



INFORMATICS INSTITUTE OF TECHNOLOGY

INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

Module: Cybersecurity

Module Code: 6COSC019C

Coursework – Scenario Based Lab Report

Date of Submission: 09th May 2023

Student name	Tharindu De Silva
Student ID	2018367
UoW ID	W1761890

Contents

Scenario	1
Penetration Testing Findings	1
A – Information Gathering	1
(1) OSINT Activities	1
Question 1 – Examples of OSINT Investigations	1
Question 2 - Effectiveness of open-source intelligence data.	5
Question 3 - Risk on gathered data.	6
(2) Reconnaissance	6
Question 1 - Discovered Hidden Directories.	6
Question 2 – Risk on gathered Data	7
(3) Port Scanning and Enumeration	8
Question 1 – Identified Ports	8
Question 2 – Research on Open Ports	9
Question 3 – Threats on the Identified Open Ports	9
B – Server-Side Exploits	10
(1) Data tampering	10
Question 1 – Identifying the Vulnerabilities for Data Tampering.	10
Question 2 – Research on Data Tampering Vulnerability	11
Question 3 – Risk on Gathered Data	11
(2) SQL Injection	12
Question 1 – Identifying Vulnerabilities for SQL Injection	12
Question 2 – Research on SQL Injections	12
Question 3 – Risk on Gathered Data	12
(3) XSS Scripting	13
Question 1 – Identifying Vulnerabilities for Cross Site (XSS) Scripting	13
Question 2 – Explanation on Cross Site Scripting	14
Question 3 – Risk on Gathered Data	14
(4) Other vulnerabilities on OWASP machine	15
C – Client-Side Exploits	16
(1) Man in the Middle Attack (MiTM)	16
Question 1 – Setting up tools for MiTM	16
Question 2 – Risk on Gathered Data	18
(2) Social Engineering Attack	18
Question 1 – Setting up tools for social engineering attack	18

Question 2 – Risk on Gathered Data	21
D – Denial of Service Attacks	22
(1) DoS the Web Server	22
E – Recommendation to protect the scenario company server	22
(1) Reducing Threats from Reconnaissance	22
(2) Port Knocking	23
(3) SQL Injection	23
(4) Cross Site (XSS) Scripting	23
(5) Man in the Middle Attacks	23
(6) Social Engineering Attacks	24
(7) DoS Attacks	24
(8) Intrusion Detection and Prevention Systems	24
Examples of UFW and Iptables	24
Effectiveness of Iptables and Firewall	25
Difference between Intrusion Detection System IDS and IPS	26
Suggestions and Recommendation	26
References	27

Scenario

I was hired as a penetration tester for a **medium-sized car dealership company**. Their web application enables **vendors (sellers)** to offer cars on their platform, and **customers (buyers)** to purchase them. The application stores **sensitive information** such as vehicle history accidents, repairs, and maintenance. Also included **sensitive personal information** about the seller/buyer, including contact details, name, address, phone numbers, and email addresses. It also saves login details for sellers and buyers in the database. Buyers and sellers have different privileges. There are also **admin users** that **manage the web application's functionality**, such as managing payments, managing users, and monitoring website activities. **The login credentials** of admin users are likewise saved in the same database.

Penetration Testing Findings

A – Information Gathering

(1) OSINT Activities

cwscenario.site will be the public URL of the company web application. This URL will be used to gather information using the OSINT tools.

Question 1 – Examples of OSINT Investigations

I. Maltego

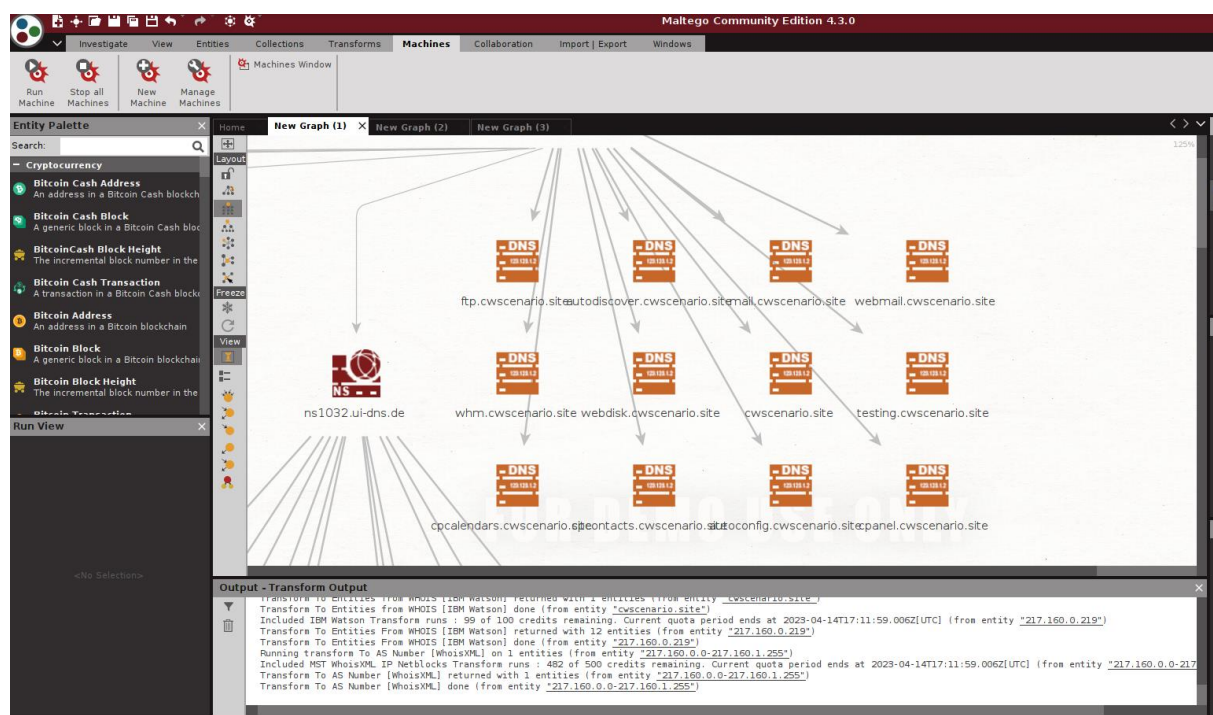


Figure 1 – Maltego results

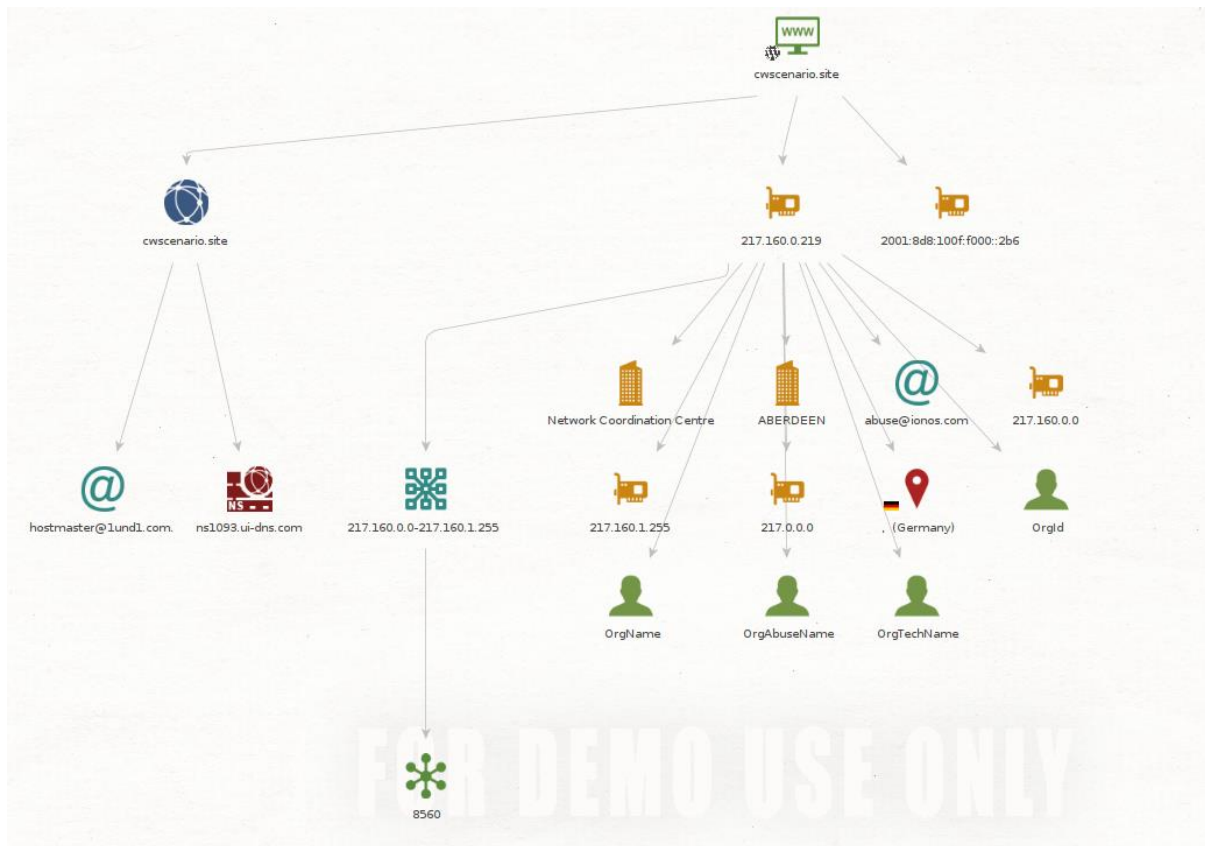


Figure 2 – Maltego email results

MX Records (2)	
mx00.ionos.co.uk	mx01.ionos.co.uk
NS Records (4)	
ns1032.ui-dns.de	ns1093.ui-dns.com
ns1108.ui-dns.org	ns1115.ui-dns.biz
Netblocks (1)	
217.160.0.0-217.160.0.255	

Figure 3 – NS records

II. SpiderFoot

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ spiderfoot -l 127.0.0.1:5001  
2023-03-15 09:57:37,638 [INFO] sf : Starting web server at 127.0.0.1:5001 ...  
  
