INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

6COSC019C Cyber Security

Module leader: Mr. Saman Hettiarachchi

A Coursework by

Mr. Wehan Withana

W1761296 / 2019349

Submitted in partial fulfilment of the requirements for the BEng in Software Engineering degree at the University of Westminster.

16th May 2023

Content

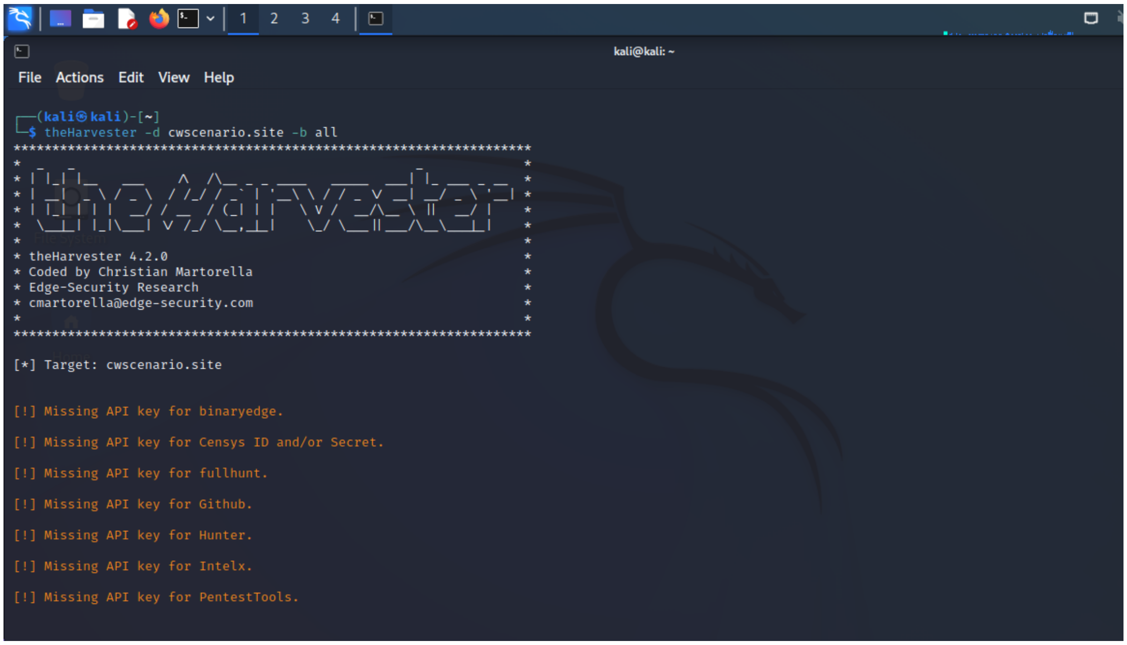
Table of Figures

A. Information Gathering

A.1. OSINT Activities

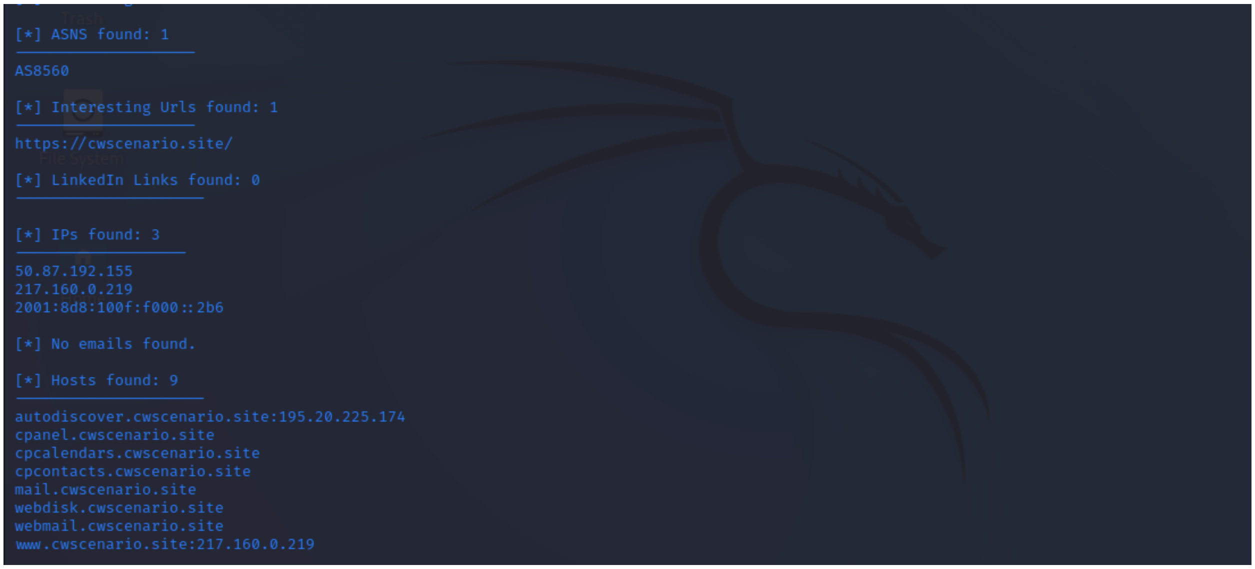
i. Information collection is a crucial stage that involves a variety of actions intended to acquire pertinent data. Extracting data from websites, such as IP addresses, job postings, emails, and certain keywords, may be one of these actions. Public reporting and social media sites may also be excellent sources of information.

a) Harvesters are essential tools used in OSINT operations to collect and extract data from a variety of internet sources. The automated data collection process using websites, social media platforms, public documents, and other easily available sources is made possible by these tools. Harvester programs may swiftly scan and gather pertinent data, including usernames, email addresses, and other important data points. Harvesters allow OSINT practitioners to efficiently gather a lot of data and find connections or patterns that could be important for an investigation. To preserve the privacy and security of people and organizations, it's crucial to remember that the usage of harvesters must always adhere to legal and ethical rules.(*Mastering Kali Linux for Advanced Penetration Testing: Secure Your Network ... - Vijay Kumar Velu, Robert Beggs - Google Books*, n.d.)



```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d cwscenario.site -b all
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* 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.

[!] Missing API key for Github.

[!] Missing API key for Hunter.

[!] Missing API key for Intelx.

[!] Missing API key for PentestTools.
```

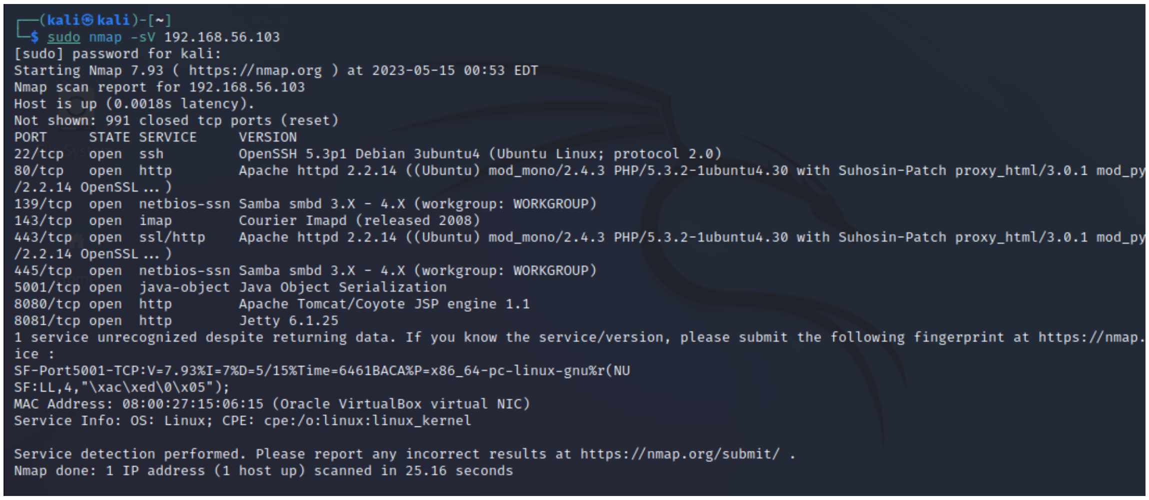
Figure A.1 - Harvester using in OSINT Activities



```
[*] 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: 9
---------------------

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 A.2 - Harvester using in OSINT Activities (2)

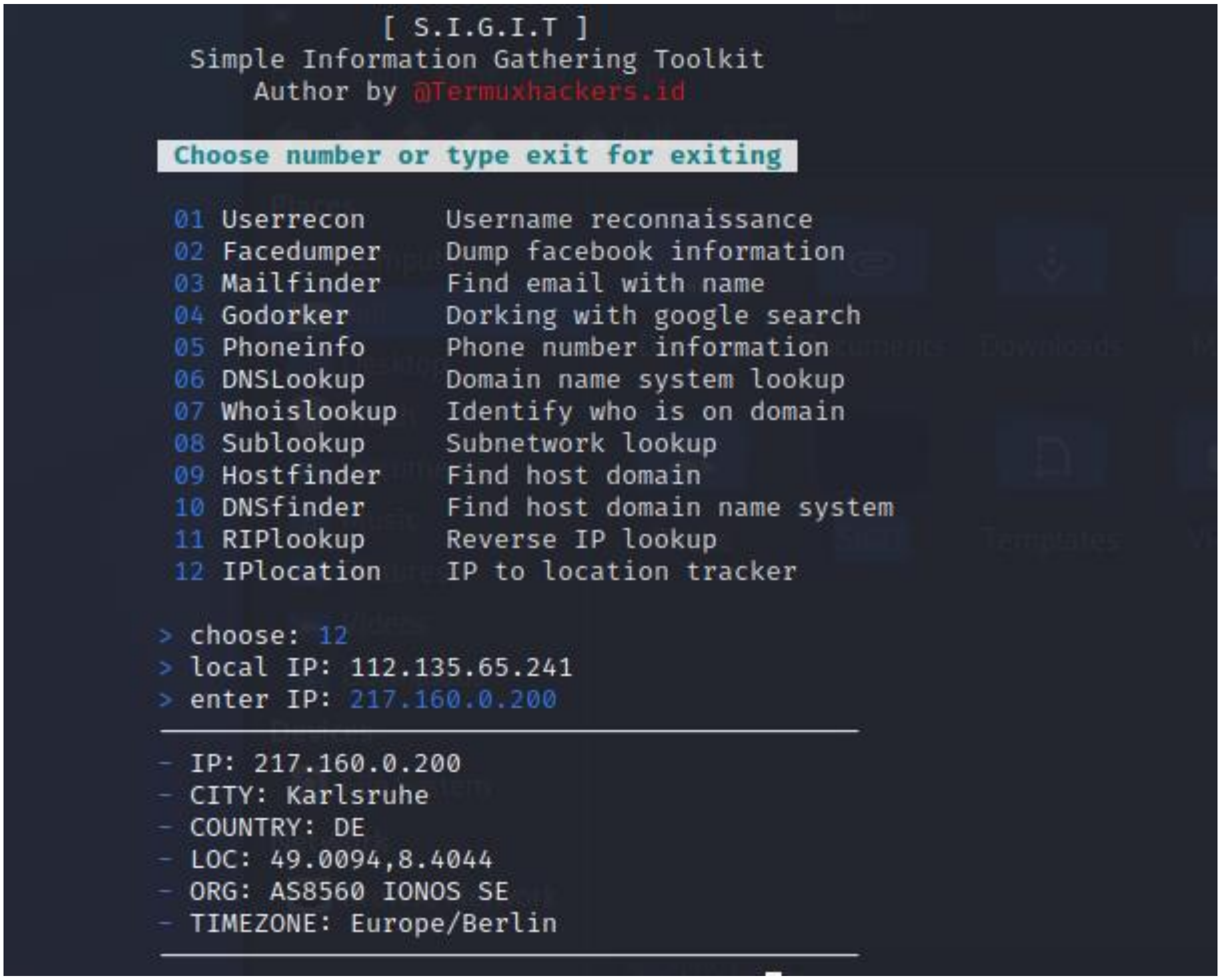
b) Nmap is a widely used tool in OSINT activities due to its versatility and capability to provide valuable insights into network infrastructure. With the help of Nmap, users may locate active hosts, open ports, and actively running services on target systems. Nmap is typically used for network scanning and discovery. Nmap may be used in OSINT efforts to acquire details about a target's network topology, spot potential flaws or incorrect setups, and gauge the network's overall security posture. OSINT practitioners may gather useful information about a target's network architecture by utilizing Nmap's comprehensive scanning capabilities. This information is useful for decision-making, vulnerability assessment, and risk analysis.(*Mastering Kali Linux for Advanced Penetration Testing - Vijay Kumar Velu - Google Books*, n.d.)



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.56.103
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 00:53 EDT
Nmap scan report for 192.168.56.103
Host is up (0.0018s 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_py
/2.2.14 OpenSSL ... )
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_py
/2.2.14 OpenSSL ... )
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 submit the following fingerprint at https://nmap.
ice :
SF-Port5001-TCP:V=7.93%I=7%D=5/15%Time=6461BACA%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"\xac\xed\0\x05");
MAC Address: 08:00:27:15:06:15 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.16 seconds
```

Figure A.3 - Nmap using in OSINT Activities

c) Various information collecting toolkits are utilized in OSINT efforts to acquire and analyze data from publicly accessible sources. These toolkits frequently include specialized software, web resources, and search strategies to help with the extraction and organizing of important data.



