



INFORMATICS
INSTITUTE OF
TECHNOLOGY

UNIVERSITY OF
WESTMINSTER 

Informatics Institute of Technology

Department of Computing

Module: 6COSC019C Cyber Security

Coursework

Scenario-Based Lab Report

Module Leader: Saman Hettiarachchi

UoW ID - Student ID	Student Name
W1761767 - 2018130	Luqman Rumaiz

Table of Contents

Table of Contents.....	2
List of Abbreviations.....	4
Scenario.....	5
Chapter A: Information Gathering.....	6
A.1: OSINT Activities.....	6
A.1.1: Examples of OSINT Investigation.....	6
A.1.1.1: WHOIS.....	6
A.1.1.2: dnsenum.....	7
A.1.1.3: theHarvester.....	9
A.1.2: How effective is OSINT and why is it important to do when starting a Penetration Test.....	10
A.1.3: Scenario Assessment.....	10
A.2: Reconnaissance.....	12
A.2.1: Testing Web Applications in Lab.....	12
A.2.1.1: WackoPicko.....	12
A.2.1.2: robots.txt.....	13
A.2.1.3: dirbuster.....	14
A.2.2: Scenario Assessment.....	16
A.3: Port Scanning and Enumeration.....	17
A.3.1: Identified Ports.....	17
A.3.2: What is an open port and what threats can it potentially pose?.....	18
A.3.3: Assessing the Threats for each Open Port.....	18
Chapter B: Server-side Exploits.....	20
B.1: Data Tampering.....	20
B.1.1: Attempting to tamper data in Login.....	20
B.1.2: What is Data Tampering?.....	21
B.1.3: Scenario Assessment.....	21
B.2: SQL Injection.....	22

B.2.1: Attempting SQL Injection on Database.....	22
B.2.2: What is SQL Injection?.....	22
B.2.3: Scenario Assessment.....	23
B.3: XSS Scripting.....	24
B.3.1: Attempting XSS Scripting Injection with Form.....	24
B.3.2: What is XSS Scripting?.....	25
B.3.3: Scenario Assessment.....	25
B.4: Additional Vulnerabilities.....	26
B.4.1: Attempts to exploit Additional Vulnerabilities.....	26
B.4.1.1: Buffer Overflow Attack.....	26
B.4.1.2: File Inclusion.....	27
B.4.2: Scenario Assessment.....	28
Chapter C: Client-side Exploits.....	29
C.1: Man in the Middle Attack.....	29
C.1.1: Ettercap.....	29
C.1.2: Scenario Assessment.....	29
C.2: Social Engineering Attack.....	30
C.2.1: Examples of Social Engineering Attack.....	30
C.2.2.1: Social-Engineer Toolkit.....	30
C.2.2.2: Phishing Site.....	31
C.2.2: Scenario Assessment.....	32
Chapter D: Denial of Service Attacks.....	33
D.1: DoS Attack.....	33
D.1.1: Examples of DoS Attacks.....	33
D.1.1.1: TCP SYN Flood.....	33
D.1.1.2: Smurf DoS Attack.....	34
D.2: What Tenant does DoS violate?.....	34
D.3: Scenario Assessment.....	34
Chapter E: Recommendations to Solve Vulnerabilities.....	36

E.1: Mitigation for A.2.....	36
E.2: Mitigation for A.3.....	36
E.3: Mitigation for B.2.....	37
E.4: Mitigation for B.3.....	37
E.5: Mitigation for C.1.....	37
E.6: Mitigation for C.2.....	37
E.7: Mitigation for D.1.....	38
E.8: Intrusion Detection and Prevention Systems.....	38
E.8.1: Examples of firewall and iptable Rules.....	38
E.8.2: Which Firewall Tool should the Company use?.....	38
E.8.3: What are the differences between an Intrusion Detection System and an Intrusion Prevention System?.....	38
E.8.4: Scenario Assessment.....	39
Bibliography.....	40

List of Abbreviations

OSINT - *Open Source Intelligence*

IP - *Internet Protocol*

DNS - *Domain Name System*

SQL - *Structured Query Language*

XSS - *Cross Site Scripting*

LFI - *Local File Infusion*

MitM- *Man in The Middle*

HTTP - *HyperText Transfer Protocol*

HTTPS - *HyperText Transfer Protocol Secure*

TSL - *Transport Layer Security,*

SSL - *Secure Sockets Layer*

IDS - *Intrusion Detection System*

IPS - *Intrusion Prevention System*

Scenario

My company was recently hired to perform a penetration test on a **medium-size IT startup based** in Sri Lanka, the startup has a **few branches** in parts of Central Asia. The website that we have been required to test is one of their HR management applications that allow the company to store and track information and performance for employees in the company, employees also have the ability to view their information and request appraisals. **Personal information** of the **staff** is stored in the website such as their address, phone number, date of birth and likewise. Employees who work in the HR department and the CEO have roles in the website to **view and manage the information and appraisals** of all employees in the company, the **credentials of the CEO, HR staff** and other employees are stored on a database separate from the database that stores employee information.

Chapter A: Information Gathering

A.1: OSINT Activities

A.1.1: Examples of OSINT Investigation

A.1.1.1: WHOIS

The author conducted an OSINT activity by executing a WHOIS lookup on the HR management system.

```
whois cwscenario.site

(kali㉿kali)-[~]
$ whois cwscenario.site

Domain Name: CWSCENARIO.SITE
Registry Domain ID: D268362727-CNIC
Registrar WHOIS Server: whois.ionos.com
Registrar URL: https://ionos.com
Updated Date: 2023-01-01T05:34:42.0Z
Creation Date: 2022-01-07T10:56:28.0Z
Registry Expiry Date: 2024-01-07T23:59:59.0Z
Registrar: IONOS SE
Registrar IANA ID: 83
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant Organization: 1&1 Internet Limited
Registrant State/Province: GLS
Registrant Country: GB
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for each contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for each contact of the queried domain name.
Name Server: NS1032.UI-DNS.DE
Name Server: NS1108.UI-DNS.ORG
Name Server: NS1115.UI-DNS.BIZ
Name Server: NS1093.UI-DNS.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for Tech contact of the queried domain name.
Registrar Abuse Contact Email: abuse@ionos.com
Registrar Abuse Contact Phone:
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-05-13T14:02:21.0Z <<<
```

The WHOIS information for the domain `cwscenario.site` reveals its creation on **2022-01-07** and expiration on **2024-01-07**, and that the domain was registered with IONOS SE. Several name servers were found, also it is noted that the registrant's email, as well as the admin and tech contacts, are hidden from public view, likely to reduce the risk of phishing attacks. Additionally, the domain has several status codes (**clientTransferProhibited**, **clientUpdateProhibited**, **clientDeleteProhibited**) which restrict certain actions.