*****  
Use SpiderFoot by starting your web browser of choice and  
browse to http://127.0.0.1:5001/  
*****  
  
2023-03-15 09:57:37,671 [WARNING] sf :  
*****  
Warning: passwd file contains no passwords. Authentication disabled.  
Please consider adding authentication to protect this instance!  
Refer to https://www.spiderfoot.net/documentation/#security.  
*****
```

Figure 4 – SpiderFoot starting in local server.

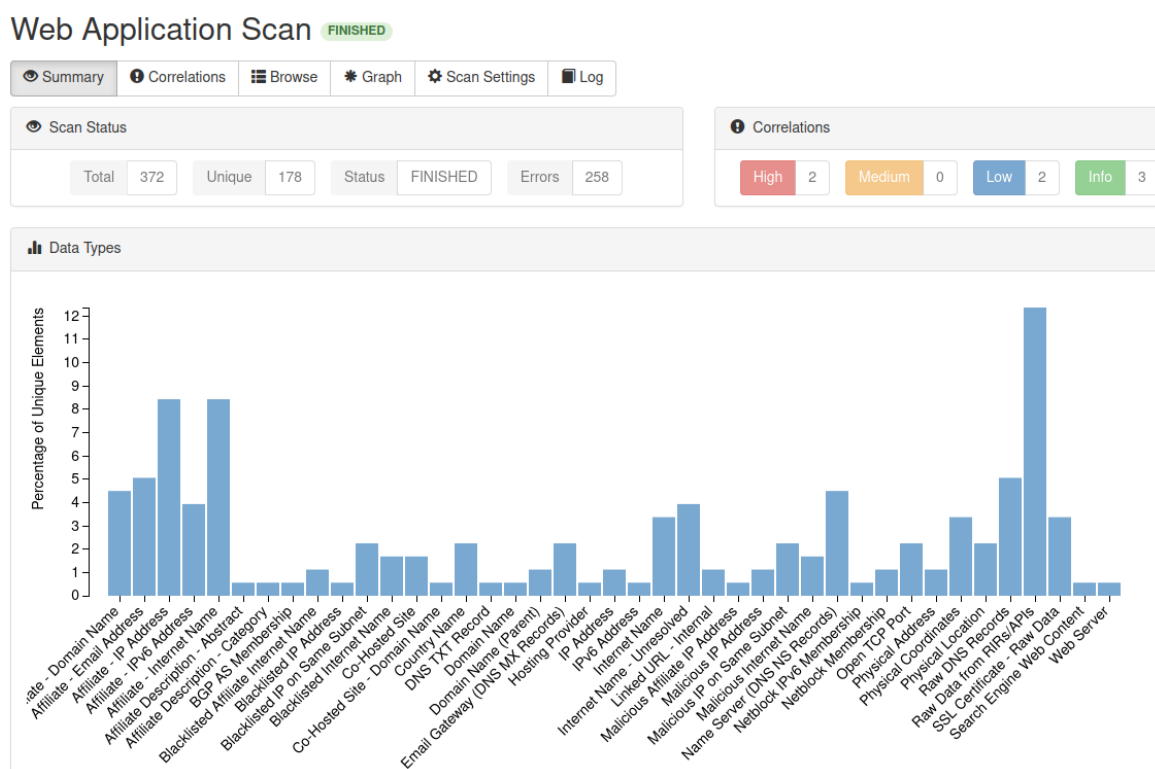


Figure 5 – SpiderFoot results graph format

Web Application Scan FINISHED

[Summary](#)
[Correlations](#)
[Browse](#)
[Graph](#)
[Scan Settings](#)
[Log](#)

[Refresh](#)
[Download](#)

[Search](#)

Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Domain Name	8	20	2023-03-15 10:10:29
Affiliate - Email Address	9	13	2023-03-15 10:05:49
Affiliate - IP Address	15	15	2023-03-15 10:10:29
Affiliate - IPv6 Address	7	7	2023-03-15 10:10:29
Affiliate - Internet Name	15	40	2023-03-15 10:11:16
Affiliate Description - Abstract	1	1	2023-03-15 10:08:35
Affiliate Description - Category	1	1	2023-03-15 10:08:35
BGP AS Membership	1	7	2023-03-15 10:04:31
Blacklisted Affiliate Internet Name	2	2	2023-03-15 10:11:02
Blacklisted IP Address	1	1	2023-03-15 10:03:08
Blacklisted IP on Same Subnet	4	4	2023-03-15 10:04:14
Blacklisted Internet Name	3	3	2023-03-15 10:09:04
Co-Hosted Site	3	11	2023-03-15 10:05:28
Co-Hosted Site - Domain Name	1	2	2023-03-15 10:04:31
Country Name	4	9	2023-03-15 10:09:59
DNS TXT Record	1	1	2023-03-15 10:00:27
Domain Name	1	9	2023-03-15 10:01:05
Domain name (-parent)	2	2	2023-03-15 10:07:44
Email Gateway (DNS MX Records)	4	6	2023-03-15 10:07:59
Hosting Provider	1	2	2023-03-15 10:03:58
IP Address	2	3	2023-03-15 10:02:07
IPv6 Address	1	3	2023-03-15 10:07:44
Internet Name	6	41	2023-03-15 10:09:28
Internet Name - Unresolved	7	79	2023-03-15 10:09:29
Linked URL - Internal	2	2	2023-03-15 10:02:01
Malicious Affiliate IP Address	1	1	2023-03-15 10:05:15
Malicious IP Address	2	2	2023-03-15 10:03:08
Malicious IP on Same Subnet	4	4	2023-03-15 10:04:14
Malicious Internet Name	3	3	2023-03-15 10:09:04
Name Server (DNS NS Records)	8	12	2023-03-15 10:07:59
Netblock IPv6 Membership	1	2	2023-03-15 10:02:51
Netblock Membership	2	4	2023-03-15 10:04:16
Open TCP Port	4	4	2023-03-15 10:04:27
Physical Address	2	3	2023-03-15 10:04:46
Physical Coordinates	6	6	2023-03-15 10:04:30
Physical Location	4	6	2023-03-15 10:04:27
Raw DNS Records	9	9	2023-03-15 10:07:59
Raw Data from RIRs/APIs	22	22	2023-03-15 10:07:55
SSL Certificate - Raw Data	6	8	2023-03-15 10:05:28
Search Engine Web Content	1	1	2023-03-15 10:08:35
Web Server	1	1	2023-03-15 10:02:01

Figure 6 – SpiderFoot results table format

iii) SIGIT

```
File Actions Edit View Help
!KKKKKKKKKKKKKK2>' '>2KKKKKKKKKKKKKK!
!KKKKKKKKKKKKKKKKZ ZKKKKKKKKKKKKKKKK!
!KKKKKKKKKKKKKKKK5 eKKKKKKKKKKKKKKKK!
!KKKKKKKKKKKKKKqC;- -;CqKKKKKKKKKKKK!
<KKKKKKKKKKkr, ,rSKKKKKKKKK<
-"v]qj;- -;jq]v"-

[ S.I.G.I.T ]
Simple Information Gathering Toolkit
Author by @Termuxhackers.id

Choose number or type exit for exiting

01 Userrecon Username reconnaissance
02 Facedumper Dump facebook information
03 Mailfinder Find email with name
04 Godorker Dorking with google search
05 Phoneinfo Phone number information
06 DNSLookup Domain name system lookup
07 Whoislookup Identify who is on domain
08 Sublookup Subnetwork lookup
09 Hostfinder Find host domain
10 DNSfinder Find host domain name system
11 RIPLookup Reverse IP lookup
12 IPlocation IP to location tracker

> choose: 6
> enter domain or IP: cwscenario.site

- A : 217.160.0.219
- AAAA : 2001:8d8:100f:f000::2b6
- MX : 10 mx00.ionos.co.uk.
- MX : 10 mx01.ionos.co.uk.
- NS : ns1093.ui-dns.com.
- NS : ns1108.ui-dns.org.
- NS : ns1032.ui-dns.de.
- NS : ns1115.ui-dns.biz.
- TXT : "Well done for finding this. However I am afraid you wont get an extra ma
rk :)"
- SOA : ns1093.ui-dns.com. hostmaster.lund1.com. 2017060103 28800 7200 604800 600