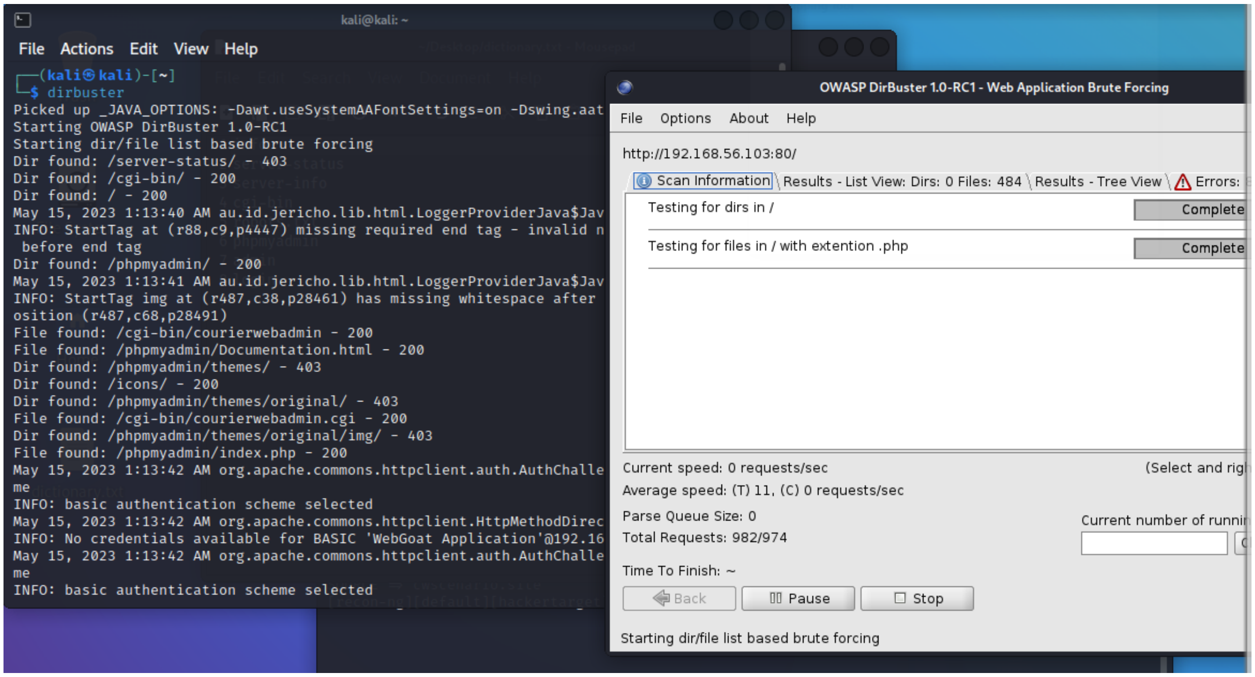
```
                   [ S.I.G.I.T ]
          Simple Information Gathering Toolkit
              Author by @Termuxhackers.id

         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: 12
         > local IP: 112.135.65.241
         > enter IP: 217.160.0.200
         ────────────────────────────────────────────
         - IP: 217.160.0.200
         - CITY: Karlsruhe
         - COUNTRY: DE
         - LOC: 49.0094,8.4044
         - ORG: AS8560 IONOS SE
         - TIMEZONE: Europe/Berlin
         ────────────────────────────────────────────
```

ii. Open-Source Intelligence, or OSINT, is essential in the early phases of information collecting for a variety of objectives. It entails gathering data from sources that are openly accessible without using a particular methodology, assuring a passive reconnaissance approach. Sources such as publicly available phone numbers, server information including open ports and operating services, and even information provided by workers on public platforms can all provide valuable data. These seemingly unimportant details that are frequently ignored might be used to plan and strategize prospective assaults. (Glassman & Kang, 2012)

iii. **Scenario assessment:** When engaging in OSINT activities, passive reconnaissance gives users access to useful data that might be used for intelligence collecting. In this process, tools like SIGINT, Harvester, and Nmap are essential. One can gain important data by utilizing geolocation tracking based on IP addresses. The use of WHOIS also enables the extraction of email addresses and the identification of related domains. Legal reports help in identifying the underlying platforms of the target websites, and weaknesses in IoT devices can be found. Tools like Wget make it easier to download full websites offline, including hidden folders that can hold important data. Even in the absence of direct assaults, OSINT techniques help to pinpoint weaknesses and build extensive profiles of targets, guaranteeing a complete awareness of the target's security posture.

A.2. Reconnaissance

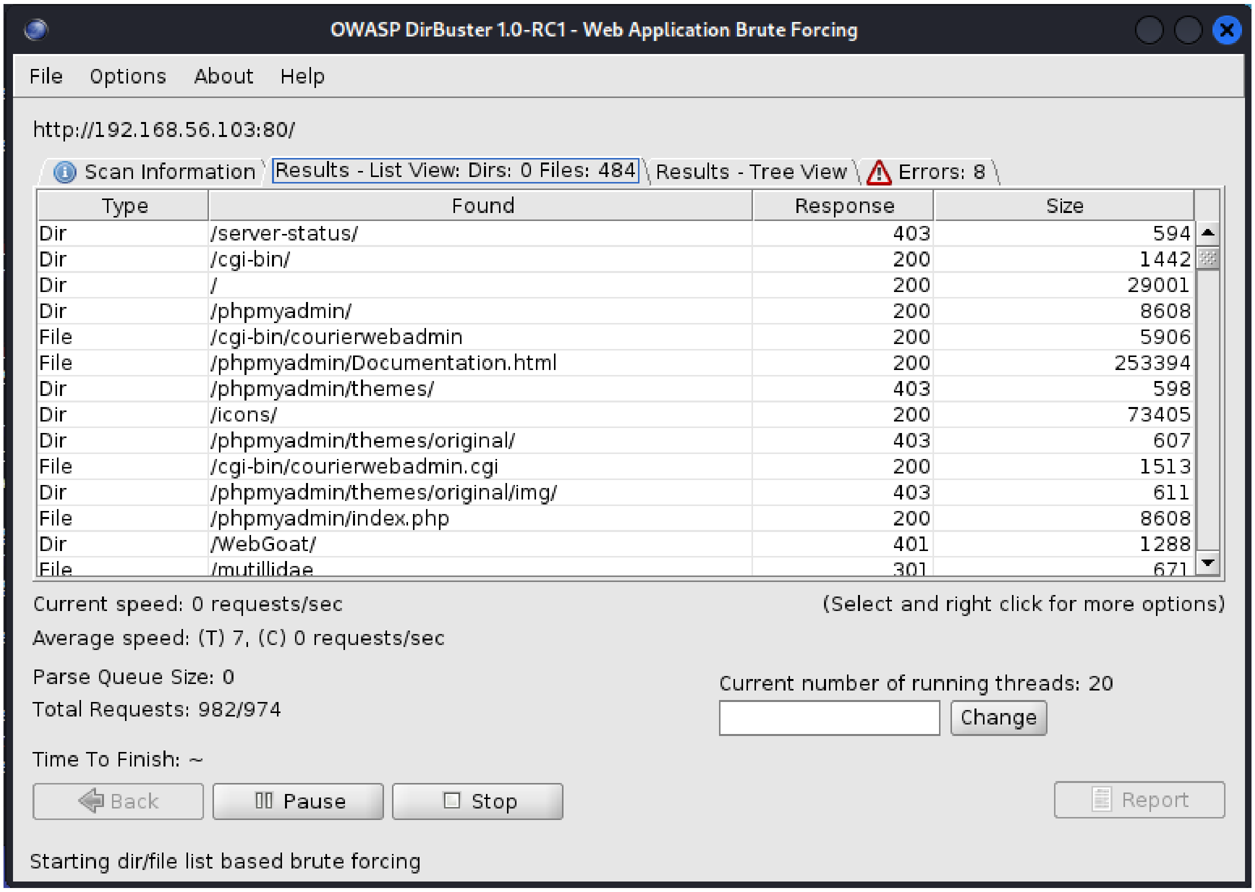
1. DirBuster is a widely used tool in the field of cybersecurity and OSINT activities. DirBuster assists in locating folders and files that might not be readily accessible or apparent through normal browsing by methodically examining a target website's directory structure. This tool is useful for gathering information since it helps users to find resources that may be hidden or contain sensitive information that might be of interest. (Richter et al., 2021)



```
┌──(kali㉿kali)-[~]
└─$ dirbuster
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aat
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: /server-status/ - 403
Dir found: /cgi-bin/ - 200
Dir found: / - 200
May 15, 2023 1:13:40 AM au.id.jericho.lib.html.LoggerProviderJava$Jav
INFO: StartTag at (r88,c9,p4447) missing required end tag - invalid n
 before end tag
Dir found: /phpmyadmin/ - 200
May 15, 2023 1:13:41 AM au.id.jericho.lib.html.LoggerProviderJava$Jav
INFO: StartTag img at (r487,c38,p28461) has missing whitespace after
osition (r487,c68,p28491)
File found: /cgi-bin/courierwebadmin - 200
File found: /phpmyadmin/Documentation.html - 200
Dir found: /phpmyadmin/themes/ - 403
Dir found: /icons/ - 200
Dir found: /phpmyadmin/themes/original/ - 403
File found: /cgi-bin/courierwebadmin.cgi - 200
Dir found: /phpmyadmin/themes/original/img/ - 403
File found: /phpmyadmin/index.php - 200
May 15, 2023 1:13:42 AM org.apache.commons.httpclient.auth.AuthChalle
me
INFO: basic authentication scheme selected
May 15, 2023 1:13:42 AM org.apache.commons.httpclient.HttpMethodDirec
INFO: No credentials available for BASIC 'WebGoat Application'@192.16
May 15, 2023 1:13:42 AM org.apache.commons.httpclient.auth.AuthChalle
me
INFO: basic authentication scheme selected
```

```
http://192.168.56.103:80/
Testing for dirs in /                                   Complete
Testing for files in / with extention .php              Complete
Current speed: 0 requests/sec                           (Select and rig
Average speed: (T) 11, (C) 0 requests/sec
Parse Queue Size: 0                                     Current number of runnir
Total Requests: 982/974
Time To Finish: ~
Starting dir/file list based brute forcing
```

Figure A.4 - DirBuster (1)


