://www.dnv.com/article/the-three-pillar-approach-to-cyber-security-data-and-information-protection-165683> [Accessed 14 May 2023].

Weamie, S.J.Y. and Weamie, S.J.Y. (2022). Cross-Site Scripting Attacks and Defensive Techniques: A Comprehensive Survey\*. *International Journal of Communications, Network and System Sciences*, 15 (8), 126–148. Available from <https://doi.org/10.4236/IJCNS.2022.158010> [Accessed 10 May 2023].

Web Parameter Tampering | OWASP Foundation. (no date). Available from [https://owasp.org/www-community/attacks/Web\\_Parameter\\_Tampering](https://owasp.org/www-community/attacks/Web_Parameter_Tampering) [Accessed 14 May 2023].

What is Cross Site Scripting? How to Protect against XSS Attacks. (no date). Available from <https://www.freecodecamp.org/news/cross-site-scripting-what-is-xss/> [Accessed 14 May 2023].

What is Cross-Site Scripting (XSS)? How to Prevent and Fix It. (no date). Available from <https://www.techtarget.com/searchsecurity/definition/cross-site-scripting> [Accessed 14 May 2023].

Xue, P.C. (2011). SQL injection attack and guard technical research. *Procedia Engineering*, 15, 4131–4135. Available from <https://doi.org/10.1016/J.PROENG.2011.08.775> [Accessed 10 May 2023].