press enter for back to previous menu
```

Figure 7 - SIGIT DNS Lookup

Question 2 - Effectiveness of open-source intelligence data.

Gathering publicly available data through the OSINT tools allows the tester to identify potential threats for the target system with the use of social media profiles, email addresses, phone numbers and other personal information. These data can be used mainly for social engineering attacks by targeting the application users. OSINT is considered as a low-cost approach for gathering information and identifying vulnerabilities on the targeted system. This can be conducted as the first activities by the penetration tester which will help to gain a better understanding of the target system by identifying potential vulnerabilities with publicly available data (Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT) - ScienceDirect, 2012).

Question 3 - Risk on gathered data.

With analysis of the gathered data through the OSINT tools some email addresses, outdated http ports and information related to email gateway were gathered. The risk of exposing email addresses can be considered as a potential threat. These email addresses can be targeted by the attacker for phishing. In the context of the company attackers may try to trick the application user into revealing sensitive information related to both personal and vehicle information. Another approach is to redirect the buyer to a fraudulent website to steal credit card information or even for a fraudulent payment.

Another risk of easily gathered email gateway data which is responsible for proper email delivery. This data also can be used by an attacker for spoofing the email or sending phishing emails using the company server to the application users.

(2) Reconnaissance

Question 1 - Discovered Hidden Directories.

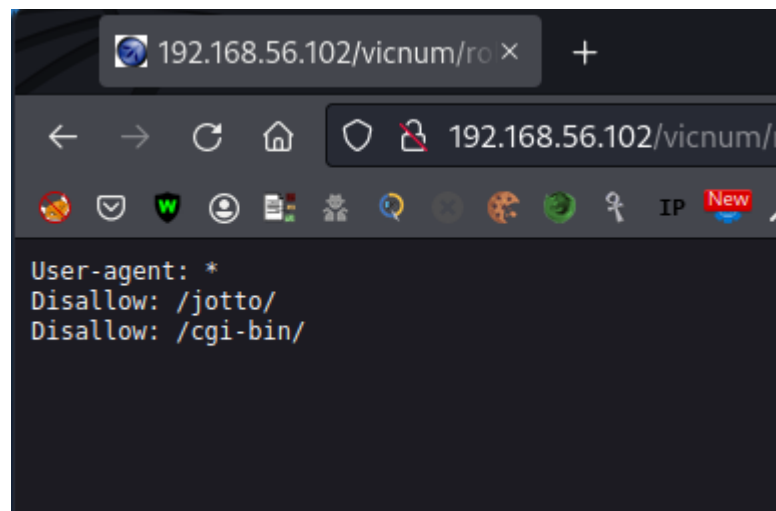


Figure 8 – Hidden directories found.

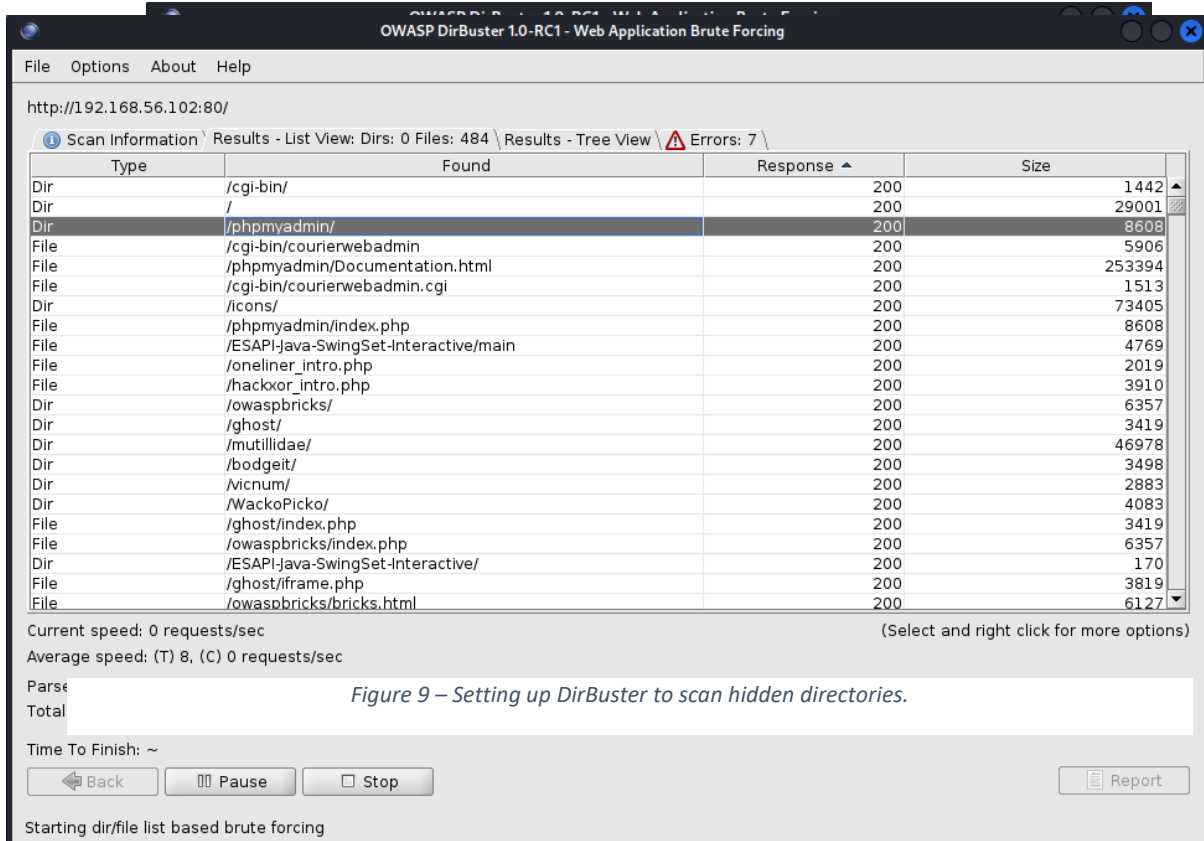


Figure 10 - Results

Question 2 – Risk on gathered Data

While the robots.txt file's main intention is to communicate with the web crawlers regarding which pages are allowed to access, it can expose the website's directory structure and may lead to potential attacks. From the above analysis finding of cgi-bin directory can lead to command execution vulnerabilities. Also, the expose of phpMyAdmin directory could expose company database which stores login credentials may allow attacker to steal data and extract sensitive data or even gain access as an admin user to edit the content of the web application.

(3) Port Scanning and Enumeration

Question 1 – Identified Ports

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ nmap 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-18 10:45 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00062s latency).
Not shown: 991 closed tcp ports (conn-refused)
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 0.21 seconds
```

Figure 11 – port scanning using nmap for open ports.

```
(kali@kali)-[~]
$ sudo nmap -sU 192.168.56.102
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-11 04:27 EST
Nmap scan report for 192.168.56.102
Host is up (0.00052s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)
MAC Address: 08:00:27:48:DE:B7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1102.68 seconds
```

Figure 12 – checking the host is up.

```

(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV -O 192.168.56.102
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-18 10:46 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00046s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4
.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 Opens
SL ...)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Courier Imapd (released 2008)
443/tcp   open  ssl/http     Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4
.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 Opens
SL ...)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp  open  java-object  Java Object Serialization
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http         Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version, please sub
mit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.92%I=7%D=3/18%Time=6415CEDA%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"\xac\xed\x05");
MAC Address: 08:00:27:48:DE:B7 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.35 seconds

```

Figure 13 – guessing the open ports operating system version.

Question 2 – Research on Open Ports

Open ports indicate when a server is actively waiting and listening for a request through a port. In a misconfigured security environments attackers may use these open ports to infect services with malicious services. Attackers can take advantage of these open ports to gain unauthorized access to targeted systems. Examples of open ports include SSH, Telnet, SMTP and FTP (Mathew, Tabassum and lu, 2014)

Question 3 – Threats on the Identified Open Ports

Port	Risk
SSH port	This port allows to access the server remotely. If an attacker performs a brute force attack on the port and gains access to the server which will result a potential security risk. The attacker will be able to gain personal information of the buyers and sellers, vehicle information and website activity data.
HTTP port	This is an outdated port and has high security risk. An attacker can use this port to perform a DOS attack for the web application which will result in users unable to access the web application. Furthermore, payments and updating of the content of the web application will be on hold till the necessary measurements are taken.
HTTP proxy port	Using the Slowloris Dos vulnerability, an attacker can send unexpected traffic to the web server, making the web-based

	application inaccessible. When using the company's website, application users might experience very poor performance.
--	---

Table 1 – Ports and Risks

B – Server-Side Exploits

(1) Data tampering

Question 1 – Identifying the Vulnerabilities for Data Tampering.

The data tampering vulnerabilities of the web application were identified using the 'OWASP Mantra' tool. Upon analysis, it was discovered that an attacker, intercepting the post request sent to the webserver during a user login, could modify the request data and retrieve confidential information. Bellow image shows the intercepted post request with

Requested initial credentials.

Username: user123

Password: pwr123

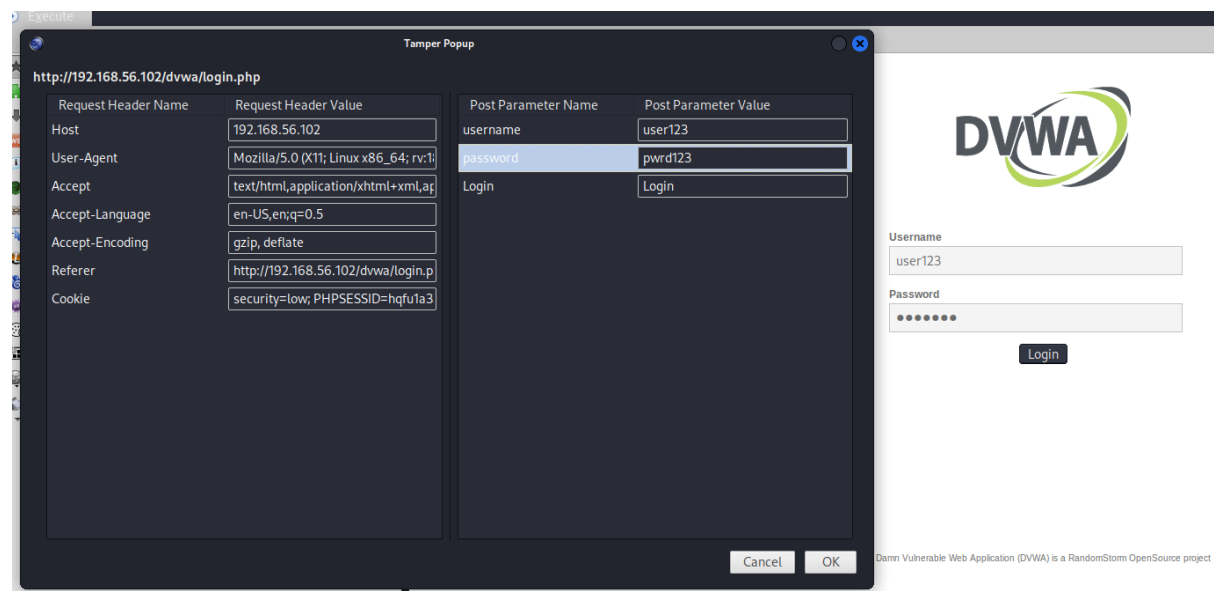


Figure 14 – Data tamper popup for modifying data.