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 0 Files: 484
Results - Tree View
Errors: 8
Change
Back
Pause
Stop
Report

http://192.168.56.103:80/

Type	Found	Response	Size
Dir	/server-status/	403	594
Dir	/cgi-bin/	200	1442
Dir	/	200	29001
Dir	/phpmyadmin/	200	8608
File	/cgi-bin/courierwebadmin	200	5906
File	/phpmyadmin/Documentation.html	200	253394
Dir	/phpmyadmin/themes/	403	598
Dir	/icons/	200	73405
Dir	/phpmyadmin/themes/original/	403	607
File	/cgi-bin/courierwebadmin.cgi	200	1513
Dir	/phpmyadmin/themes/original/img/	403	611
File	/phpmyadmin/index.php	200	8608
Dir	/WebGoat/	401	1288
File	/mutillidae	301	671

Current speed: 0 requests/sec

(Select and right click for more options)

Average speed: (T) 7, (C) 0 requests/sec

Parse Queue Size: 0

Total Requests: 982/974

Current number of running threads: 20

Time To Finish: ~

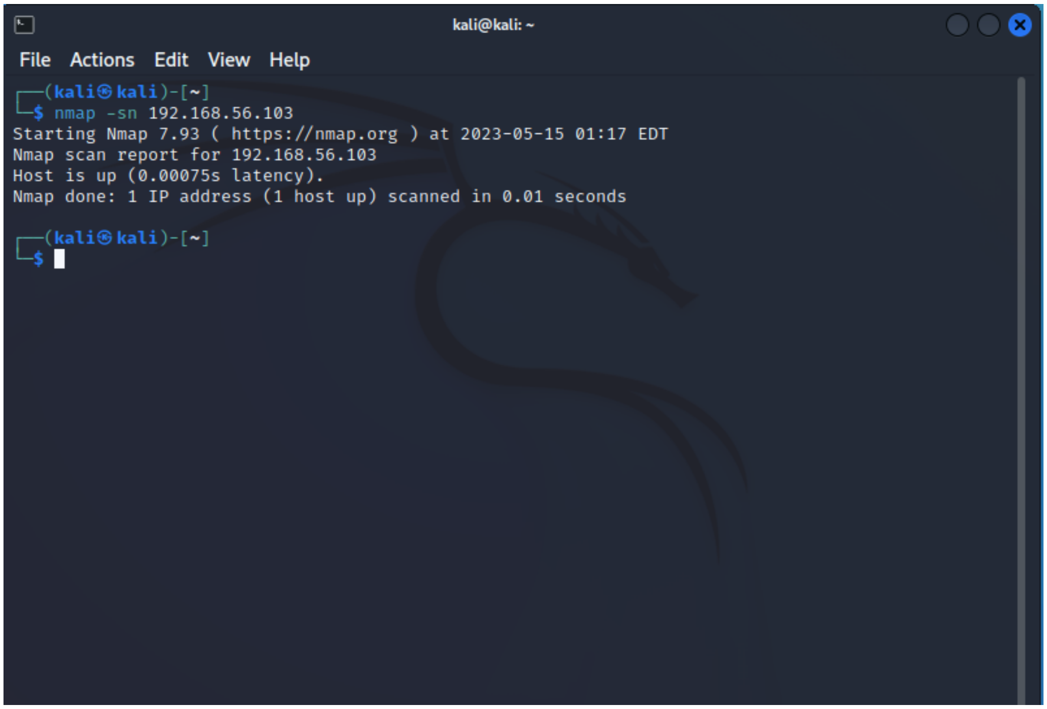
Starting dir/file list based brute forcing

Figure A.5 - DirBuster (2)

2. **Scenario assessment:** Active reconnaissance entails actively exploring the system to find weaknesses in out-of-date services operating on different ports, finding hidden folders, and trying brute-force assaults by profiling passwords. If the system is not sufficiently protected, sensitive financial data, passwords, and other personal information that rental firms are required to acquire might be made public. Customers may become vulnerable to targeted spam emails or social engineering scams as a result, and the business may become a target of ransomware attacks or command/SQL injections. In the scenario of the website relevant information that can be obtained through testing the web application may include user login credentials, customer data such as names and contact information, order details, payment information, and server configuration details.

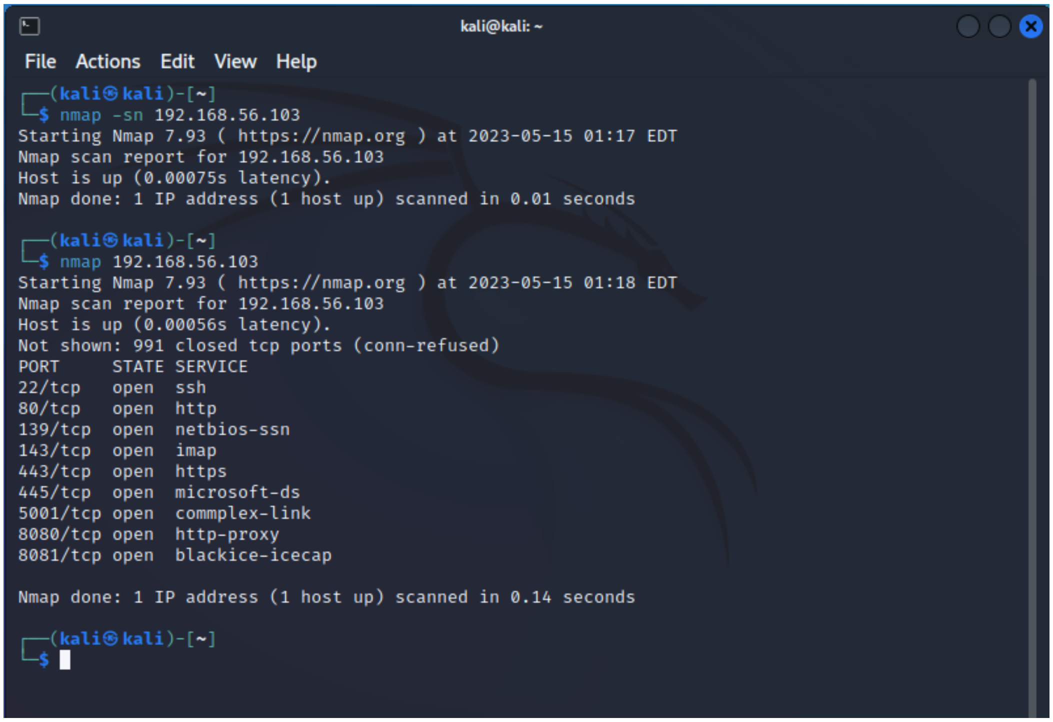
A.3. Port Scanning and Enumeration

i. Network traffic may be captured using programs like Wireshark and Ettercap during the login process of a company's online application, giving access to vital information. These technologies give testers the ability to examine the information sent between a user's device and a server, assisting in the detection of potential security flaws. It is essential to employ these technologies ethically and in a responsible manner, though. Companies may secure their systems and user data by using such strategies to proactively detect and resolve security problems.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.56.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 01:17 EDT
Nmap scan report for 192.168.56.103
Host is up (0.00075s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Figure A.6 - Port Scanning and Enumeration (1)



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.56.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 01:17 EDT
Nmap scan report for 192.168.56.103
Host is up (0.00075s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds

┌──(kali㉿kali)-[~]
└─$ nmap 192.168.56.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 01:18 EDT
Nmap scan report for 192.168.56.103
Host is up (0.00056s 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  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Figure A.7 - Port Scanning and Enumeration (2)

ii. Open ports show that the server is currently accepting connections and actively monitoring certain ports for communication. Open ports, however, can constitute an important risk in security systems that are improperly configured as they may let unwanted access and harmful activities. FTP, SSH, Telnet, and SMTP are a few examples of open ports. These open ports expose network and server information, which may result in information leakage and service interruption. This compromises the confidentiality, integrity, and availability of the system.

iii. **Scenario assessment:**

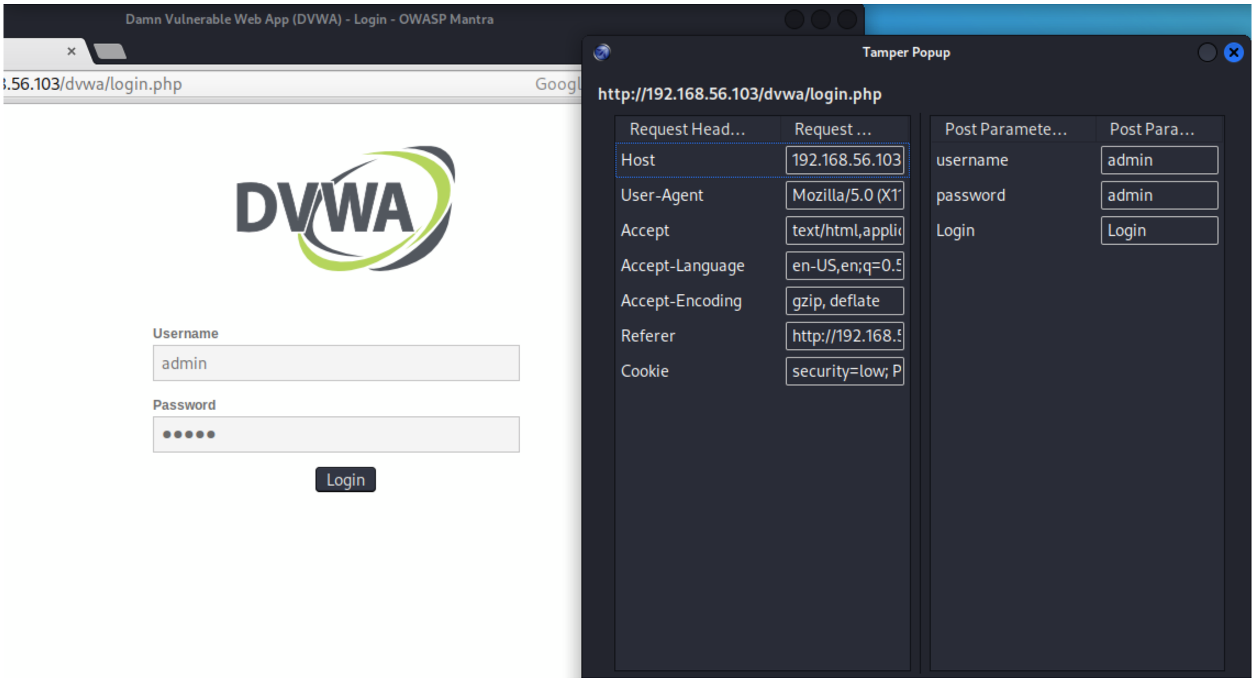
Port	Service	Status	Scenario
22	SSH	Open	The vulnerability allows write operations in read-only mode. Attackers can exploit this vulnerability.
80	HTTP	Open	Outdated servers can pose a danger by potentially causing the unavailability of web services.
8080	HTTP - Proxy	Open	The availability of the web service might potentially be affected, which would be a serious consequence of

			this vulnerability. Attackers can take advantage of the flaw by barraging the server with malicious and illegal traffic, rendering the service unavailable.

B. Server-side exploits

B.1 Data tampering

i. Below is an example of the login page for the web application of a shoe store.