A.1.1.2: dnsenum

In order to obtain a comprehensive overview of the domain infrastructure of the site, the author conducted a background check and then proceeded to investigate the associated servers. This enabled the identification of potential vulnerability points.

```
dnsenum --enum cwscenario.site
```

```
(kali㉿kali)-[~]
$ dnsenum --enum cwscenario.site

dnsenum VERSION:1.2.6

-----  cwscenario.site  -----
DNS System

Host's addresses:
-----
cwscenario.site.                3600      IN      A       217.160.0.219

Name Servers:
-----
ns1032.ui-dns.de.              152096    IN      A       217.160.80.32
ns1093.ui-dns.com.             241606    IN      A       217.160.82.93
ns1108.ui-dns.org.             151141    IN      A       217.160.83.108
ns1115.ui-dns.biz.             161767    IN      A       217.160.81.115

Mail (MX) Servers:
-----
mx00.ionos.co.uk.              68805     IN      A       212.227.15.41
mx01.ionos.co.uk.              81338     IN      A       217.72.192.67

Trying Zone Transfers and getting Bind Versions:
-----

Trying Zone Transfer for cwscenario.site on ns1093.ui-dns.com ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for cwscenario.site on ns1115.ui-dns.biz ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for cwscenario.site on ns1108.ui-dns.org ...
AXFR record query failed: NOTAUTH
```



```
Trying Zone Transfer for cwscenario.site on ns1032.ui-dns.de ...
AXFR record query failed: NOTAUTH

Scraping cwscenario.site subdomains from Google:
-----

      Google search page: 1

Google Results:
-----

perhaps Google is blocking our queries.
Check manually.

Brute forcing with /usr/share/dnsenum/dns.txt:
-----

www.cwscenario.site.          721      IN      A      217.160.0.219

Launching Whois Queries:
-----

whois ip result:  217.160.0.0      →      217.160.0.0/23

cwscenario.site
217.160.0.0/23

Performing reverse lookup on 512 ip addresses:
-----

0 results out of 512 IP addresses.

cwscenario.site ip blocks:
-----

done.
```

Through DNS Enumeration, the author was able to obtain essential information, such as the IP address of the server, as well as the IP addresses of the domain's mail servers. Additionally, all attempts at a zone transfer were denied, demonstrating good security measures to prevent unauthorised users from getting a copy of the entire DNS zone.