Modifying data to

Username: admin

Password: admin

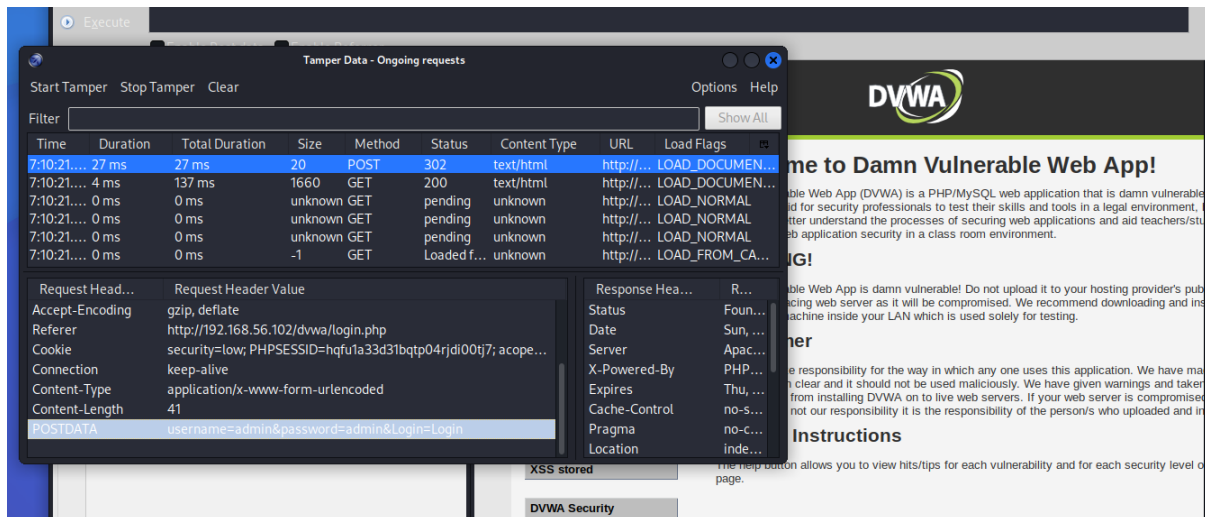


Figure 15 – Modified data

Question 2 – Research on Data Tampering Vulnerability

The Open Web Application Security Project (OWASP) states that, data tampering is a type of vulnerability that allows an attacker to modify data without authorization, which can lead to unauthorized access, data loss, or data corruption. Data tampering can occur through various means, such as interception of data in transit, injection of malicious code, or modification of data at rest (OWASP Top 10:2021, no date). Data tampering vulnerability violates the integrity tenet of cybersecurity, which ensures that data is accurate, complete, and unmodified. This tenet aims to prevent unauthorized access and changes to data and to ensure that any changes made are authorized and legitimate (Confidentiality, Integrity and Availability - The CIA Triad, 2018).

Question 3 – Risk on Gathered Data

Attackers can obtain various sensitive information, including vehicle information, vehicle history, seller/buyer information, and login credentials. They can modify or delete the vehicle's make, model, year, and mileage, leading to legal and financial issues for the company if buyers purchase vehicles with incorrect specifications. Attackers can also tamper with the vehicle history records, leading to hidden issues such as accidents or repairs, causing more legal and financial issues for the company. Additionally, attackers can obtain personal information about sellers and buyers, including their contact details, names, addresses, mobile numbers, and email addresses, and use it for fraudulent activities, damaging the company's reputation and its customers. Finally, attackers can steal login credentials, allowing them unauthorized access to the web application, resulting in data theft, manipulation, and other malicious activities that can cause significant damage to the company.

(2) SQL Injection

Question 1 – Identifying Vulnerabilities for SQL Injection

DVWA

Vulnerability: SQL Injection

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
Logout

User ID:

ID: ' or '1'=1
First name: admin
Surname: admin

ID: ' or '1'=1
First name: Gordon
Surname: Brown

ID: ' or '1'=1
First name: Hack
Surname: Me

ID: ' or '1'=1
First name: Pablo
Surname: Picasso

ID: ' or '1'=1
First name: Bob
Surname: Smith

ID: ' or '1'=1
First name: user
Surname: user

More info

Figure 16 – vulnerable to SQL injection

Question 2 – Research on SQL Injections

SQL injection is a particular type of cybersecurity vulnerability that allows an attacker to insert malicious code into a database query using input fields related to login forms, search boxes, and comments sections on online applications. By doing so, the attacker can access or modify sensitive data stored in the database, or even gain administrative privileges to the entire system (Ma et al., 2019). SQL injection violates the confidentiality, integrity, and availability (CIA) triad of cybersecurity. It primarily violates the integrity tenet since it can modify or delete data in the database without proper authorization. Additionally, it can also compromise the confidentiality of sensitive information and affect the availability of the system by disrupting its normal operations.

Question 3 – Risk on Gathered Data

Performing a SQL injection on the company site can lead to obtaining sensitive information stored in the database. This information includes vehicle information, vehicle history, seller/buyer information, and login credentials for sellers, buyers, and admin users. If attackers were able to obtain login credentials for admin users, they could gain access to the

web application's back-end systems and manipulate or steal sensitive data, such as payment information or user data. This could be devastating for the company and its customers, as it could result in significant financial and reputational damage.

(3) XSS Scripting

Question 1 – Identifying Vulnerabilities for Cross Site (XSS) Scripting

Using special characters as input to see if the website's layout is vulnerable to cross-site scripting.



Figure 17 – Vulnerable to cross site scripting

Obtaining cookie through input box using 'Test<script>alert(docuemt.cookie)</script>'

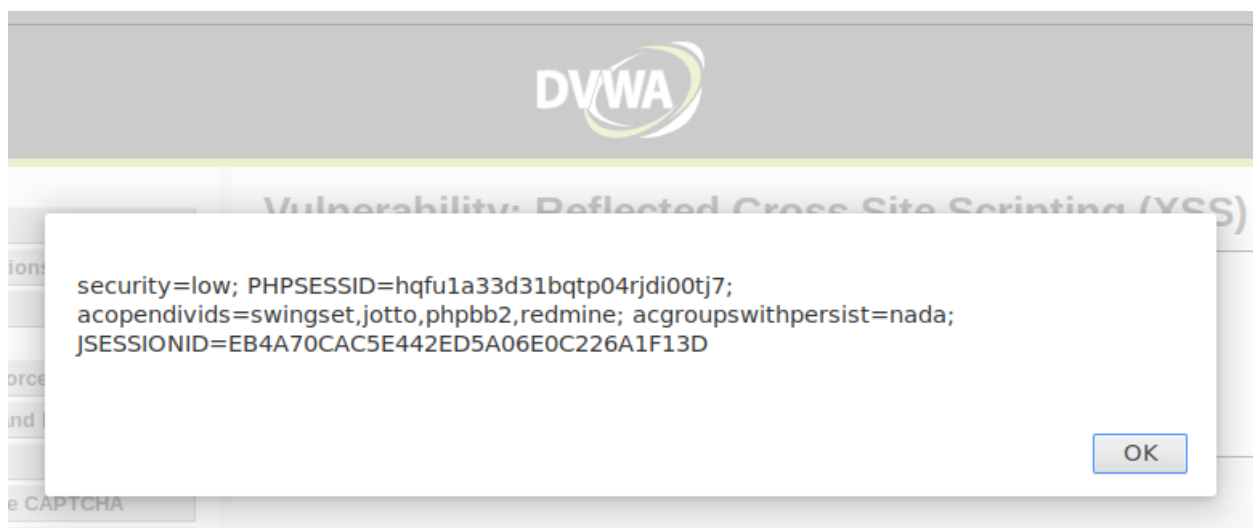


Figure 18 – Viewing the cookies using cross site scripting.

Added script can view through page source.

```

38
39 <div class="body_padded">
40   <h1>Vulnerability: Reflected Cross Site Scripting (XSS)</h1>
41
42   <div class="vulnerable_code_area">
43
44     <form name="XSS" action="#" method="GET">
45       <p>What's your name?</p>
46       <input type="text" name="name">
47       <input type="submit" value="Submit">
48     </form>
49
50     <pre>Hello Test<script>alert(document.cookie)</script></pre>
51
52   </div>
53
54   <h2>More info</h2>
55
56   <ul>
57     <li><a href="http://hiderefer.com/?http://hacker.org/xss.html" target="_b
58     <li><a href="http://hiderefer.com/?http://en.wikipedia.org/wiki/Cross-site_
59     <li><a href="http://hiderefer.com/?http://www.cgisecurity.com/xss-faq.html"
60   </ul>
61 </div>
62
63   <br />
64   <br />
65

```

Figure 19 – Modified web page source with added script

Question 2 – Explanation on Cross Site Scripting

Cross-Site Scripting (XSS) is a form of vulnerability type that occurs when attackers inject malicious code into web pages viewed by other users. This code can be used to steal data, such as login credentials or credit card numbers, or to manipulate the user's web experience. The attacker can use a variety of techniques to inject the code, including input forms, cookies, and search queries. This vulnerability violates the Confidentiality and Integrity tenets of the CIA triad (Confidentiality, Integrity and Availability - The CIA Triad, 2018). Confidentiality is violated because attackers can steal sensitive data, such as login details or credit card numbers, and use it for fraudulent activities. Integrity is violated because attackers can manipulate the user's web experience.

Question 3 – Risk on Gathered Data

If an XSS vulnerability is exploited in the web application of the company, attackers can gain access to sensitive information and cause significant harm to the organization. The attackers can obtain login credentials of the users, including sellers, buyers, and admin users, which can lead to unauthorized access to the system. Furthermore, attackers can manipulate the user's web experience, leading to unexpected or unintended actions, such as acting on the user's behalf or pointing them to a malicious website.

(4) Other vulnerabilities on OWASP machine

Command Execution Vulnerability

It was identified that the company web application is vulnerable for OS Command execution. The vulnerability of OS command execution allows attackers to execute random commands on the victim machine. If properly exploited, this vulnerability can grant attackers entire control of the system, allowing them to engage in a variety of illegal activities.