Damn Vulnerable Web App (DVWA) - Login - OWASP Mantra

.56.103/dvwa/login.php

Username: admin

Password: ●●●●●

Login

Tamper Popup

http://192.168.56.103/dvwa/login.php

Request Head...	Request ...
Host	192.168.56.103
User-Agent	Mozilla/5.0 (X1
Accept	text/html,applic
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Referer	http://192.168.5
Cookie	security=low; P

Post Paramete...	Post Para...
username	admin
password	admin
Login	Login

Figure B.1 - Login page for shoe store webpage

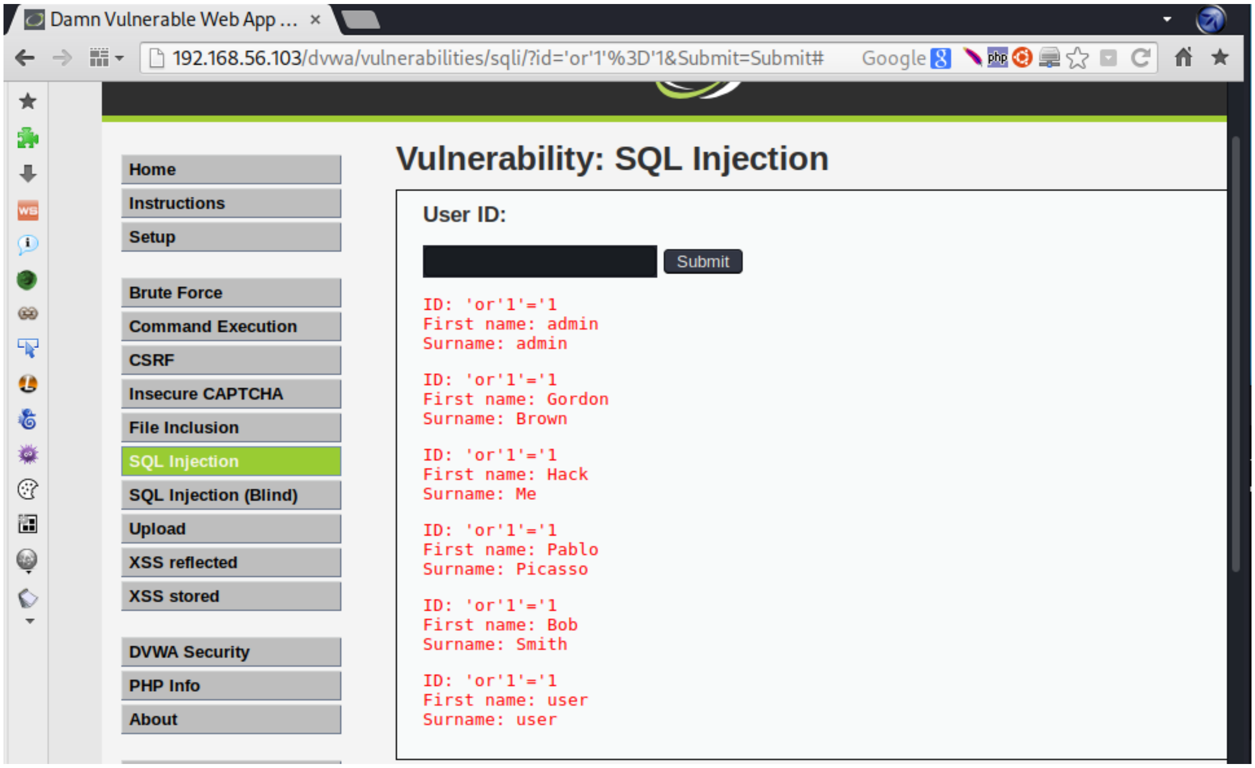
ii. The illegal change or alteration of data that compromises its accuracy and integrity is known as data tampering. Without legal authority, it entails adding, removing, or altering data, which might pose a security risk and encourage unlawful behavior. In addition to cookies, form fields, and HTTP headers, URLs are the primary method used for data manipulation. Some implications of data tampering include: (Huang et al., 2021)

- Loss of data integrity
- Legal and regulatory consequences
- Compromised trust and credibility.

iii. **Scenario assessment:** During the penetration test of the online shoe store, it was discovered that the login page of the system was susceptible to data manipulation. This vulnerability allowed an attacker to modify the entered credentials and retrieve the login and password information provided by users. Exploiting this weakness, attackers can employ brute force techniques to uncover valid account credentials. If successfully exploited, unauthorized access to the shoe store's system could occur, potentially leading to the compromise of sensitive data belonging to customers and causing significant security breaches.

B.2 SQL Injection

i.



Vulnerability: SQL Injection

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
```

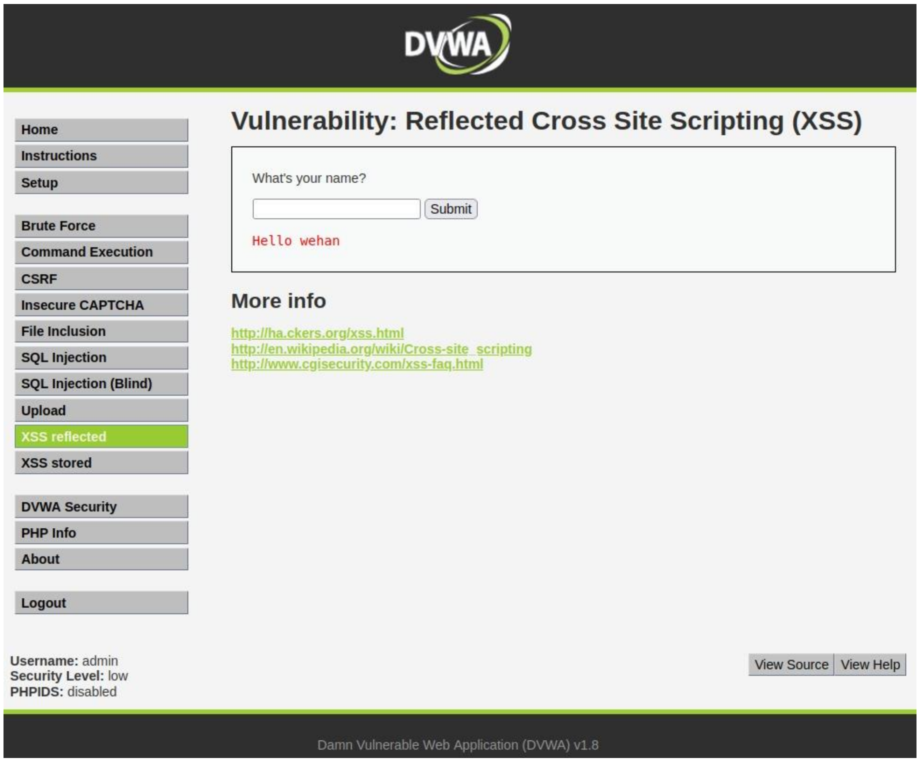
Figure B.2 - SQL Injection

ii. SQL Injection is a type of web application vulnerability where an attacker manipulates the SQL queries used in a web application through unauthorized means. The attacker can change the intended behavior of the SQL query and obtain unauthorized access to the underlying database by introducing malicious code into input fields or parameters. The integrity and confidentiality principles of cybersecurity are both broken by this security flaw. It affects the security of sensitive information by possibly exposing it to unauthorized parties, and it threatens the integrity of the data by permitting unauthorized updates to the database. (Kindy & Pathan, 2011)

iii. SQL Injection poses a significant threat as it can potentially expose an entire database. It is a significant security concern that is readily avoidable by taking the right steps. Without sufficient security, unlawful individuals might execute SQL queries to access confidential data kept in the database without authorization or alter it. In the conducted system test, it was observed that the shoe store website has been compromised through an SQL injection attack, leading to unauthorized access to user usernames and hashed passwords. In addition to endangering data integrity, this security lapse also breaches the user's personal data's confidentiality. Due to this vulnerability, there is a big chance that someone may compromise property owner information availability and violate confidentiality. To reduce the danger of SQL Injection and maintain the security of user data, website owners must implement rigorous safety precautions.

B.3 Cross Site Scripting (XSS)

i. The tester input the name, and the output was as follows.



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

```
Hello wehan
```

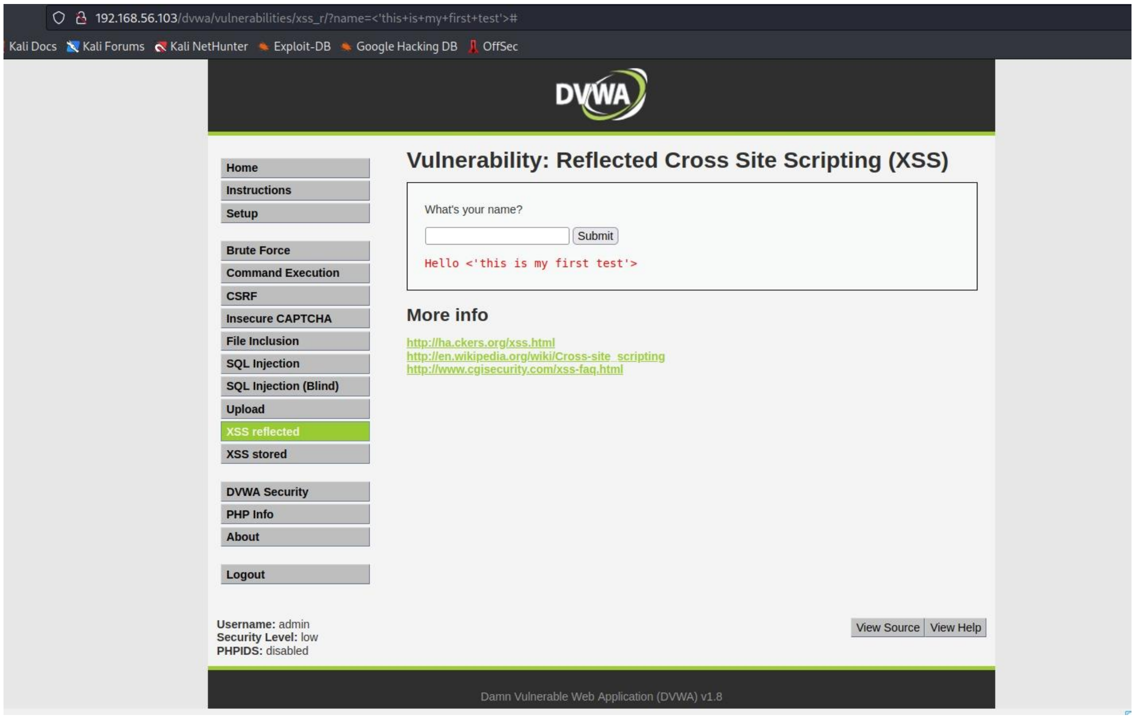
More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.8

Figure B.3 - Testing name



192.168.56.103/dvwa/vulnerabilities/xss_r/?name=<'this+is+my+first+test'>#

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