A.1.1.3: theHarvester

The author utilised a tool known as theHarvester to collect publicly available data related to the HR system domain. The below command instructed the tool to search all available sources for information related to the domain.

```
theHarvester -d cwscenario.site -b all
```

```
[*] ASNS found: 1
AS8560

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

[*] No Twitter users found.

[*] LinkedIn Users found: 5
Your search

[*] LinkedIn Links found: 0
Your search

[*] No Trello URLs found.

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

[*] No emails found.

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

A.1.2: How effective is OSINT and why is it important to do when starting a Penetration Test

OSINT is an essential and effective component of penetration testing, in which data that is legally and freely accessible to the public is collected and analysed to inform and direct further steps in the process. OSINT data gathering is a vital part of assessing the security of a system (Kelleher, 2020).

A.1.3: Scenario Assessment

Data Collected	Information
A.1.1	
Domain Name	CWSCENARIO.SITE
Creation Date	2022-01-07
Expiry Date	2024-01-07
Registrar	IONOS SE
Name Servers	NS1032.UI-DNS.DE, NS1108.UI-DNS.ORG, NS1115.UI-DNS.BIZ, NS1093.UI-DNS.COM
A.1.2	
IP Address	217.160.0.219
Mail Servers	mx00.ionos.co.uk (212.227.15.41), mx01.ionos.co.uk (217.72.192.67)
DNS Zone Transfer	Not Authorised
A.1.3	
IPs Found	50.87.192.155, 217.160.0.219, 2001:8d8:100f:f000::2b6
LinkedIn Users	5 (Data not revealed)
Hosts Found	autodiscover.cwscenario.site, cpanel.cwscenario.site, cpcalendars.cwscenario.site, cpcontacts.cwscenario.site, mail.cwscenario.site, webdisk.cwscenario.site,

	webmail.cwscenario.site, www.cwscenario.site
--	-------------------------------------------------

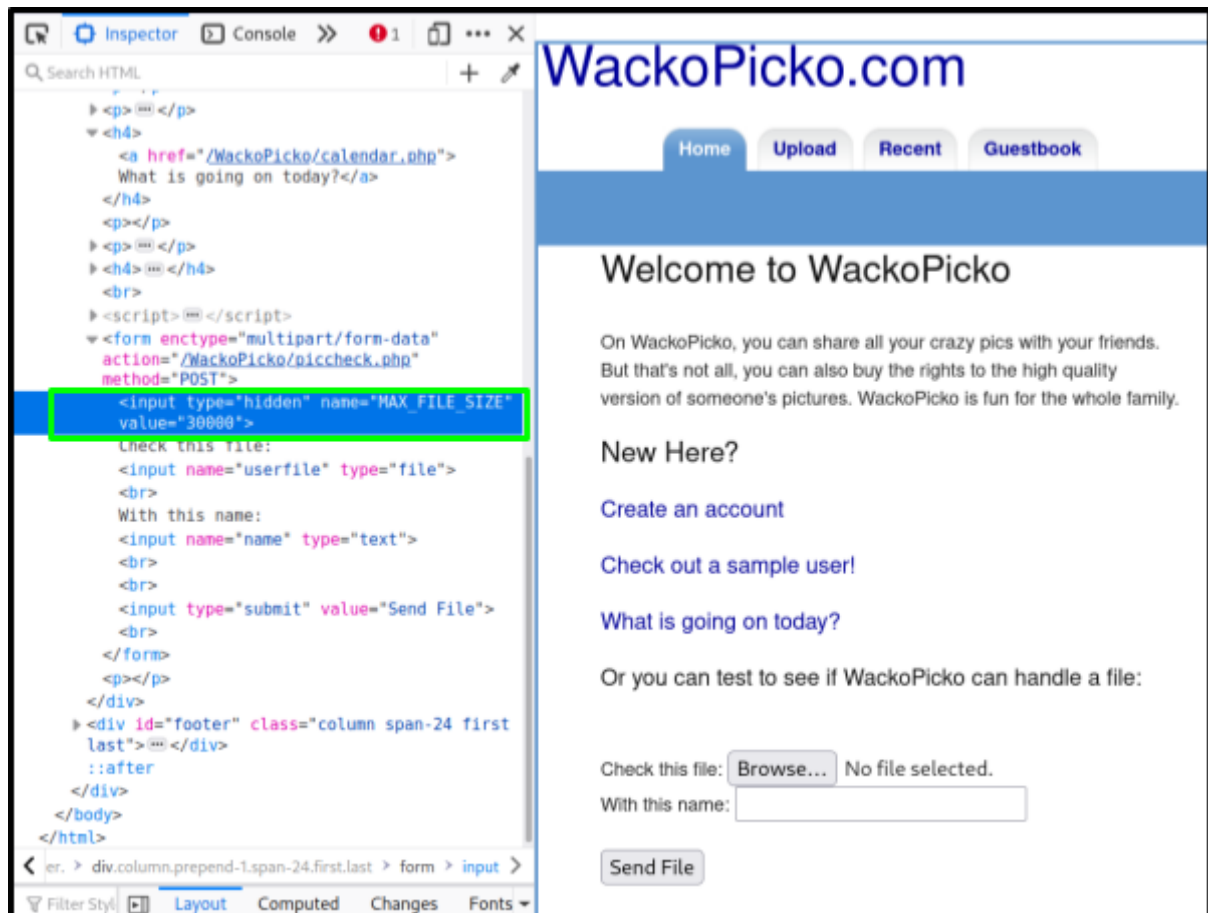
Based on the OSINT data that was gathered as part of the penetration test, there were a lot of insights provided into the target system's infrastructure. This information would be useful when discovering vulnerabilities, some of the information as you can see above contains knowledge of the domain registrar, name servers, IP addresses, and mail server. This gathered information does not expose any data that is sensitive or a certain type of vulnerability, it essentially provides data that can be used as a stepping stone for more extreme attacks if not handled well.

A.2: Reconnaissance

A.2.1: Testing Web Applications in Lab