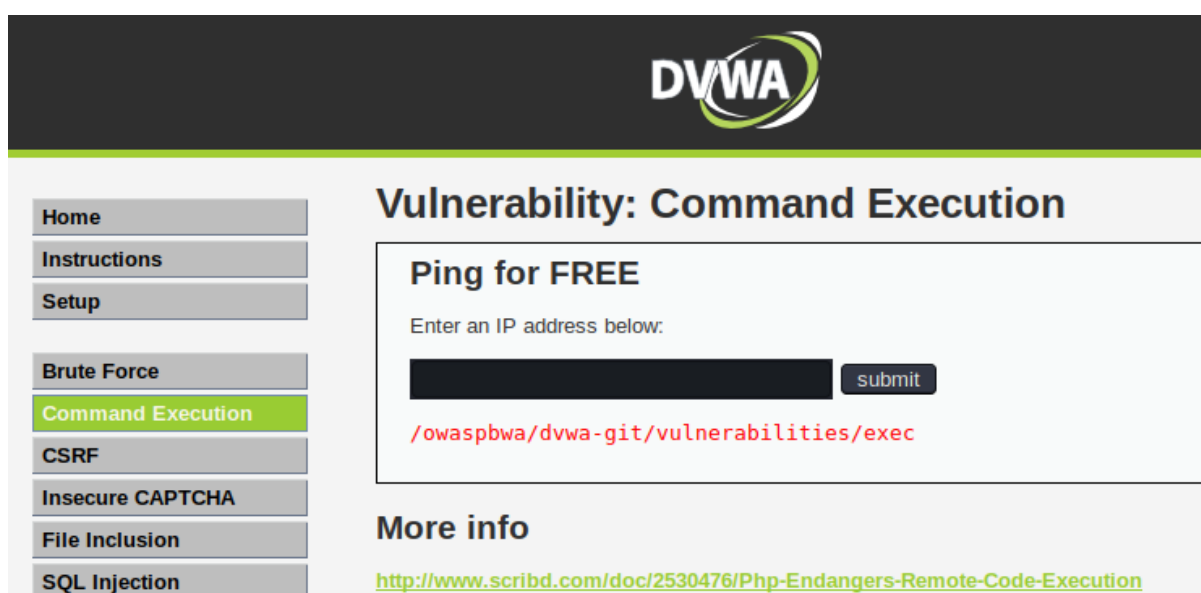


Figure 20 – command execution results

Attacker can view the server files from the current directory and possibly can navigate between folders using commands.

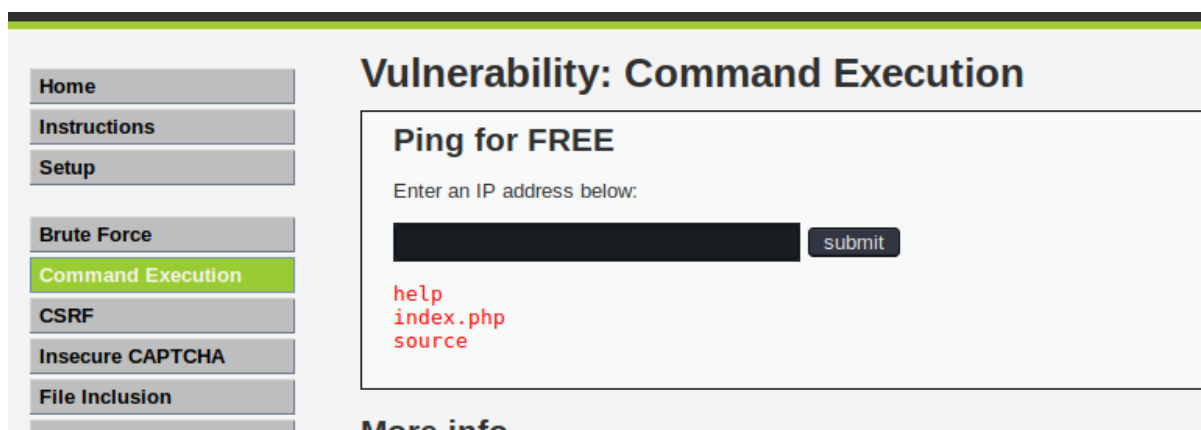


Figure 21 – Viewing the resources using command execution.

Buffer Overflow Vulnerability

This type of attack occurs due to the code of the web application. The large amount of repetition value is going through input validation which at some point can cause the overflow the allocated buffer. By inspecting the web page source, it was identified that the memory allocated for input is 20bytes.

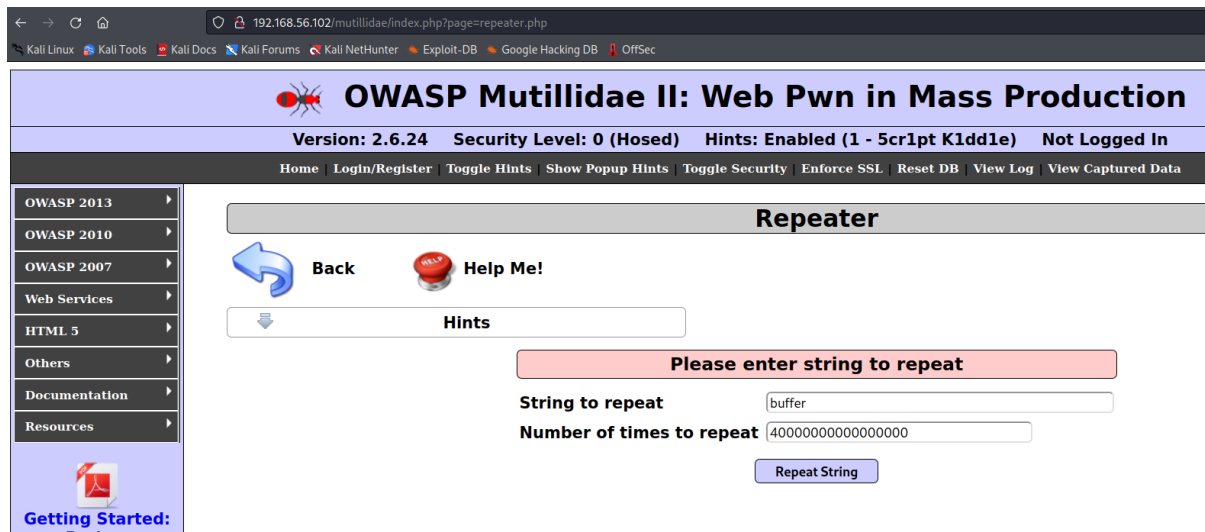


Figure 22 – Overflowing the buffer using number of repeats

Page becomes unavailable.

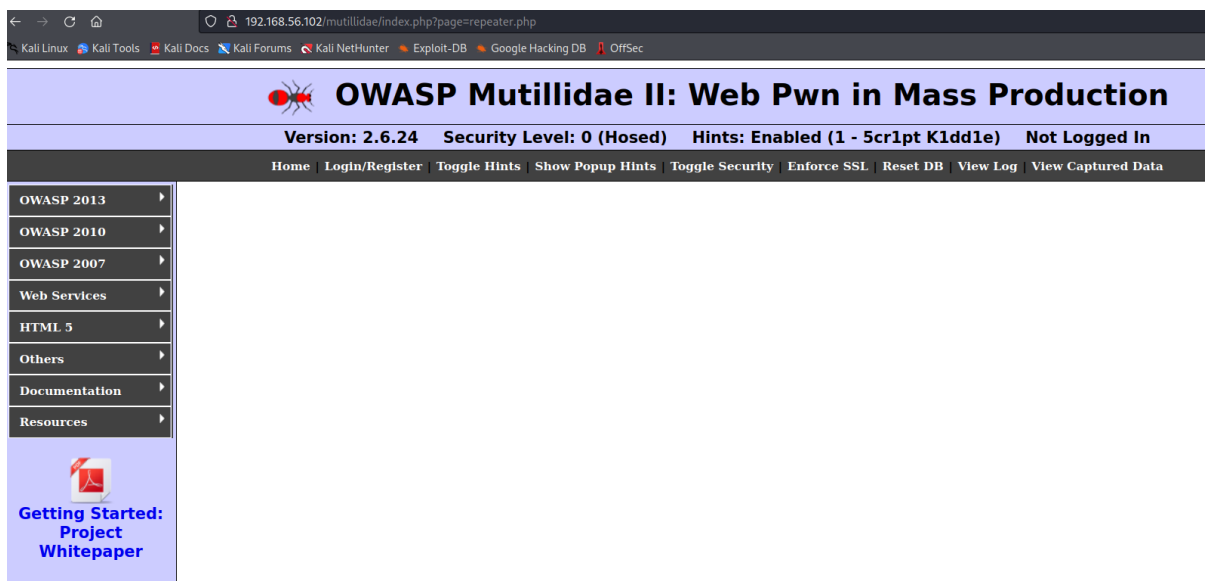


Figure 23 – Unresponsive webpage with overflowed buffer

C – Client-Side Exploits

(1) Man in the Middle Attack (MiTM)

Question 1 – Setting up tools for MiTM

Intercepting the traffic between the web server and the target machine was captured using the Ettercap tool.