```
Hello <'this is my first test'>
```

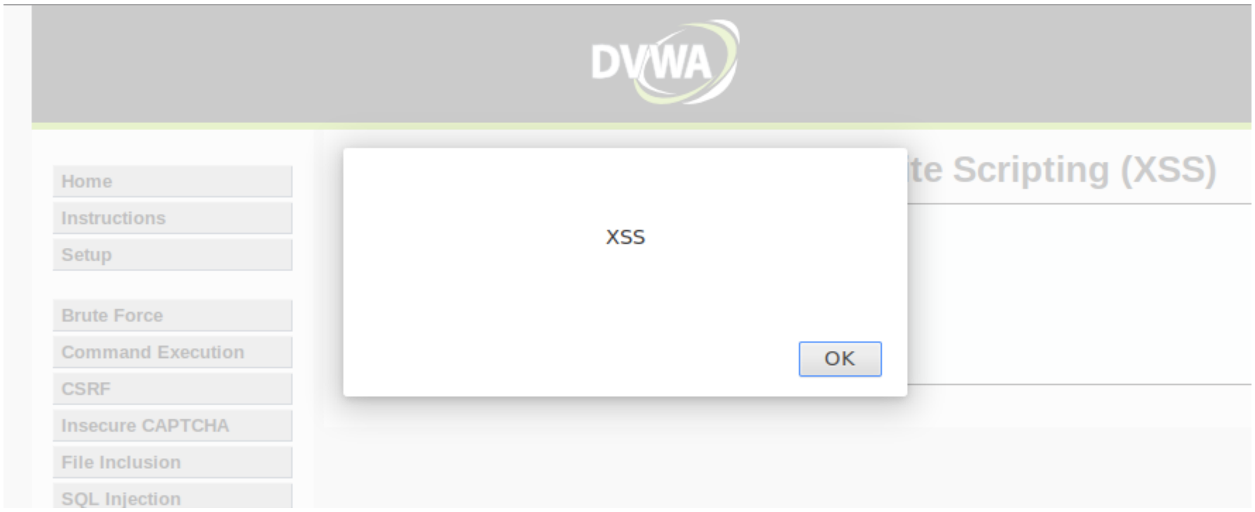
More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.8

Figure B.4 - Test XSS with HTML script



XSS

Figure B.5 - Testing

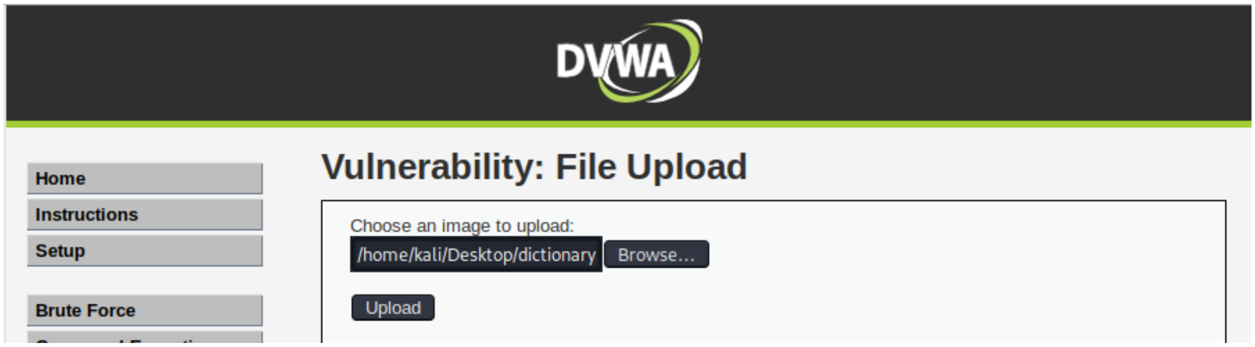
i. Cross-Site Scripting (XSS) assaults are a type of injection that takes place when an application lacks input validation or sanitization, which makes it possible for malicious code to be inserted. Once evaluated as a component of the original source code, this code alters the application's typical behavior while tricking unwary users into giving over their private information. Both the client and server sides of a website are vulnerable to XSS attacks. The security of user data is seriously threatened by this kind of assault since it may be used by attackers to steal personal data.

ii. **Scenario Assessment:** A phishing attempt on the shoe store website had collected consumers' login information, it was found during the checkup. Users were tricked into authenticating themselves using a fake login form by the attackers' deceitful methods. Users are exposed to possible financial and personal data breaches as a result of this harmful conduct, which also increases the danger of unauthorized access to their accounts. The website is also susceptible to stored XSS attacks, which can interfere with the regular operation of the page and display intrusive pop-ups, reducing user experience and perhaps posing more security problems.

B.4 Other vulnerabilities that can be exploited in OWASP.

i. File Upload

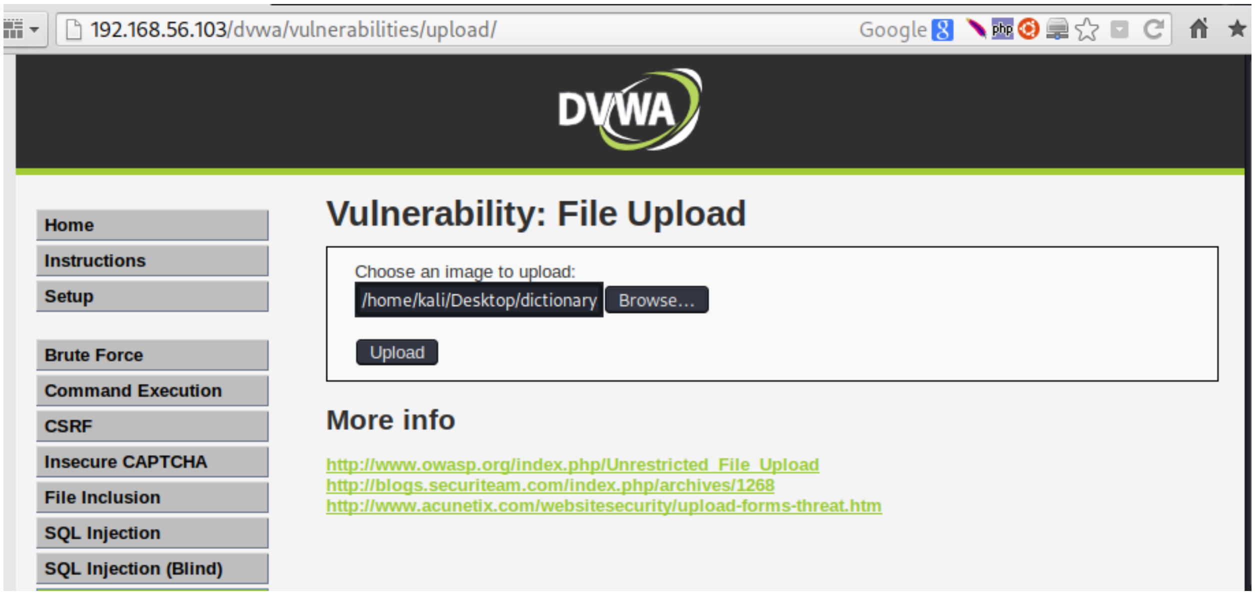
The provided code snippet provides an example of how to use a PHP file with a function to run system commands and launch the command prompt. Users can interact with the terminal and issue commands directly thanks to these capabilities.



Vulnerability: File Upload

Choose an image to upload: /home/kali/Desktop/dictionary

Figure B.6 - File Upload



192.168.56.103/dvwa/vulnerabilities/upload/

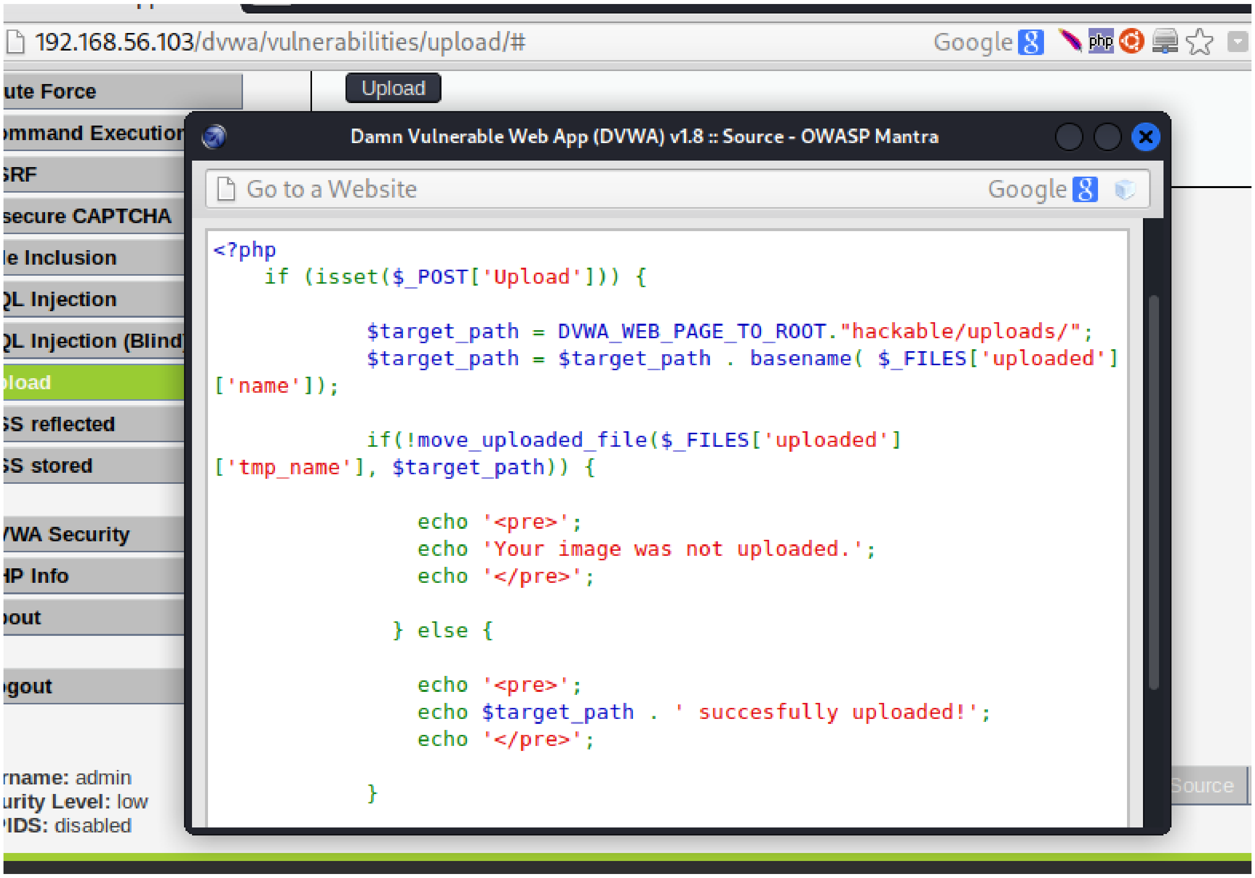
Vulnerability: File Upload

Choose an image to upload: /home/kali/Desktop/dictionary

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

Figure B.7 - Execution of the file upload vulnerability



192.168.56.103/dvwa/vulnerabilities/upload/#

Damn Vulnerable Web App (DVWA) v1.8 :: Source - OWASP Mantra

```
<?php
    if (isset($_POST['Upload'])) {

            $target_path = DVWA_WEB_PAGE_TO_ROOT."hackable/uploads/";
            $target_path = $target_path . basename( $_FILES['uploaded']
['name']);

            if(!move_uploaded_file($_FILES['uploaded']
['tmp_name'], $target_path)) {

                echo '<pre>';
                echo 'Your image was not uploaded.';
                echo '</pre>';

              } else {

                echo '<pre>';
                echo $target_path . ' succesfully uploaded!';
                echo '</pre>';

            }
```

rname: admin
urity Level: low
IDS: disabled

Figure B.8 - Command Execution

Both of these vulnerabilities have the capability of undermining all three principles of information security by taking over the system through shell access and increasing privileges based on the obtained information. The company may suffer large financial losses if the server that is hosting the program were to get hacked. This would allow attackers to modify current and past appointments and disrupt business operations across all branches.

ii. **Scenario Assessment:**

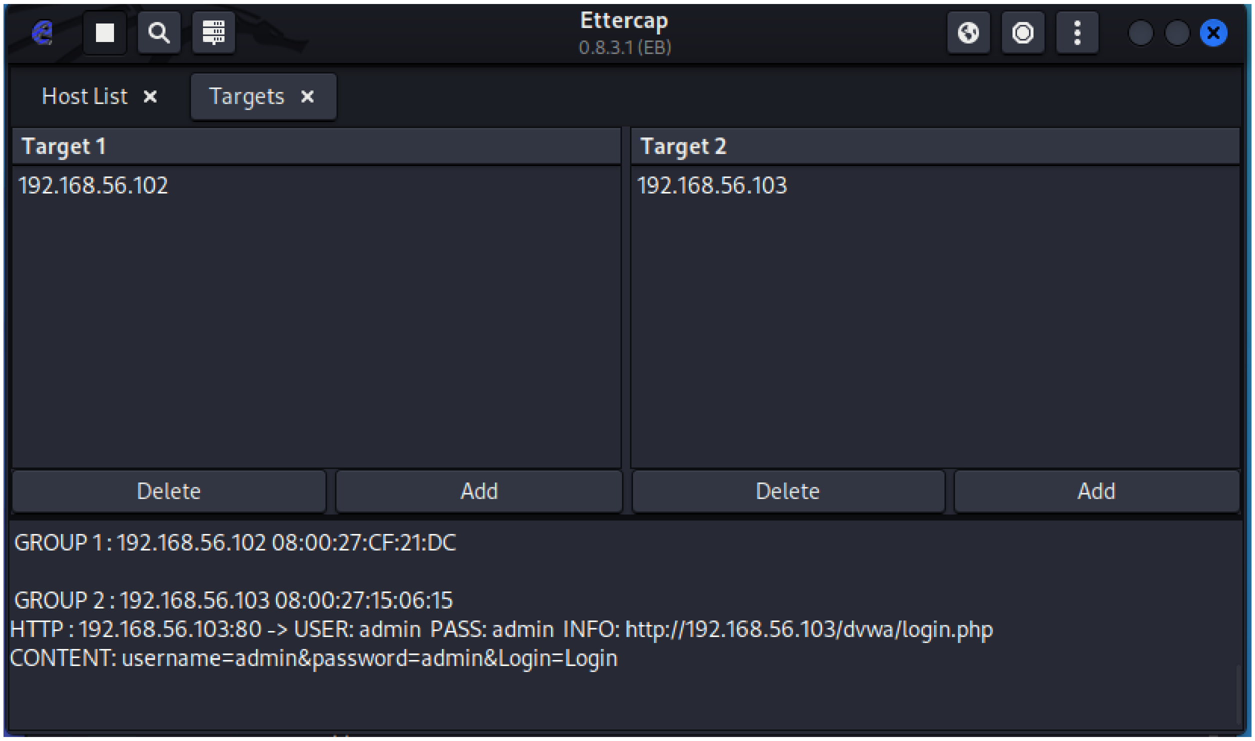
The shoe store website's command execution capabilities might be used to carry out operations like pinging an IP address. As a result, the shoe shop system may experience data breaches and illegal access to critical data. The capacity to upload files was a further vulnerability that was attacked. Figure B.4 illustrates the successful upload of an HTML file by an attacker to the website's database. This gives the attacker the opportunity to possibly upload harmful files to the shoe store system, resulting in data breaches or impeding access for both customers and staff.

C. Client-side exploits

C.1 Man in the Middle Attack (MiTM)

i. **ARP Spoofing with Ettercap**

During the login procedure of the shoe store's web application, an attacker has the capability to intercept and record different types of information using packet capturing tools such as Ettercap and Wireshark. This interception enables the attacker to obtain access to sensitive data that is being transmitted during the login process.