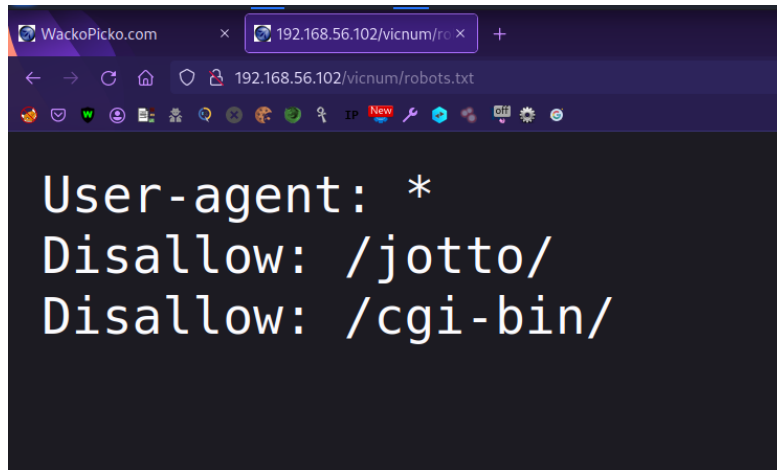
A.2.1.1: WackoPicko

The highlighted input tag in the inspector has a property indicating a character limit, an attacker could edit this limit and upload a much larger file. This would result in a DoS attack if the server's hardware cannot handle it.

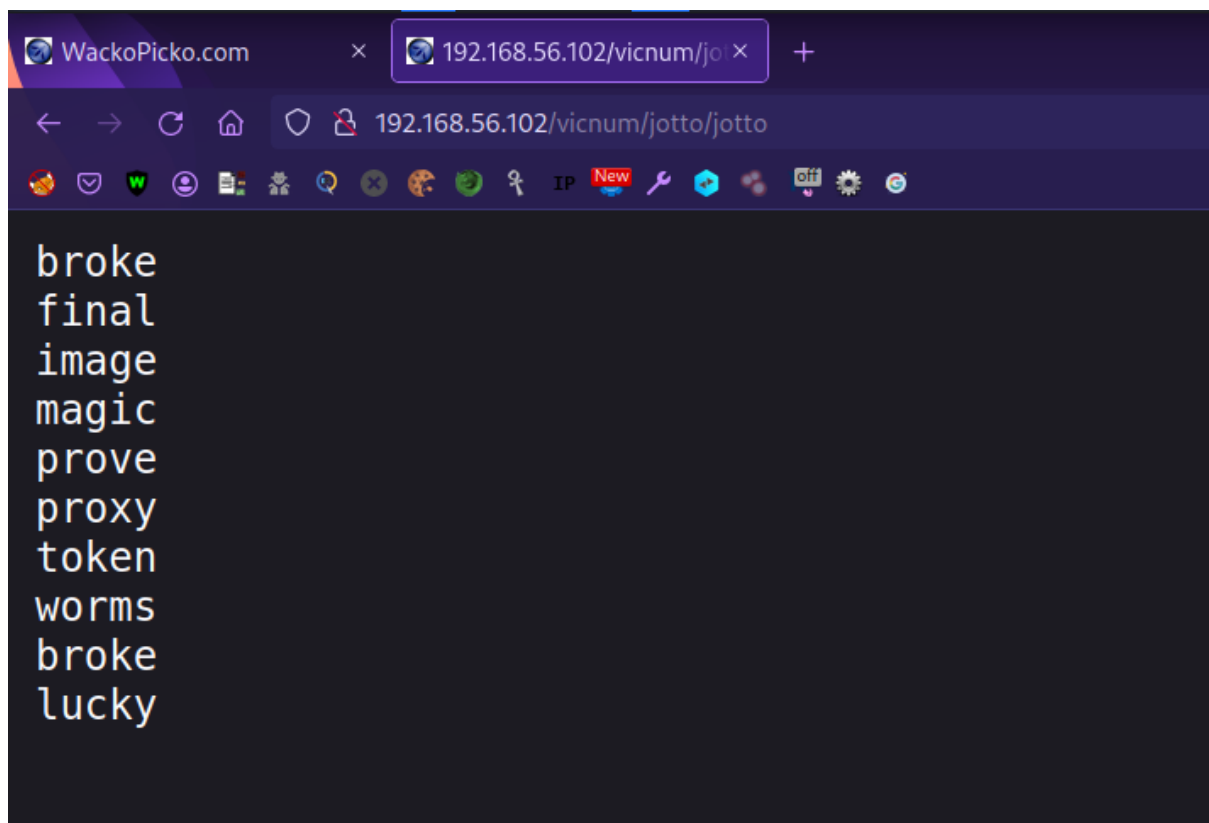


A.2.1.2: robots.txt

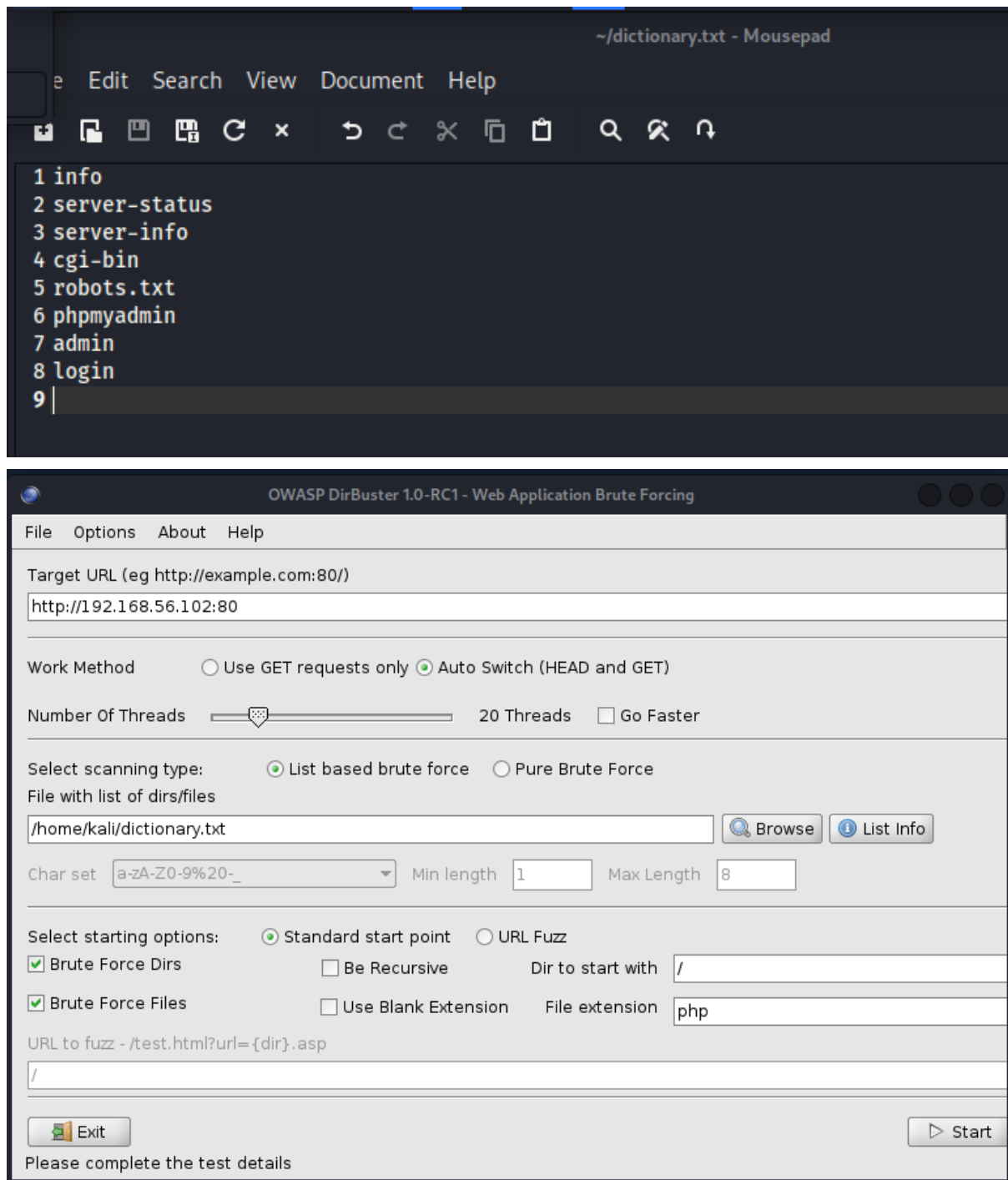
Vicnum is a site containing multiple games, the author attempted to access the robots.txt file of the site. This file contains information about parts of the site that web crawlers and bots should not use.



The above paths were discovered, and by accessing “/jotto/”, the author the below words that are supposed to be guessed in the Jotto game of the Vicnum site



A.2.1.3: dirbuster



This tool was used to brute force files and directories on the server hosting the site, the configuration can be seen above. And the findings uncovered several directories and files. Web apps like phpMyAdmin, OWASP Bricks, Vicnum and so forth were found. There were different server responses with some indicating successfully accessing a directory, some were forbidden and some required authentication.

The scan also revealed a significant number of Javascript and PHP files, thereby posing the potential for vulnerability if the associated security measures are inadequate. Ultimately, the file structure of the server is revealed as these files and directories are uncovered, this can aid the attacker in their understanding of the system architecture.

A.2.2: Scenario Assessment

The data that was obtained by the web applications gives more in-depth information about the systems architecture, vulnerabilities and entry points. The attacker can use the data that was produced to target exploits and possibly gain unauthorised access to sensitive information.

The files and directories uncovered the system's file structure and also vulnerable applications like phpMyAdmin and others were discovered. The aforementioned vulnerabilities can be used as a map to guide the attack along a path to comprise the company's web services.

phpMyAdmin is a potential vulnerability for the company, as this database management tool can be attacked and would exploit the credentials of the CEO, HR staff and other employees, consequently putting sensitive information at risk. The attacker could also manipulate appraisals in favour of a particular employee.

A.3: Port Scanning and Enumeration

A.3.1: Identified Ports