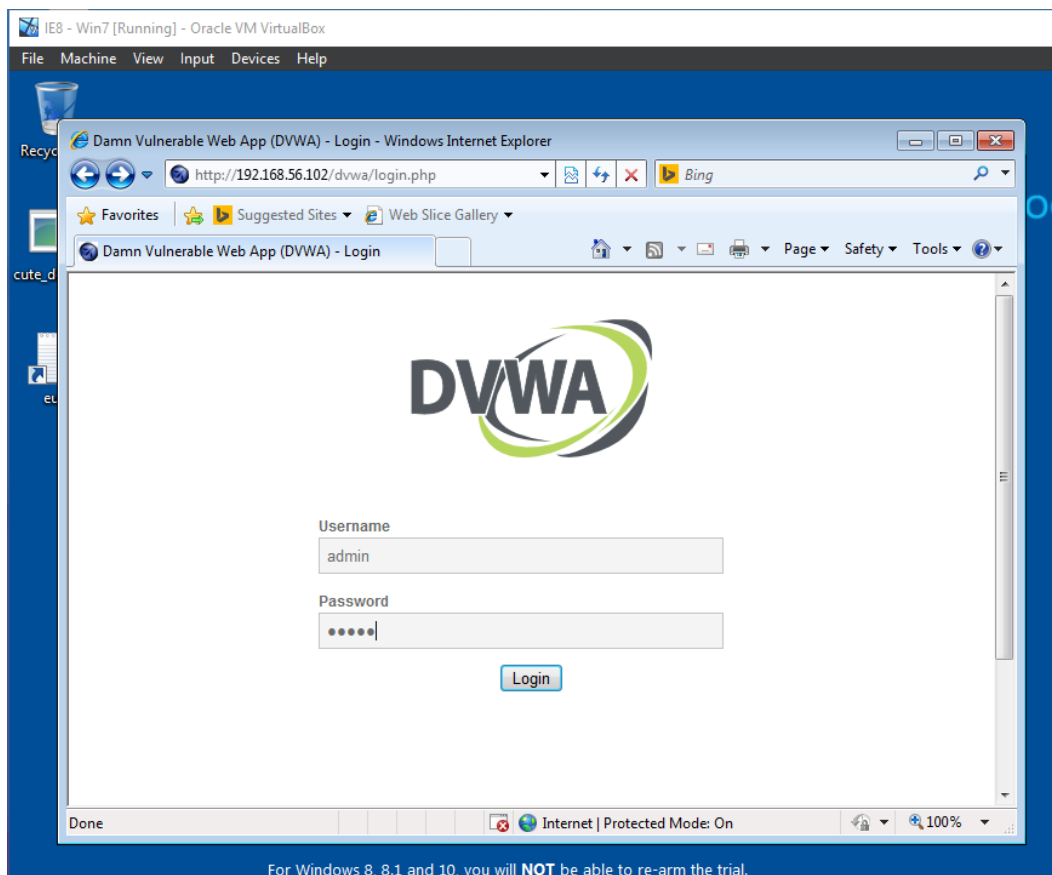


Figure 24 – User entering login credentials.

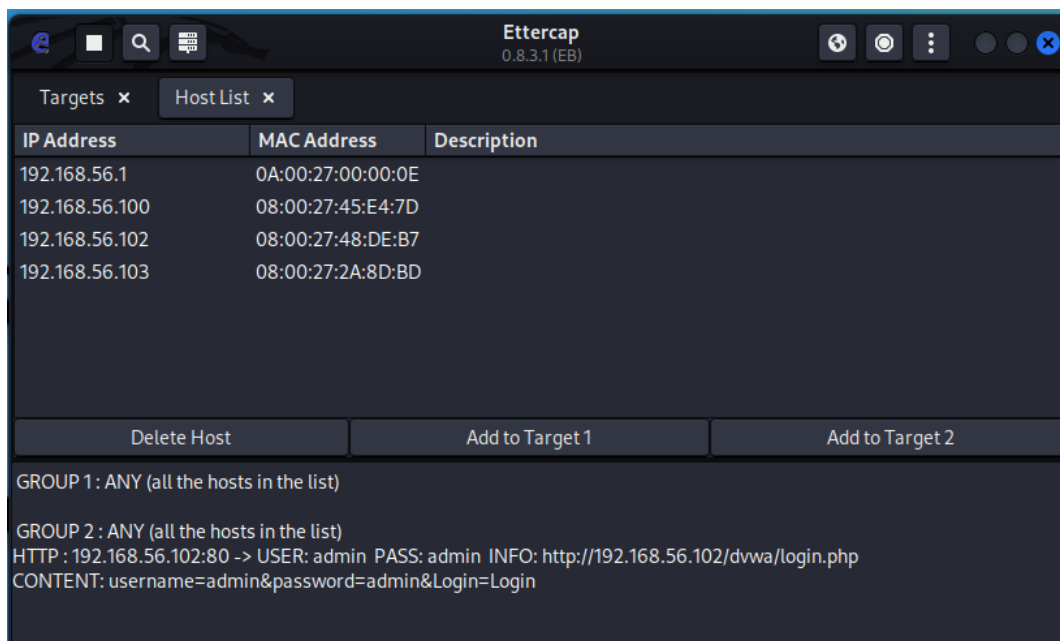


Figure 25 – Intercepting user login using ettercap.

This was done using ARP poisoning.

Login credentials can be captured from the Wireshark tool.

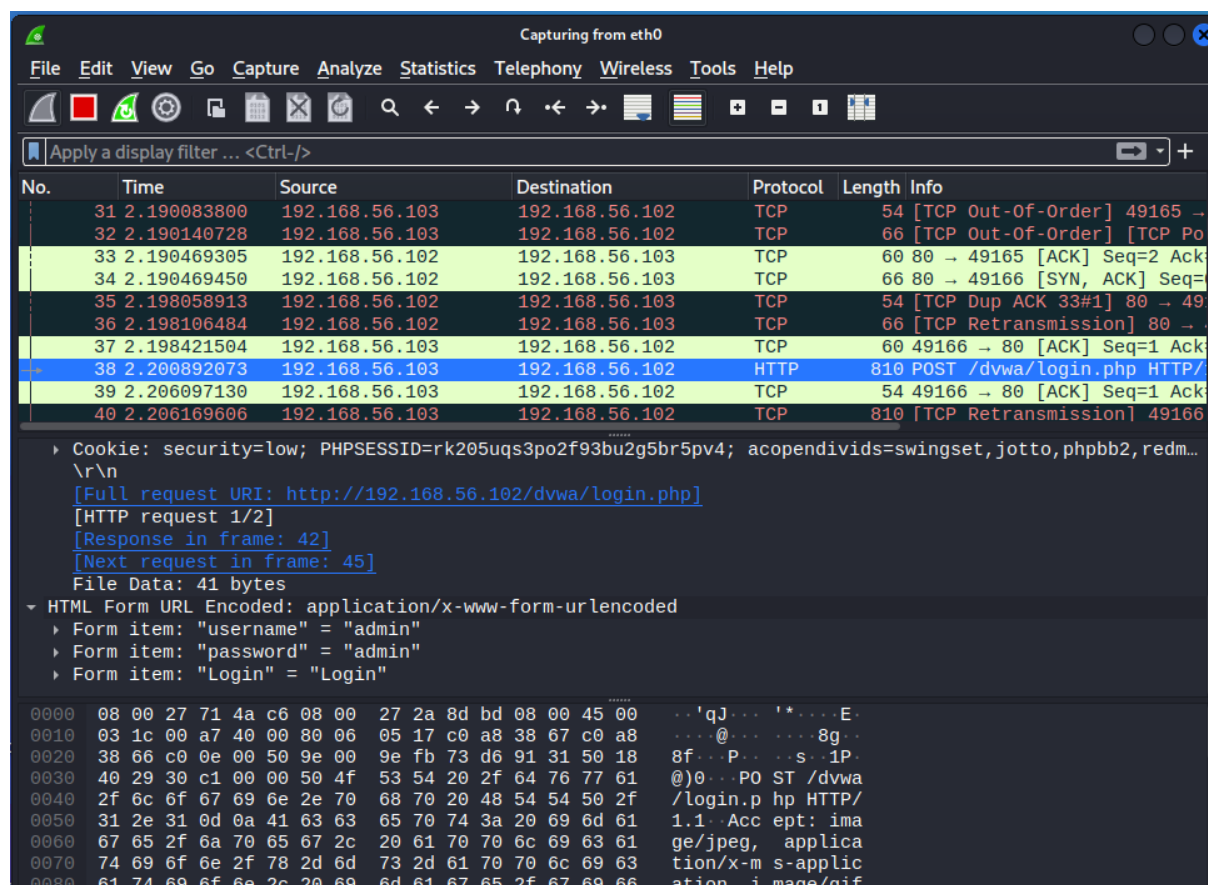


Figure 26 – Viewing the modified post request using Wireshark.

Question 2 – Risk on Gathered Data

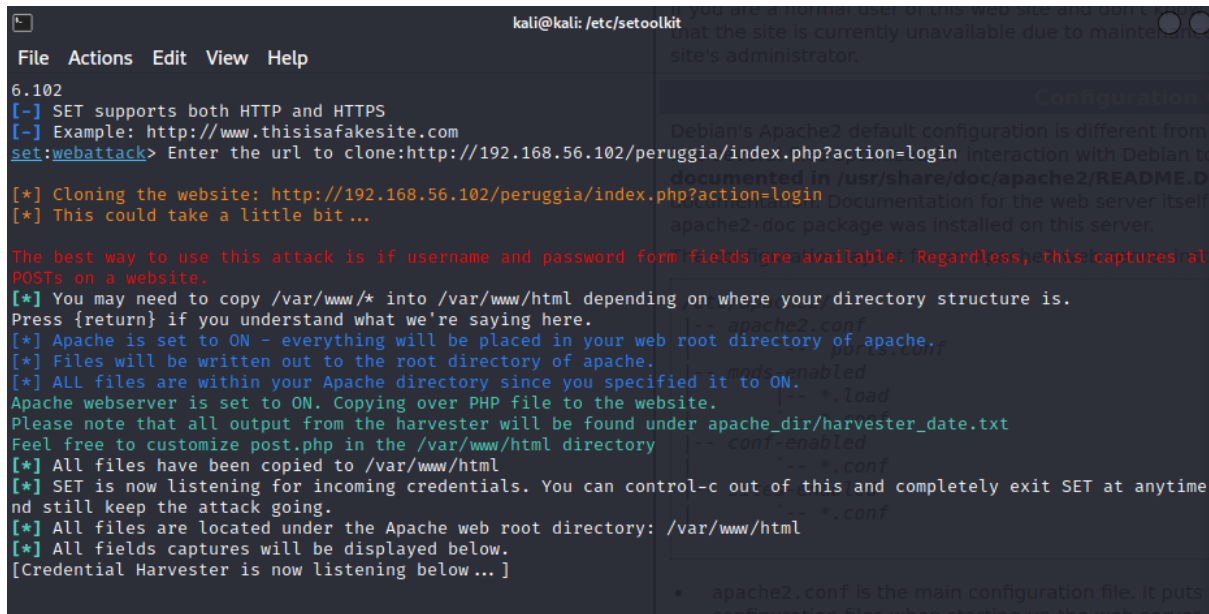
In a man-in-the-middle (MITM) attack, an attacker intercepts the communication between two endpoints, such as between the car buying and selling company's web application and a user's browser, allowing them to access and potentially modify the data exchanged between the two parties. If successfully executed, an attacker can obtain sensitive information, including login details, personal details, and financial information, which can be used for identity theft, phishing scams, or other fraudulent activities. Also, this can compromise the privacy and security of its customers' sensitive information, resulting in significant financial and reputational damage to the company.