```
192.168.56.102
192.168.56.103
GROUP 1 : 192.168.56.102 08:00:27:CF:21:DC

GROUP 2 : 192.168.56.103 08:00:27:15:06:15
HTTP : 192.168.56.103:80 -> USER: admin  PASS: admin  INFO: http://192.168.56.103/dvwa/login.php
CONTENT: username=admin&password=admin&Login=Login
```

Figure C.1 - ARP Spoofing with Ettercap

Traffic Capturing with Wireshark

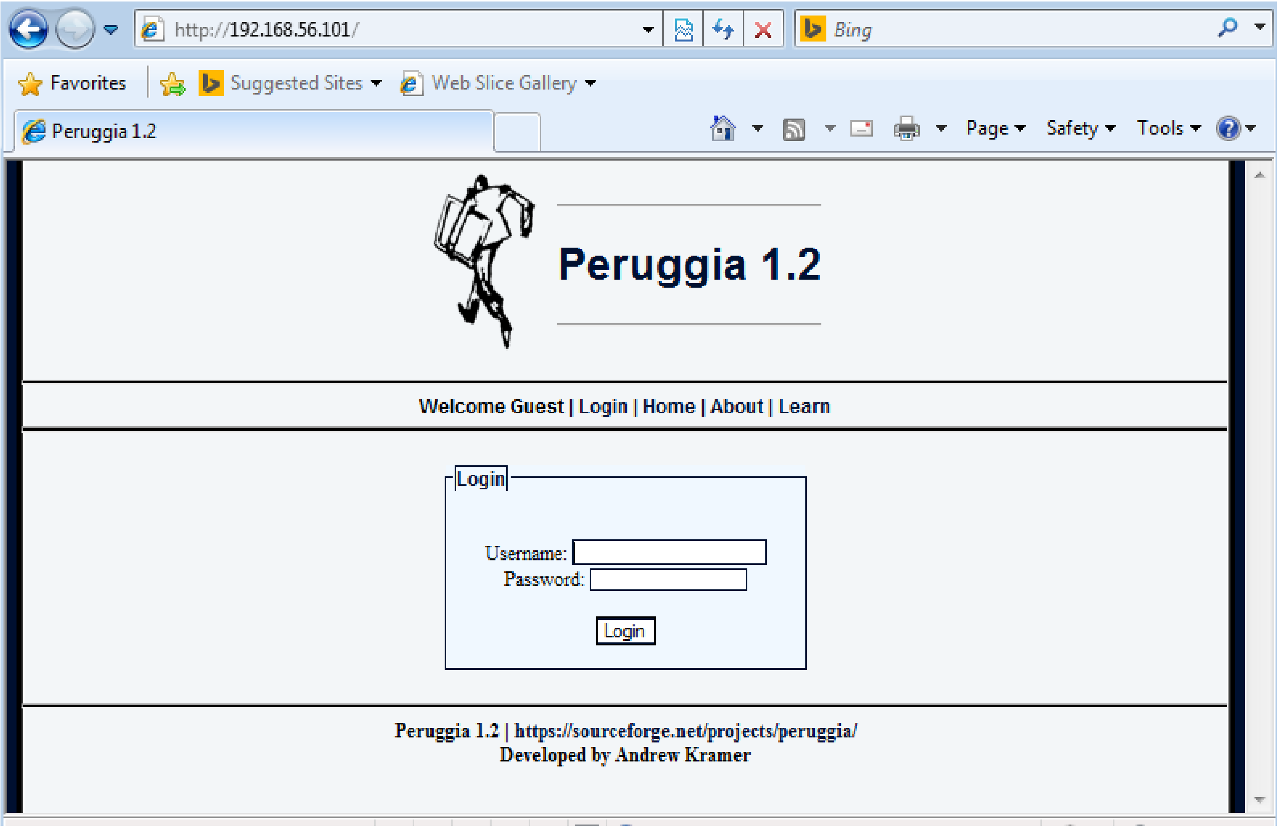
During the penetration test of the shoe store's web application, additional information beyond user credentials was examined, including customer's personal details and property owner's financial information. Wireshark, a network packet capturing tool, was utilized to monitor all network traffic on the "eth0" interface. As shown in Figure C.2, the tester successfully intercepted the HTTP requests and collected all packets when the victim signed into the system via the login page, giving him access to the victim's passwords and other crucial data.

ii. **Scenario Assessment**:

A Man-in-the-between (MitM) attack involves the attacker placing their computer in the between of two target devices, such as a client and a server, in order to intercept and filter their communications. In this approach, the attacker essentially serves as the man-in-the-middle by gaining access to all data transmitted between the targets and hijacking the session. A MitM attack has serious repercussions since it gives attackers access to private information and gives them the ability to control the information being transmitted. The security and privacy of the shoe store's customers' personal and financial information would be jeopardized if a MitM attack were to take place on the website. Sensitive information like social security numbers and credit card numbers might be obtained in this way, resulting in a serious data breach.

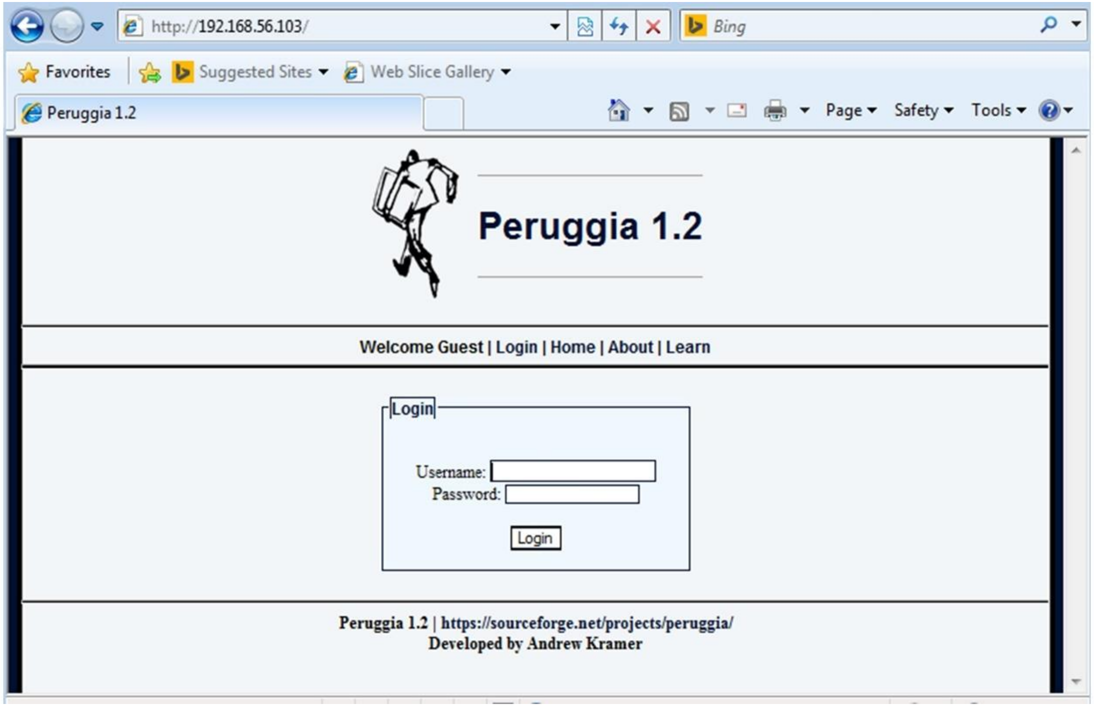
C.2 Social Engineering Attack

i.



Peruggia 1.2 | https://sourceforge.net/projects/peruggia/
Developed by Andrew Kramer

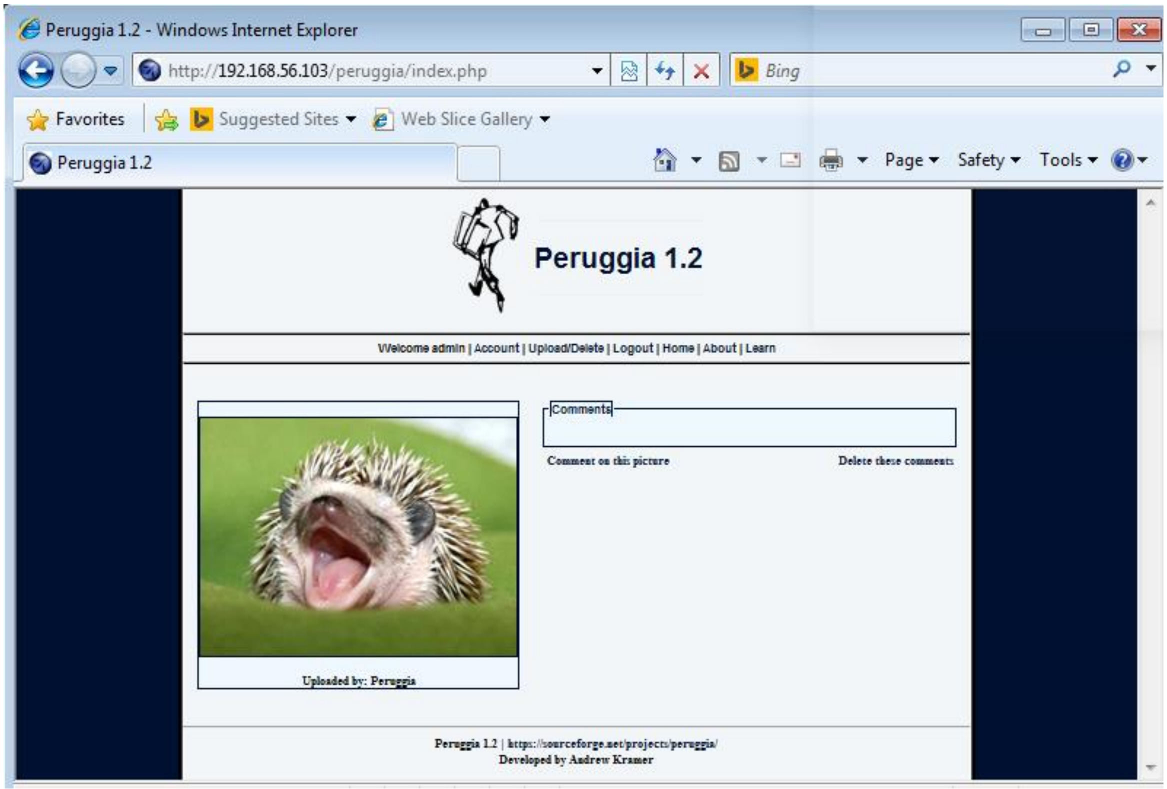
Figure C.2 - Reference page for cloning in the Social Engineering Attack



Peruggia 1.2 | https://sourceforge.net/projects/peruggia/
Developed by Andrew Kramer

Figure C.3 - cloned page for the Social Engineering Attack

Once the cloned site is successfully hosted on the attacker's server, they can employ techniques like ARP poisoning to deceive the user's machine into believing it is communicating with the legitimate server. The attacker can intercept and collect the user's requested data by enticing the user to log in via the cloned site. They can then send the user back to the original website while still giving them access to the data they had previously collected.


Peruggia 1.2 - Windows Internet Explorer
http://192.168.56.103/peruggia/index.php
Bing
Favorites
Suggested Sites
Web Slice Gallery
Peruggia 1.2
Page
Safety
Tools

Peruggia 1.2

Welcome admin | Account | Upload/Delete | Logout | Home | About | Learn

Comments

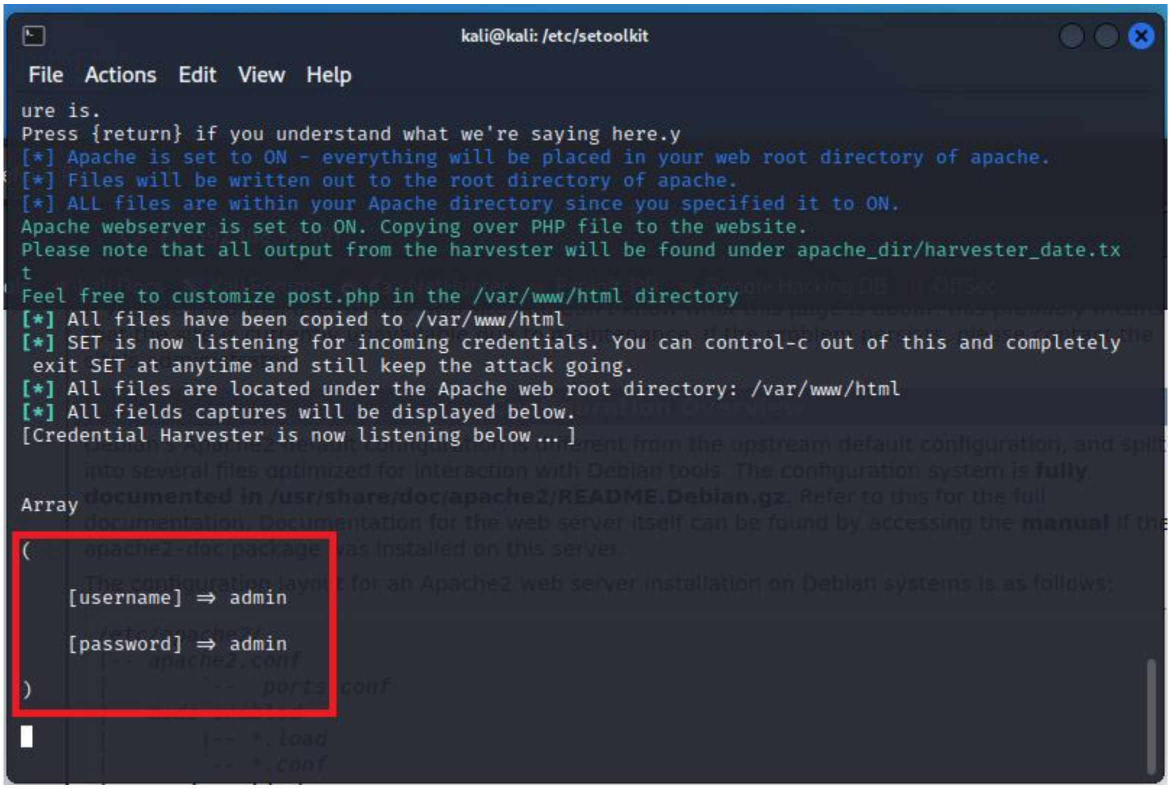
Comment on this picture

Delete these comments

Uploaded by: Peruggia

Peruggia 1.2 | https://sourceforge.net/projects/peruggia/
Developed by Andrew Kramer

Figure C.4 - After login to the cloned site