```
sudo nmap -sV -O 192.168.56.102
```

```
(kali@kali)-[~/recon-ng]
$ sudo nmap -sV -O 192.168.56.102
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-14 20:46 EDT
Nmap scan report for 192.168.56.102 (192.168.56.102)
Host is up (0.00037s 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)
h proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/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)
h proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/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.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.92%I=7%D=5/14%Time=646180EAXP=x86_64-pc-linux-gnuXr(NU
SF:LL,4,"\\xac\\xed\\0\\x05");
MAC Address: 08:00:27:89:D6:52 (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 15.72 seconds
```

Using nmap, the author was able to gather all the open ports of the server as can be seen in the above diagram. The open ports highlighted also have another column of text indicating the version of the port, this can be used by the attacker to match known exploits for the specific version. This also applies to the OS of the server which can be seen as highlighted in the above image.

A.3.2: What is an open port and what threats can it potentially pose?

An open port is essentially a communication endpoint which allows network traffic to enter and leave a system, almost like an open door; it provides access to an entry point that could pose a risk if left unsecured (Tyas Tunggal., 2023).

The attacker could gain unauthorised access, malware infiltration, DoS attacks and data infringement (Tyas Tunggal., 2023). Therefore it is very important to monitor, project and limit open ports to minimise associated dangers.

A.3.3: Assessing the Threats for each Open Port

The author will discuss the threats of only the most important open ports that he decided could pose a major threat to the system if exploited in the below table,

Port	Service	Assessment
22	SSH	SSH is designed to ensure the secure remote login and execution of commands between 02 systems. If the Secure Shell port is improperly secured, the attacker could gain full control of the system which poses a major risk to the company and site.
80	HTTP	Since HTTP is not encrypted, any communication going through this port is prone to MitM attacks, the attacker could also read and manipulate new data.
443	HTTPS	Although HTTPS is a secure version of HTTP, it could be vulnerable to certain exploits if the SSL/TLS configuration of the server is obsolete or weak.
139	NetBIOS-SSN	This port can be exposed to a variety of security risks by giving unauthorised access to file shares,