(2) Social Engineering Attack

Question 1 – Setting up tools for social engineering attack

Social Engineering Toolkit is designed to perform attacks such as phishing, malicious websites and more. Using SET first will try to setup a fake webpage by cloning a valid website. For this example, will be using peruggia web login page. Also, will be setting up an IP address to send back the credentials via the fake web page. After the victim entered the credentials, the page will redirect to its original website.

In the bellow image it represents the actively listening SET tool for a response from the fake website. In this case the URL will be the attacker's Ip address.



```
kali@kali: /etc/setoolkit
File Actions Edit View Help
6.102
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://192.168.56.102/peruggia/index.php?action=login
[*] Cloning the website: http://192.168.56.102/peruggia/index.php?action=login
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all
POSTs on a website.
[*] You may need to copy /var/www/* into /var/www/html depending on where your directory structure is.
Press {return} if you understand what we're saying here.
[*] Apache is set to ON - everything will be placed in your web root directory of apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/harvester_date.txt
Feel free to customize post.php in the /var/www/html directory
[*] All files have been copied to /var/www/html
[*] SET is now listening for incoming credentials. You can control-c out of this and completely exit SET at anytime
and still keep the attack going.
[*] All files are located under the Apache web root directory: /var/www/html
[*] All fields captures will be displayed below.
[Credential Harvester is now listening below...]
```

Figure 27 - Starting the SET as a local server in the KALI vm

If the victim entered the fake IP on the address bar without knowing it's a fake one, the user will try to login using the credentials.

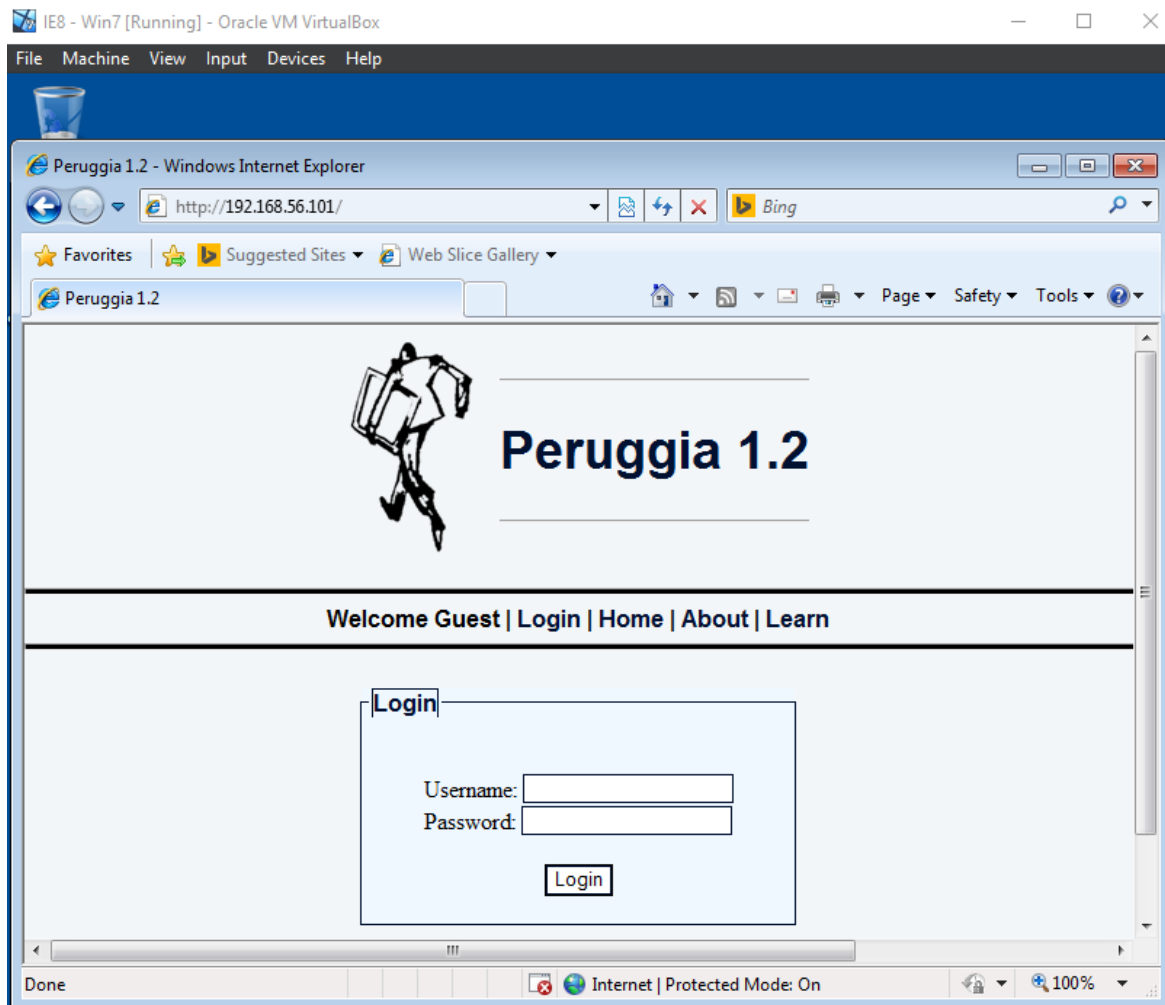


Figure 28 – Cloned fake user login page.

After clicking the login button, the request will be sent to the attacker's webserver with gathered login credentials and the user will be redirected to the original web page without noticing anything suspicious. By sending the victim the fake URL by use of social engineering skills the attacker can steal the login credentials and the victim will be redirected to the original web page.

```
kali@kali: ~/Desktop/social
File Actions Edit View Help
[*] You may need to copy /var/www/* into /var/www/html depending on where your directory structure
Press {return} if you understand what we're saying here.
[*] Apache is set to ON - everything will be placed in your web root directory of apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/harvester_date.txt
Feel free to customize post.php in the /var/www/html directory
[*] All files have been copied to /var/www/html
[*] SET is now listening for incoming credentials. You can control-c out of this and completely ex
and still keep the attack going.
[*] All files are located under the Apache web root directory: /var/www/html
[*] All fields captures will be displayed below.
[Credential Harvester is now listening below...]

Array
(
    [username] => admin
    [password] => admin
)
```

Figure 29 – Intercepted user credentials

Question 2 – Risk on Gathered Data

If an attacker uses social engineering to send a fake URL that steals the login credentials of sellers, buyers, or admin users, it can be very dangerous for the scenario. The attacker can use these stolen credentials to gain unauthorized access to the web application, which can result in data theft, data manipulation, or other malicious activities. This can cause significant damage to the company, such as compromising the integrity of the information stored in the application, stealing financial information or customer data, and damaging the reputation of the company. In addition, if the admin user credentials are compromised, the attacker can gain full control of the web application, which can be disastrous for the company's operations and customers.

D – Denial of Service Attacks

(1) DoS the Web Server

The web server becomes unavailable by sending large number of TCP requests from the attacker's machine. This causes unbalance to access the web application from the user's machine.

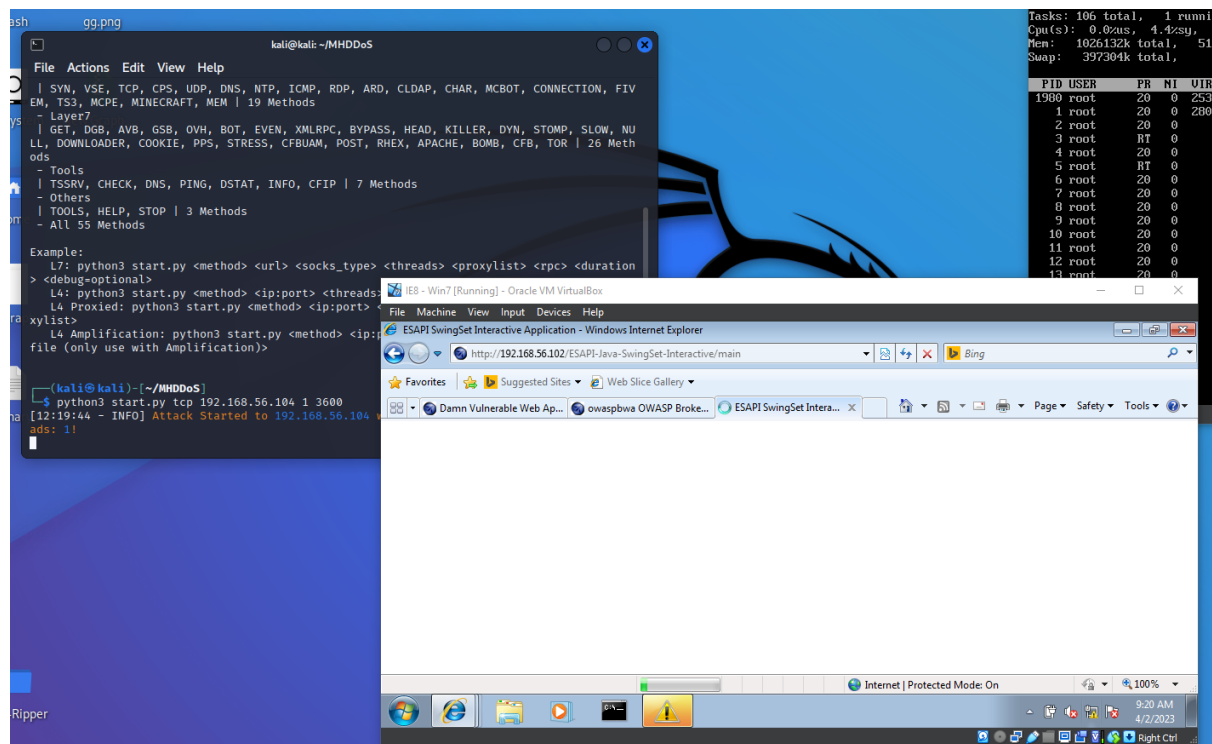


Figure 30 – Web application becomes slow after performing the dos attack on web server.