```
ure is.
Press {return} if you understand what we're saying here.y
[*] 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.tx
t
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...]

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

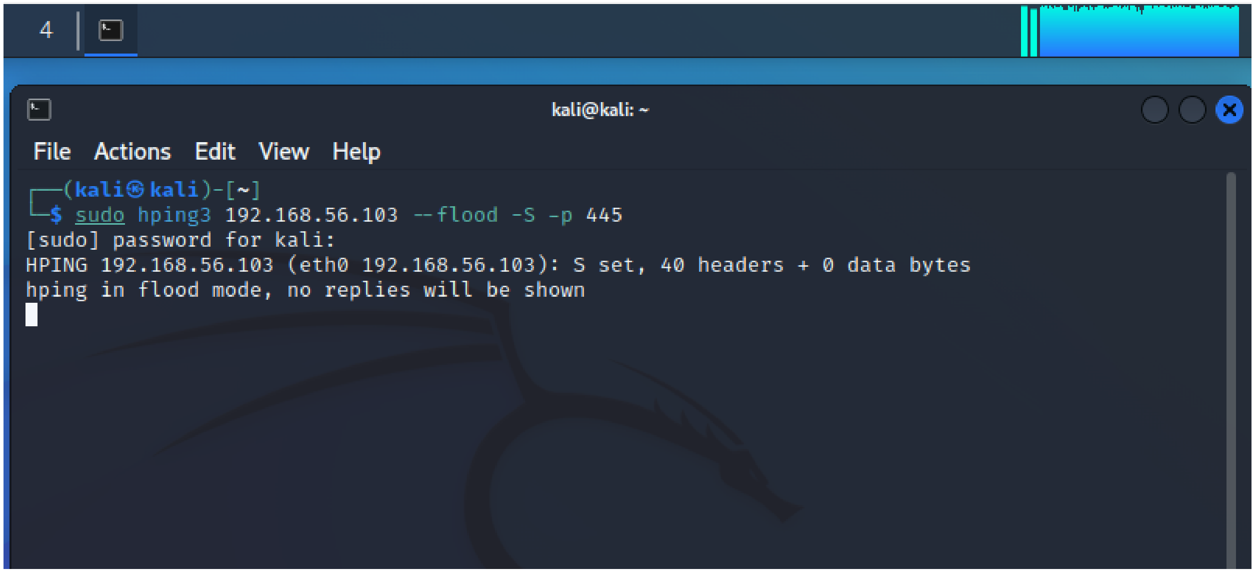
Figure C.5 - Capture password using cloned site

ii. **Scenario assessment:** This sophisticated attack method exploits psychological techniques rather than relying on specific devices, allowing malicious actors to gather or manipulate information with potentially severe consequences. In our scenario, the attacker built a fake URL to trick the victim after cloning the shoe store's login page on their own computer. The attacker grabs the data and gets unauthorized access when the victim inputs their credentials on the cloned page. The victim is then redirected to the original login page, remaining unaware of the phishing attack. This method can be used to obtain sensitive information like credit card details and personal information. As the shoe store's system contains valuable data, such an attack would put the customers at risk of data theft.

D. Denial of Service attacks

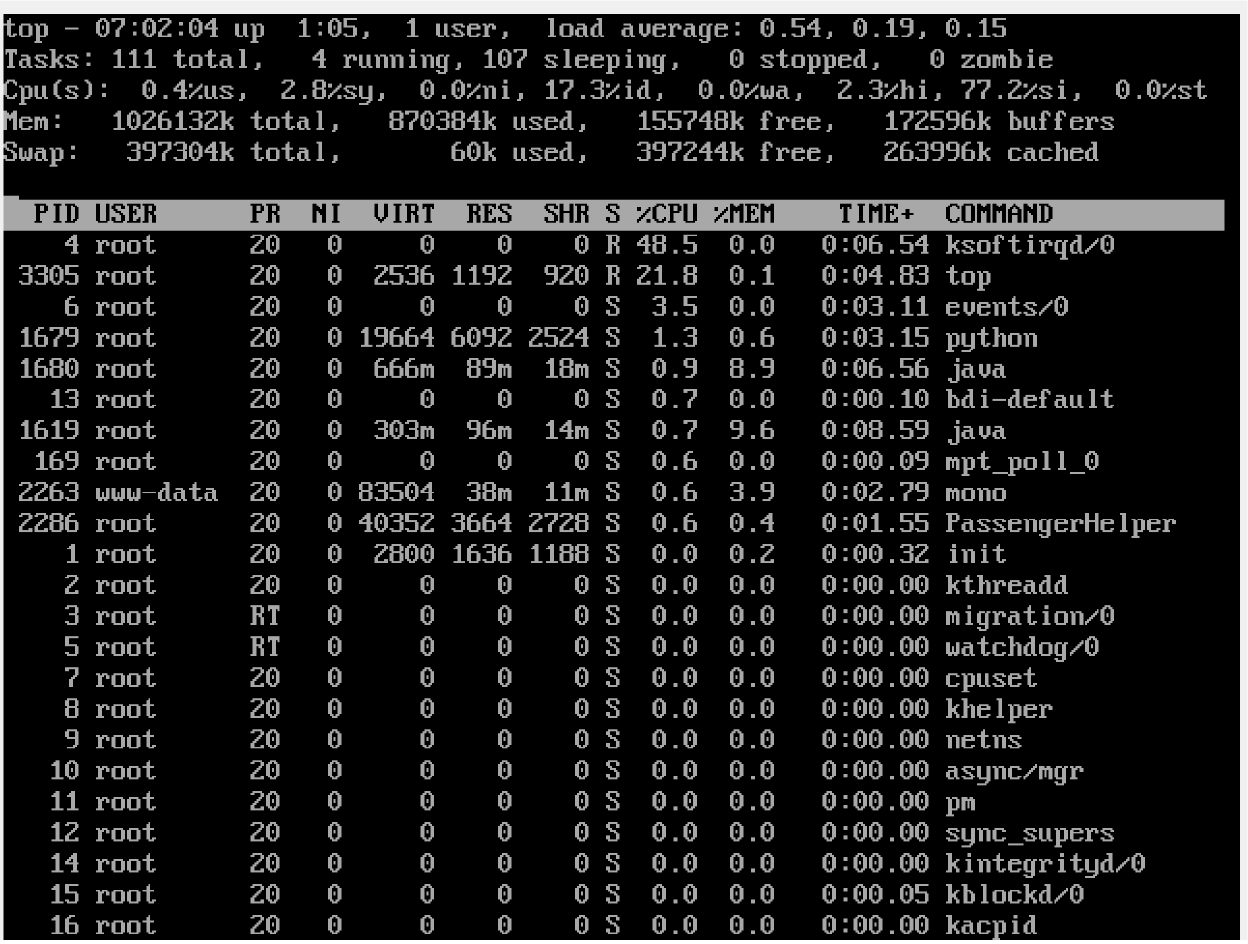
D.1 DoS the web server

i.