		conducting reconnaissance and potentially even brute-force attacks to crack employee credentials.
445	Microsoft-DS	This port is associated with Server Message Block (SMB) protocol and therefore is commonly exploited as it can lead to be used for data theft, remote code execution, ransomware, MitM attacks, directory travellers and more. Therefore this open port is a major vulnerability.
8080	HTTP-Proxy	This port can be exploited by attackers to gain unauthorised access in the HTTP proxy server and the applications running in the port.

Chapter B: Server-side Exploits

B.1: Data Tampering

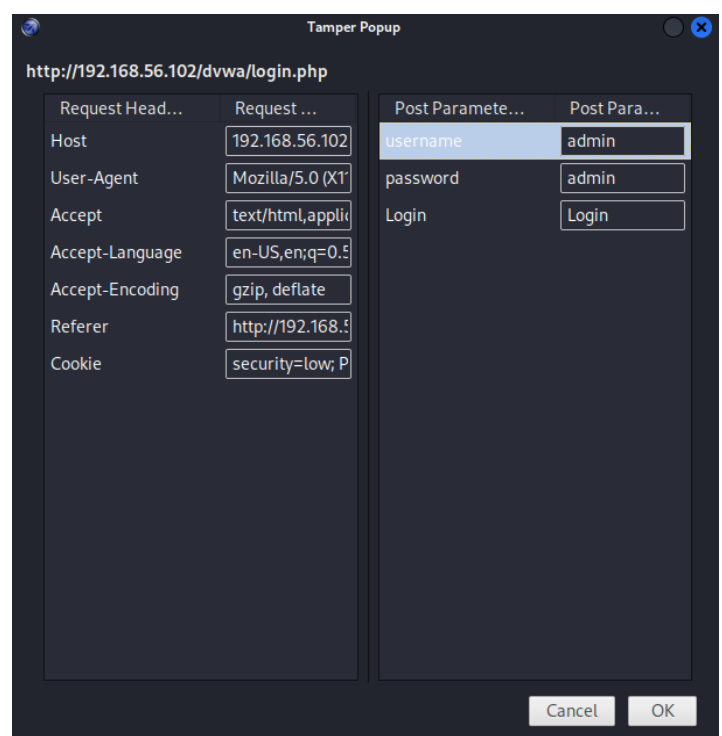
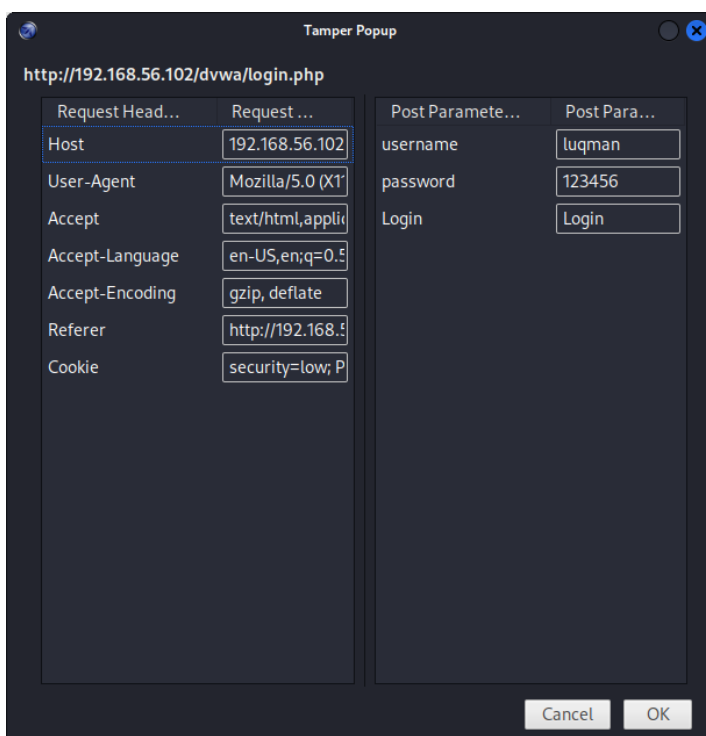
B.1.1: Attempting to tamper data in Login

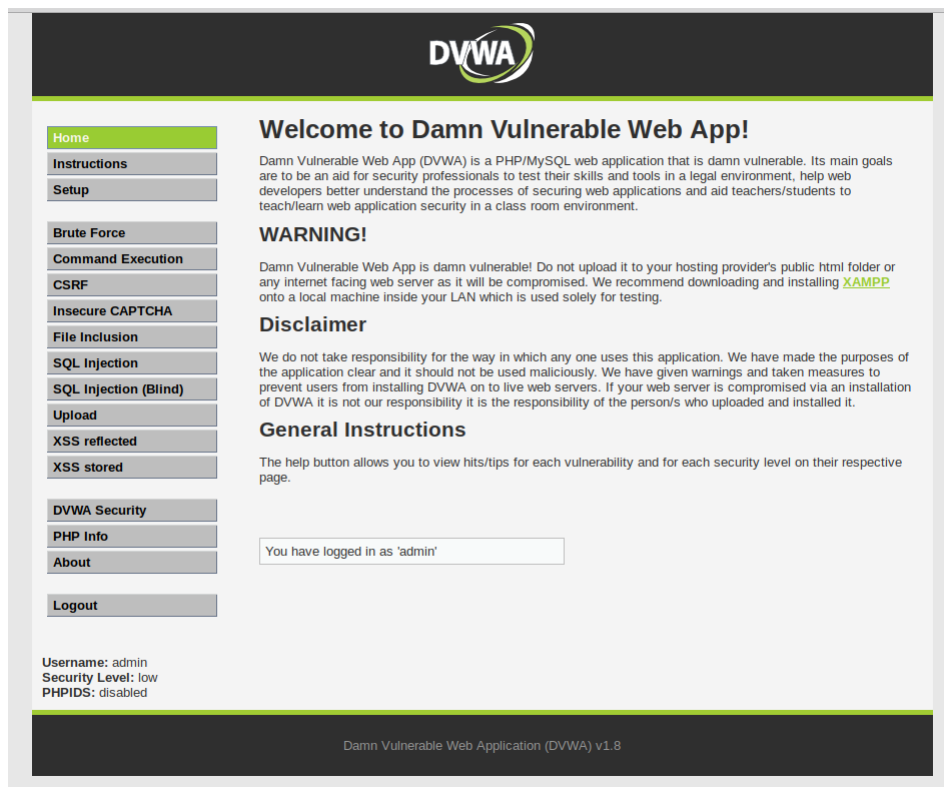


The image shows the DVWA (Damn Vulnerable Web Application) login page. At the top is the DVWA logo. Below it are two input fields: 'Username' with the text 'luqman' and 'Password' with five dots. A 'Login' button is centered below the password field.

This is the login page of the site. I am going to attempt to manipulate these invalid credentials used in the login with the Tamper Data tool in Owasp Mantra.

The screenshot on the bottom left shows as soon as the PHP script for the login is triggered, the popup containing data regarding the request options are presented. The username and password can be seen in plaintext. On the right side you can see that the author has modified the username and password to a valid credential.





The author is able to gain access to the site after tampering with the login data.

B.1.2: What is Data Tampering?

Data tampering is a form of malicious alteration which targets data in transit between 02 points of the application; this manipulation can affect the decision of an application (Kapsamer, 2022).

This vulnerability breaches the cyber security tenant of **Integrity**, it is essentially the assurance that the data is trustworthy and reliable. This would not be the cause if the attacker can tamper with the data, thus weakening its reliability and sacrificing its integrity.

B.1.3: Scenario Assessment

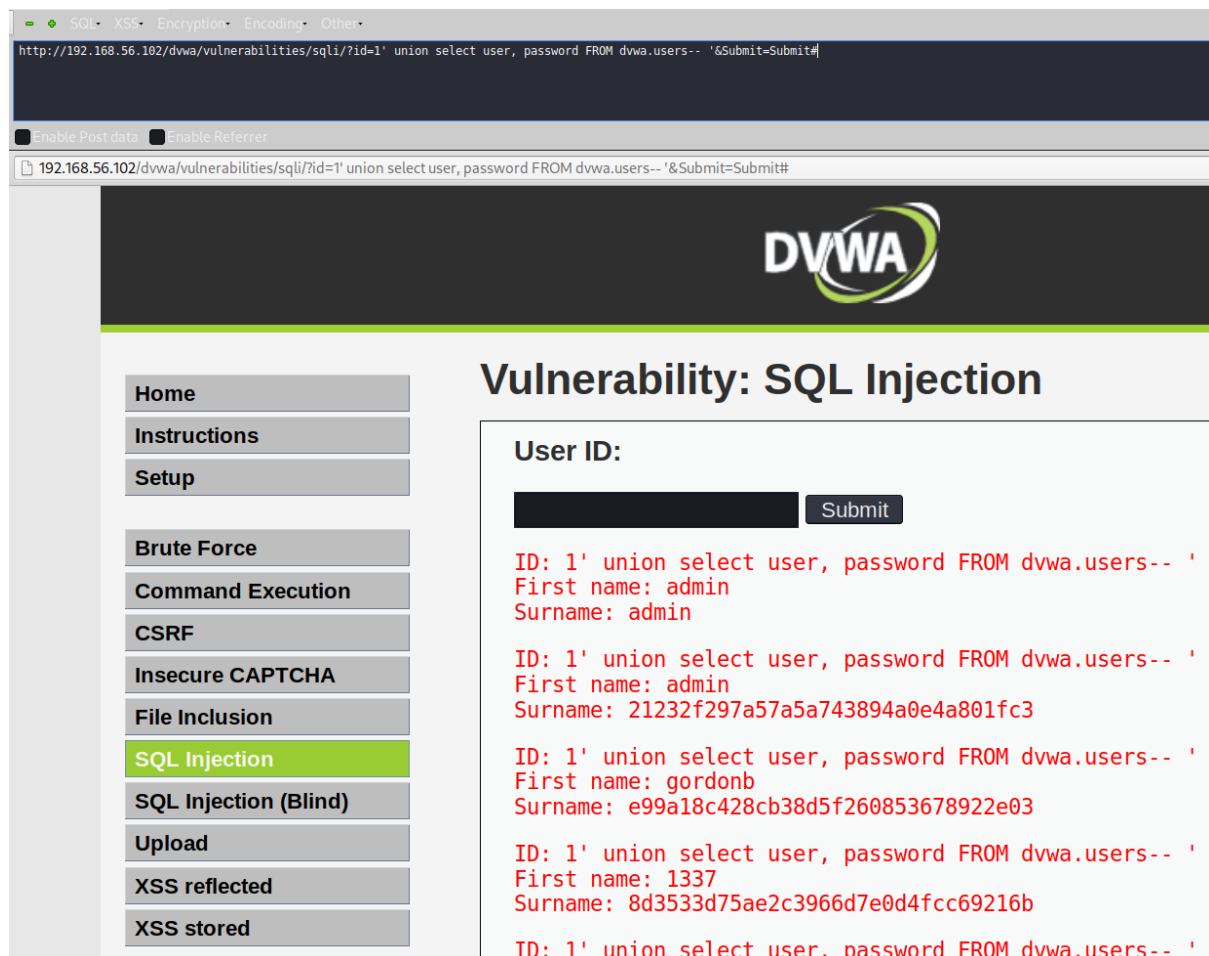
The login page of the HR management system can be exposed to data tampering, making it a vulnerable entry point for the attacker. The Plaintext transmission of credentials has a major negative impact on security, this is because it gives the ability to unauthorised users to intercept and tamper with the data to gain access to staff accounts.

B.2: SQL Injection

B.2.1: Attempting SQL Injection on Database

The author discovered that there was no input validation done when filtering users based on the ID, the author was also able to run queries.