Denial of Service (DoS) attacks violate the availability tenet of cybersecurity. The availability tenet ensures that the information and resources are accessible and usable by authorized users whenever they are needed.

In the scenario provided, a Denial of Service (DoS) attack could have a significant impact on the availability of the web application, making it inaccessible to legitimate users, including buyers, sellers, and admin users. This can result in a loss of revenue for the company and damage to its reputation. If the web application is critical to the company's operations, the impact of a DoS attack can be even more severe, leading to a halt in business activities, loss of productivity, and potential legal and financial consequences. Additionally, if the attack is prolonged, it can cause damage to the underlying infrastructure and lead to extended downtime, which can be costly to repair.

E – Recommendation to protect the scenario company server

(1) Reducing Threats from Reconnaissance

To minimize threats from reconnaissance attacks carried out by hackers on the car buying and selling company's web application, it is recommended to turn off the ICMP echo and close all unused ports. Additionally, the use of a masking service can be employed to hide sensitive

information of customers and sellers on the platform. A firewall can also be utilized to filter incoming traffic to the web server, thereby preventing malicious traffic from reaching the system. These measures can help reduce the potential for reconnaissance attacks and enhance the overall security of the web application.

(2) Port Knocking

Port knocking can protect against threats by adding an additional layer of security to the system. By hiding open ports and only allowing access to specific ports or services after the correct sequence of connections is detected, it can prevent attackers from gaining access to sensitive information or services on the system (Manzanares et al., 2005). This technique makes it difficult for attackers to scan for open ports and launch attacks, as they need to know the specific sequence of connections to gain access. Port knocking can be used alongside other security measures such as firewalls, intrusion detection systems (IDS), and access control lists to further enhance the security of a system.

(3) SQL Injection

One effective way to prevent cyberattacks, especially SQL injection attacks, is to monitor and validate user input channels for any suspicious activity. This can be achieved by implementing technical measures such as input validation, which only allows values that have passed the testing procedure. Another approach is using parametrized queries, where user input is dynamically quoted and verified to prevent any malicious intent. In addition, implementing a firewall can also help prevent such attacks (Boyd and Keromytis, 2004).

(4) Cross Site (XSS) Scripting

Cross-site scripting (XSS) attacks can be prevented by the following factors. One important strategy is to filter input on arrival, which includes checking all user input to make sure that it's valid and free of malicious code. This can be achieved by applying proper input validation filters that only allow expected characters and inputs to be entered into the system. Another approach is to encode data on output, which involves encrypting client data in HTTP messages so that it is not perceived as active content. This can be achieved by using proper encoding mechanisms, such as HTML entity encoding or URL encoding. Furthermore, using appropriate response headers can also help prevent XSS attacks by instructing web browsers on how to handle content that is sent to them. These measures can greatly reduce the risk of XSS attacks and enhance the security of web applications.

(5) Man in the Middle Attacks

Two-factor authentication: The security analyst can implement two-factor authentication to ensure that even if an attacker intercepts a user's login credentials, they still cannot gain access to the system without an additional authentication factor.

Intrusion detection and prevention: The security analyst can implement intrusion detection and prevention systems to detect and block suspicious traffic.

Allow organizations to use VPN.

(6) Social Engineering Attacks

Educate employees: Companies should educate their employees about the dangers of social engineering attacks and provide them with training to recognize and respond to such attacks. The training should cover topics such as phishing emails, pretexting, and baiting.

Security measures should be reviewed and updated on a regular basis to ensure that they are effective against the most recent threats. This includes updating software and hardware, monitoring network traffic for suspicious activity, and conducting regular security audits.

(7) DoS Attacks

Firewalls are possible to be configured to block traffic from specific IP addresses or ranges. By blocking traffic from known malicious IP addresses, companies can prevent their web services from being attacked. Also, some companies offer DDoS protection services that can detect and block attacks before they reach a company's servers. These services use advanced algorithms to identify and block malicious traffic, allowing legitimate traffic to reach the web service uninterrupted.

(8) Intrusion Detection and Prevention Systems

Examples of UFW and Iptables

By enabling ufw firewall and allow access to specified ports. In this example firewall rule is added and allowed for port 443 and 80.

```
In all these cases, you can use username "root" and password "owaspbwa".
root@owaspbwa:~# sudo ufw
ERROR: not enough args
root@owaspbwa:~# sudo ufw allow 80/tcp
Rules updated
root@owaspbwa:~# sudo ufw allow 443/tcp
Rules updated
root@owaspbwa:~# sudo ufw status
Status: inactive
root@owaspbwa:~# sudo ufw enable
Firewall is active and enabled on system startup
root@owaspbwa:~# sudo ufw status
Status: active
```

To	Action	From
--	-----	----
80/tcp	ALLOW	Anywhere
443/tcp	ALLOW	Anywhere

```
root@owaspbwa:~# _
```

Figure 31 – Adding firewall rules to the ports.

Then the iptables rules were added to the following ports,

Port Number	Command
80	sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
443	sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

Table 2 – Ports and iptables rule

```

File Machine View Input Devices Help
-A ufw-before-input -d 224.0.0.0/4 -j ACCEPT
-A ufw-before-input -j ufw-user-input
-A ufw-before-output -o lo -j ACCEPT
-A ufw-before-output -m state --state RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-output -j ufw-user-output
-A ufw-logging-allow -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW ALLOW] "
-A ufw-logging-deny -m state --state INVALID -m limit --limit 3/min --limit-burst 10 -j RETURN
-A ufw-logging-deny -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW BLOCK] "
-A ufw-not-local -m addrtype --dst-type LOCAL -j RETURN
-A ufw-not-local -m addrtype --dst-type MULTICAST -j RETURN
-A ufw-not-local -m addrtype --dst-type BROADCAST -j RETURN
-A ufw-not-local -m limit --limit 3/min --limit-burst 10 -j ufw-logging-deny
-A ufw-not-local -j DROP
-A ufw-skip-to-policy-forward -j DROP
-A ufw-skip-to-policy-input -j DROP
-A ufw-skip-to-policy-output -j ACCEPT
-A ufw-track-output -p tcp -m state --state NEW -j ACCEPT
-A ufw-track-output -p udp -m state --state NEW -j ACCEPT
-A ufw-user-input -p tcp -m tcp --dport 80 -j ACCEPT
-A ufw-user-input -p tcp -m tcp --dport 443 -j ACCEPT
-A ufw-user-limit -m limit --limit 3/min -j LOG --log-prefix "[UFW LIMIT BLOCK] "
-A ufw-user-limit -j REJECT --reject-with icmp-port-unreachable
-A ufw-user-limit-accept -j ACCEPT
COMMIT
# Completed on Sun Apr 23 18:31:14 2023
root@owaspbwa:~#

```

Figure 32 – Adding iptables rules to the specified ports.

After the attacker's machine IP is blocked from the webserver using bellow command,

`sudo iptables -A INPUT -s 192.168.56.101 -j DROP.`

Effectiveness of Iptables and Firewall

Iptables is a powerful tool for configuring the Linux kernel's built-in firewall, providing granular control over network traffic. Unlike the UFW firewalls, It enables the administrator to create complex rules for filtering network traffic based on various factors including both source and destination IP addresses, ports, protocols, and more (iptables(8) - Linux man page, no date).

Feature	iptables	ufw
Type	Command-line interface	Command-line interface
Level of control	Higher	Lower
Complexity	High	Low
Syntax	Complex	Simplified
Configuration	Must be manually configured	Simplified configuration
Rules	Highly customizable	Limited
Network Traffic Analysis	Can analyze and block specific types of traffic	Limited network traffic analysis
Learning curve	Steep	Easy

Table 3 – Comparison of iptables and firewalls

Difference between Intrusion Detection System IDS and IPS

The primary distinction between IDS and IPS is how they deal with security threats. IDS is a passive security system that merely detects and notifies malicious network activity. IDS analyzes network traffic for patterns that may indicate a security violation. When an attack is identified, the intrusion detection system (IDS) delivers an alert to the network administrator, who is responsible for taking corrective action.

Suggestions and Recommendation

Since the car buying and selling platform holds highly sensitive and confidential data from both customers, sellers, and company users; The most suitable recommendation can be given with the best security practices. In this case it will be Iptables with and IPS system can reduce and mitigate the above-mentioned cybersecurity threats.

References

Boyd, S.W. and Keromytis, A.D. (2004). SQLrand: Preventing SQL Injection Attacks. In: Jakobsson, M. Yung, M. and Zhou, J. (eds.). *Applied Cryptography and Network Security*. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 292–302. Available from https://doi.org/10.1007/978-3-540-24852-1_21 [Accessed 23 April 2023].

Confidentiality, Integrity and Availability - The CIA Triad. (2018). *CertMike*. Available from <https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/> [Accessed 23 April 2023].

Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT) - ScienceDirect. (no date). Available from <https://www.sciencedirect.com/science/article/abs/pii/S0747563211002585> [Accessed 1 May 2023].

iptables(8) - Linux man page. (no date). Available from <https://linux.die.net/man/8/iptables> [Accessed 24 April 2023].

Ma, L. et al. (2019). Research on SQL Injection Attack and Prevention Technology Based on Web. *2019 International Conference on Computer Network, Electronic and Automation (ICCNEA)*. September 2019. 176–179. Available from <https://doi.org/10.1109/ICCNEA.2019.00042>.

Manzanares, A. et al. (2005). *Attacks on Port Knocking Authentication Mechanism*. Available from https://doi.org/10.1007/11424925_134.

Mathew, K., Tabassum, M. and lu, M. (2014). *A Study Of Open Ports As Security Vulnerabilities In Common User Computers*. Available from <https://doi.org/10.13140/2.1.1807.2324>.

OWASP Top 10:2021. (no date). Available from <https://owasp.org/Top10/> [Accessed 23 April 2023].