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 192.168.56.103 --flood -S -p 445
[sudo] password for kali:
HPING 192.168.56.103 (eth0 192.168.56.103): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Figure D.1 - Dos Attack



```
top - 07:02:04 up  1:05,  1 user,  load average: 0.54, 0.19, 0.15
Tasks: 111 total,   4 running, 107 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.4%us,  2.8%sy,  0.0%ni, 17.3%id,  0.0%wa,  2.3%hi, 77.2%si,  0.0%st
Mem:   1026132k total,   870384k used,   155748k free,   172596k buffers
Swap:   397304k total,       60k used,   397244k free,   263996k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    4 root      20   0     0    0    0 R 48.5  0.0   0:06.54 ksoftirqd/0
 3305 root      20   0  2536 1192  920 R 21.8  0.1   0:04.83 top
    6 root      20   0     0    0    0 S  3.5  0.0   0:03.11 events/0
 1679 root      20   0 19664 6092 2524 S  1.3  0.6   0:03.15 python
 1680 root      20   0  666m  89m  18m S  0.9  8.9   0:06.56 java
   13 root      20   0     0    0    0 S  0.7  0.0   0:00.10 bdi-default
 1619 root      20   0  303m  96m  14m S  0.7  9.6   0:08.59 java
  169 root      20   0     0    0    0 S  0.6  0.0   0:00.09 mpt_poll_0
 2263 www-data  20   0 83504  38m  11m S  0.6  3.9   0:02.79 mono
 2286 root      20   0 40352 3664 2728 S  0.6  0.4   0:01.55 PassengerHelper
    1 root      20   0  2800 1636 1188 S  0.0  0.2   0:00.32 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 migration/0
    5 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 watchdog/0
    7 root      20   0     0    0    0 S  0.0  0.0   0:00.00 cpuset
    8 root      20   0     0    0    0 S  0.0  0.0   0:00.00 khelper
    9 root      20   0     0    0    0 S  0.0  0.0   0:00.00 netns
   10 root      20   0     0    0    0 S  0.0  0.0   0:00.00 async/mgr
   11 root      20   0     0    0    0 S  0.0  0.0   0:00.00 pm
   12 root      20   0     0    0    0 S  0.0  0.0   0:00.00 sync_supers
   14 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kintegrityd/0
   15 root      20   0     0    0    0 S  0.0  0.0   0:00.05 kblockd/0
   16 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kacpid
```

Figure D.2 - Dos Output

ii. The availability tenet is compromised as the server experiences gradual slowdown until it eventually becomes unresponsive.

iii. **Scenario assessment:** Customers and staff would be significantly impacted in the case of the online shoe business if a system flaw resulted on the website being shut down. Customers wouldn't be able to explore and buy shoes on the Internet, resulting in lost sales and disgruntled customers. Employees' ability to handle orders and deliver compelling customer service would be hampered by their inability to access the system's current data or add new goods to the inventory. The online shoe company may suffer considerable financial losses due to this service outage, which might also harm its reputation in the cutthroat industry.

E. Recommendations to protect the scenario company server

E.1 Minimizing reconnaissance threats

The services using open ports must be continuously checked and assessed to reduce reconnaissance concerns. Conducting timely port scans and evaluating the service versions are essential for penetration testers. Vulnerabilities can then be found and swiftly fixed as a result. It is recommended to discontinue any services that are no longer required or relevant. Additionally, it is strongly advised to keep the services updated with the most recent patches and updates as this helps avoid the exploitation of known vulnerabilities. By taking these proactive steps, you dramatically lower the possibility of reconnaissance attacks and improve the system's overall security.

E.2 Port Knocking

Port knocking is a security mechanism that safeguards ports from unauthorized access and port scans. Only authorized users can access the firewall's ports because they must make a precise sequence of connection requests because they are closed by default. The firewall dynamically opens the required port for the authorized user when the proper sequence is identified. In this scenario, implementing port knocking in addition to the current firewall can successfully stop unwanted exposing of all accessible ports and their details. By restricting access to people who are aware of the precise connection sequence, this strategy improves system security by preventing unwanted access attempts and reducing the dangers involved with reconnaissance operations.

E.3 Prevent SQL Injection

There are several ways to prevent SQL attacks. The most crucial step to prevent SQL injection attacks is to ensure thorough input escaping and sanitization for all input fields in the application. This measure is of utmost importance since it addresses the main vulnerability that allows SQLi attacks to occur. Instead of dynamically creating SQL queries by concatenating user input, it is strongly advised to utilize parameterized queries or prepared statements to minimize SQL injection threats. By ensuring a distinct boundary between the SQL code and user input, this method successfully prevents harmful input from being mistakenly perceived as a query. By employing parameterized queries, the danger of SQL injection vulnerabilities is considerably decreased since the input values are treated as parameters rather than being directly contained in the query.(*What Is SQL Injection (SQLi) and How to Prevent Attacks*, n.d.)

E.4 Protection from XSS

Mitigating Cross-Site Scripting (XSS) attacks requires a multi-layered approach to ensure the security of web applications. Implementing stringent input validation and sanitization procedures, where user-supplied data is carefully examined and filtered to eliminate any potentially harmful script material, is one of the major security measures. This stops dangerous code from being injected into the program. Before showing output to consumers, it is crucial to adequately encode it. The danger of running injected scripts is considerably decreased by employing output encoding techniques, such as HTML entity encoding or using secure output encoding routines. This guarantees that user-generated material is presented safely without endangering the application's integrity.

E.5 Avoiding man in the middle attacks

Implement secure protocols like HTTPS with SSL certificates for login, financial transaction, and personal information-related activities to mitigate the recently revealed vulnerability of plain text transfer for user login credentials. Furthermore, installing strong intrusion detection systems and strengthening firewall policies can assist identify and stop illegal access attempts and improve overall security. These precautions guarantee data privacy, reduce the chance of being intercepted, and strengthen the system against potential flaws.(*Man in the Middle (MITM) Attacks, Definition, and Types | Rapid7*, n.d.)

E.6 Avoiding social engineering attacks in a company

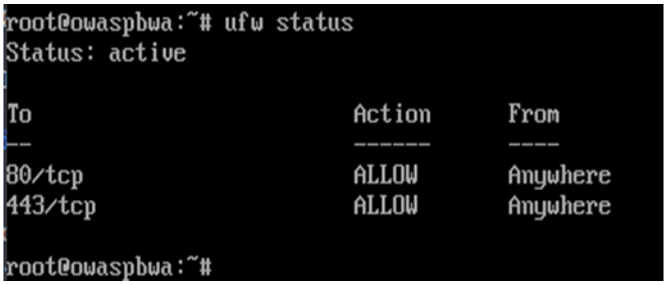
One of the most effective ways to mitigate social engineering attacks is through the implementation of multi-factor authentication. Even if an attacker succeeds in obtaining login credentials, they will still require physical access to a secure key or another authentication element in order to enter the system because various kinds of verification are used. Additionally, teaching people about social engineering assaults and spreading awareness of them may be quite successful. Users can learn to identify and respond to possible risks by conducting practice sessions and attending instructive presentations. The use of anti-phishing software adds another layer of defense against phishing efforts by scanning visited websites for harmful client-side code. Together, these steps greatly improve security and lower the possibility of successful social engineering assaults.

E.7 Protecting the company from DoS attack

Implementing rate limitation and using a content delivery network (CDN) are two practical ways to defend online services from Denial-of-Service (DoS) attacks. Rate restriction prevents resource misuse and overload by capping the number of requests coming from one source in a certain period of time. Legitimate users can use the service while malevolent actors are stopped by setting realistic thresholds. By dividing the load over several servers and regions, a CDN enables a service's content be distributed, reducing the impact of DoS assaults. This strategy makes sure that the service is always available and operates at its best, even while under assault. Web services may considerably improve their resistance against possible DoS threats by putting these safeguards into place alongside other security procedures.(*How to Prevent DDoS Attacks: 7 Tried-and-Tested Methods*, n.d.)

E.8 Intrusion detection and prevention

i. Firewall and iptables rules



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

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

root@owaspbwa:~#
```

Figure E.1 - Uncomplicated Firewall

ii. Iptables is a strong firewall program that offers sophisticated features for configuring security rules and settings at the kernel level. Alternatively, UFW is a streamlined firewall system built on top of Iptables that makes it simpler to administer security rules and regulate IP addresses and ports. Considering that the shoe store system handles sensitive data that requires strong security measures, it would be preferable to choose Iptables for setting up the firewall. Its advanced features can provide better protection and customization options to safeguard the shoe store's data and network.

iii. The table provides an overview of the distinctions between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). It outlines the key differences in their functionalities and capabilities.

Intrusion Detection System (IDS)	Intrusion Prevention System (IPS)
The system does not take the necessary actions on its own.	The system takes the actions on its own.
This technique of monitoring and surveillance can spot potential threats.	This is a control mechanism that reacts to potential threats.
IDS offers greater flexibility in terms of monitoring and analysis as it focuses on gathering information for security professionals to investigate and respond	IPS is more rigid in its predefined rules and actions for immediate prevention.
IDS may generate false positive alerts, where benign activities are flagged as potential threats.	IPS aims to minimize false positives by employing advanced detection and prevention mechanisms.

iv. In the case of the online shoe store, the web application may keep sensitive financial information and private client data in its database. Measures should be put in place to stop SQL Injection attacks through the HTTP services to guarantee the security of the system. By using privilege filtering to limit unwanted access, establishing SQL server firewalling, and adhering to safe coding guidelines, this may be accomplished. Furthermore, it's critical to take precautions against spoofing attacks like IP address, ARP, and DNS server spoofing, which hackers may employ to steal sensitive data. Implementing the Transport Layer Security (TLS) and HTTP Secure (HTTPS) protocols can help to reduce these dangers. In order to protect the confidentiality and integrity of the sent data, these protocols encrypt data while it is being transmitted and offer authentication techniques. The shoe online business may better secure the privacy and financial information of its customers by putting these security measures in place.

References

Glassman, M., & Kang, M. J. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*, *28*(2), 673–682. https://doi.org/10.1016/J.CHB.2011.11.014

How to Prevent DDoS Attacks: 7 Tried-and-Tested Methods. (n.d.). Retrieved May 16, 2023, from https://phoenixnap.com/blog/prevent-ddos-attacks

Huang, D. W., Liu, W., & Bi, J. (2021). Data tampering attacks diagnosis in dynamic wireless sensor networks. *Computer Communications*, *172*, 84–92. https://doi.org/10.1016/j.comcom.2021.03.007

D. A. Kindy and A. -S. K. Pathan, "A survey on SQL injection: Vulnerabilities, attacks, and prevention techniques," 2011 IEEE 15th International Symposium on Consumer Electronics (ISCE), Singapore, 2011, pp. 468-471, doi: 10.1109/ISCE.2011.5973873.

Man in the Middle (MITM) Attacks, Definition, and Types | Rapid7. (n.d.). Retrieved May 15, 2023, from https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/

Mastering Kali Linux for Advanced Penetration Testing - Vijay Kumar Velu - Google Books. (n.d.). Retrieved May 16, 2023, from https://books.google.lk/books?hl=en&lr=&id=JHg5DwAAQBAJ&oi=fnd&pg=PP1&dq=nmap+using+in+OSINT+Activities&ots=ltvrrLuiZR&sig=8-kMtU3Lc-WYFZ8x_48_gQCilgs&redir_esc=y#v=onepage&q&f=false

Mastering Kali Linux for Advanced Penetration Testing: Secure your network ... - Vijay Kumar Velu, Robert Beggs - Google Books. (n.d.). Retrieved May 16, 2023, from https://books.google.lk/books?hl=en&lr=&id=kQGGDwAAQBAJ&oi=fnd&pg=PP1&dq=harvester+using+in+OSINT+Activities&ots=N0yJx-83Bh&sig=j32ha7Jvap8qAzgnTid_1-5uqj0&redir_esc=y#v=onepage&q&f=false

Richter, M., Schwarz, K., & Creutzburg, R. (2021). Conception and implementation of professional laboratory exercises in the field of ICS/SCADA security part II: Red teaming and blue teaming. *IS and T International Symposium on Electronic Imaging Science and Technology*, *2021*(3). https://doi.org/10.2352/ISSN.2470-1173.2021.3.MOBMU-074

What is SQL Injection (SQLi) and How to Prevent Attacks. (n.d.). Retrieved May 15, 2023, from https://www.acunetix.com/websitesecurity/sql-injection/

Turner, P., n.d. What Are Your SSH Security Risks? [How Secure is SSH] | Venafi [WWW Document]. URL https://www.venafi.com/blog/best-practices-ssh-key-management-what-areyour-ssh security-risks (accessed 4.24.22).

cloudflare (n.d.e), 'What is transport layer security? | tls protocol | cloudflare', https://www.cloudflare.com/en-gb/learning/ssl/transport-layer-security-tls/. (Accessed on 04/27/2022).