```
http://192.168.56.102/dvwa/vulnerabilities/sqli/?id=1' union  
select user, password FROM dvwa.users-- '&Submit=Submit#
```



Subsequently the author was able to gather the database version and access the passwords of each user from the database using the above command.

B.2.2: What is SQL Injection?

SQL Injection is a type of cyberattack where the attacker exploits vulnerabilities within a web application to execute unintended SQL queries. It occurs when input data is not sanitised well (What is SQL Injection?, no date). The **Confidentiality** and **Integrity** tenants of cyber security are violated as the data in the database is

exposed to unauthorised personnel and the integrity of the data is compromised since the attacker can modify or delete the stored data.

B.2.3: Scenario Assessment

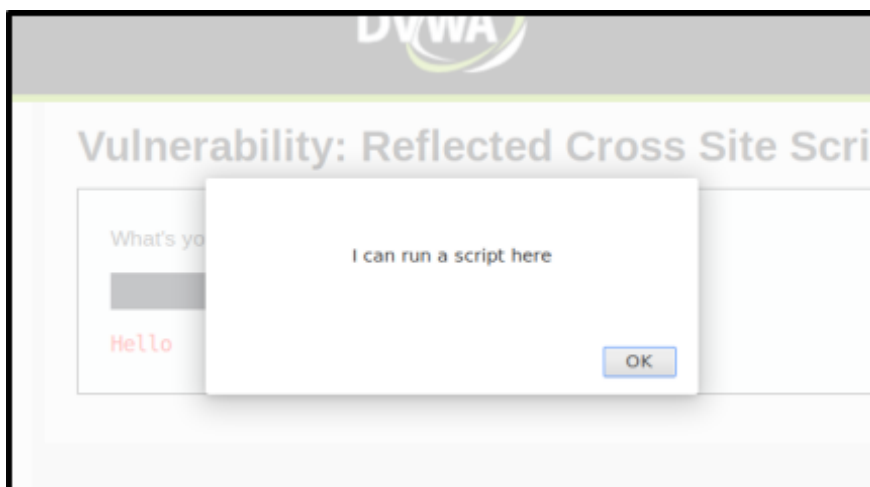
The author claims that SQL injection could be even more dangerous than data tampering, this is because the perpetrator will have access to all the employee data and their credentials without needing to sniff traffic. The data stored in the companies database is at risk of manipulation and exposure to malicious individuals without authorization and therefore this should be a major concern to the company.

B.3: XSS Scripting

B.3.1: Attempting XSS Scripting Injection with Form

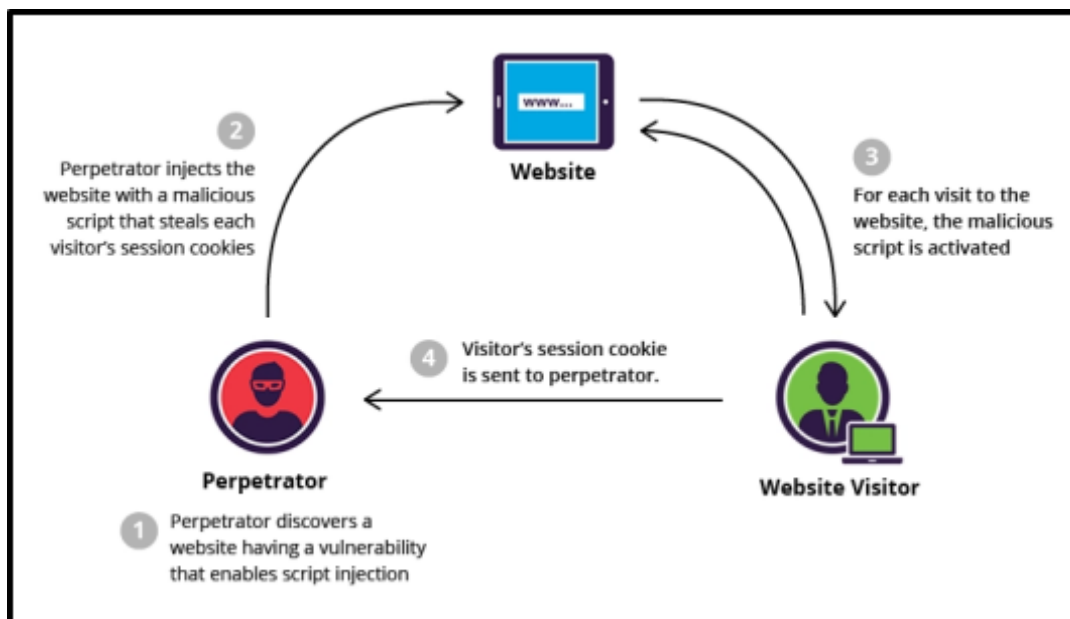


The form in the above image can be exploited, the above image indicates that the input is being displayed in the pre tag. This means that I can inject and execute scripts which lead to an XSS vulnerability, as can be seen in the below screenshot where I have imputed as script tag with an alert method.



B.3.2: What is XSS Scripting?

As you can see in the below illustration from (What is XSS | Stored Cross Site Scripting Example | Imperva, no date), the perpetrator could find a vulnerability that allows them to inject the website with a script that would execute as the visitor of the site performs an action to execute the script. This is known as XSS Scripting, and can be very risky since it has the potential for session cookie theft, website defacement and malicious script delivery to other users.



This vulnerability compromises the **Confidentiality** and **Integrity** tenants of the CIA triad. By exploiting XSS, the perpetrator could gain access to sensitive data without authorization, they could also change the behaviour or content of the website thereby impacting the integrity of it.

B.3.3: Scenario Assessment

The author asserts that XSS vulnerability uncovered for the HR system can pose a **significant** risk, an attacker could exploit it by injecting malicious script into the system. This would enable them to steal session cookies, grant them unauthorised access to confidential information related to employees.

Ultimately leading to serious implications for the company due to the breach of privacy and data integrity issues.

B.4: Additional Vulnerabilities

B.4.1: Attempts to exploit Additional Vulnerabilities

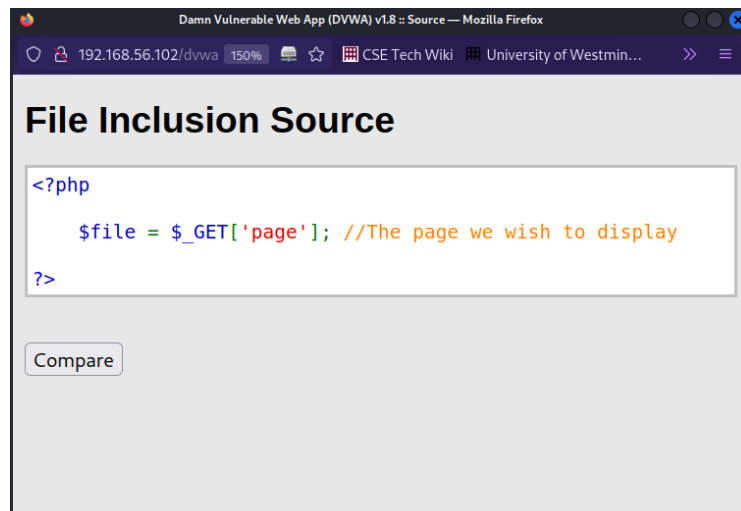
B.4.1.1: Buffer Overflow Attack



The screenshot above shows a repeater component in the website, where the user can enter a string and specify a number to display that string repeatedly based on the number given. There is no limit defined for the number of repeats and therefore could cause the site to crash.

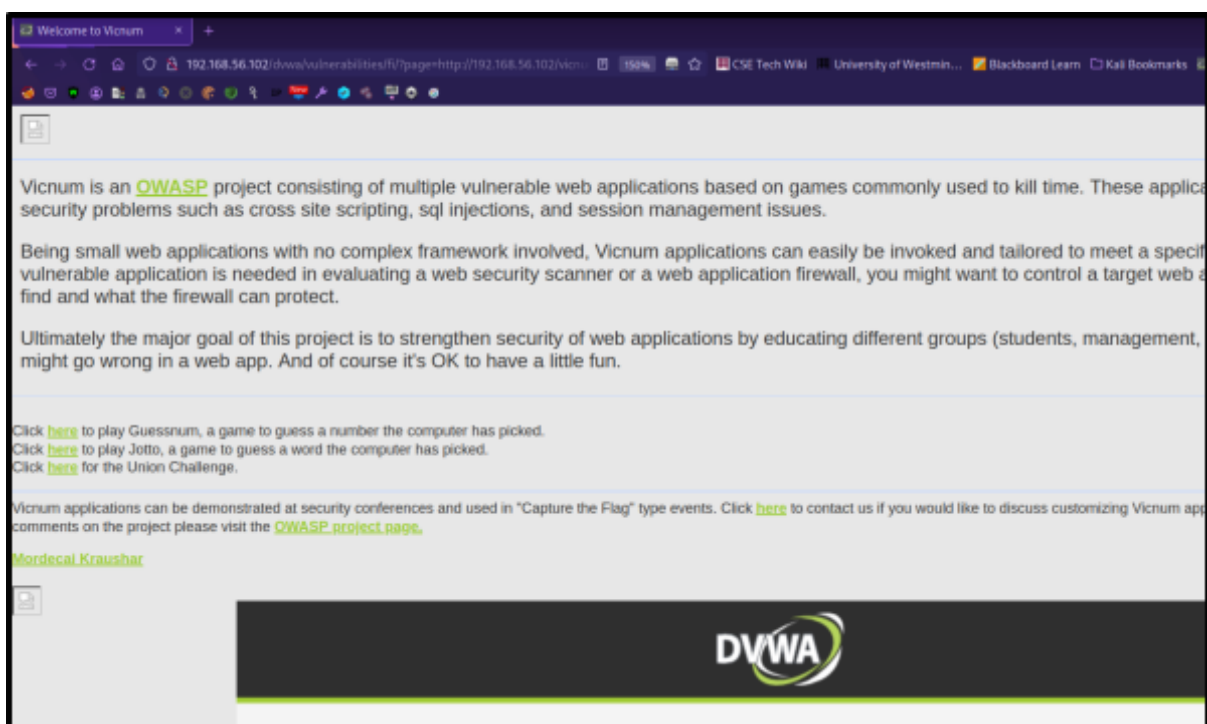
B.4.1.2: File Inclusion

The below image reveals a vulnerability in the source code, here the page query parameter determines content to serve.



```
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=http://192.168.56.102/vicnum/index.html
```

Thereby the author attempted to use the value as can be seen below for the query parameter, this includes content from the vicnum page as can be seen in the below screenshot.



B.4.2: Scenario Assessment

For the buffer overflow vulnerability, the perpetrator could write beyond the space that the block of memory can handle which would lead to the corruption of employee data, a system crash, or even the execution of malicious scripts (Buffer Overflow | OWASP Foundation, 2022).

The cybersecurity tenet that is violated here would be **Integrity**, since the accuracy of the employee data would be distorted if such an attack were to take place, also if malicious scripts are run then sensitive data could be altered. In this scenario, the integrity of the HR system and the reliability of the data it stores have been compromised. It would also affect the **Availability** of the system as the crash caused by this attack would consume system resources hindering the services of the HR management application.

If the attacker exploits the file and includes vulnerability, they could quite literally take over the server. Since the attacker could select random files in the server like index.html, then they could include malicious content from another remote file.

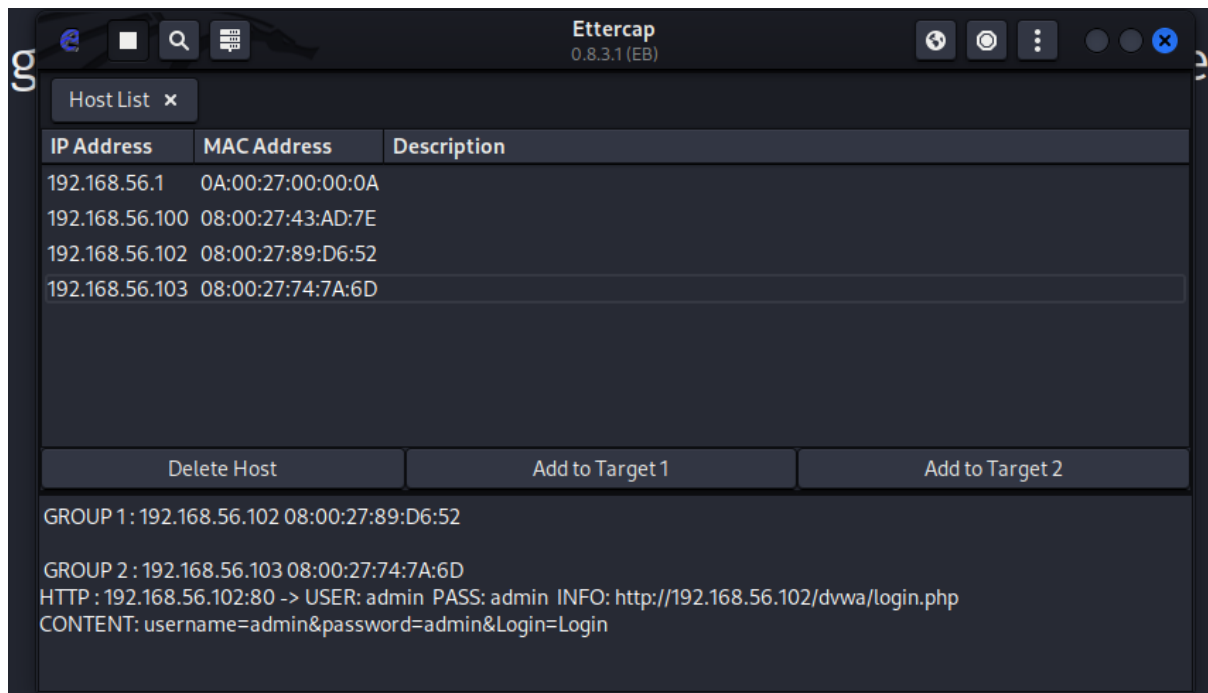
If the perpetrator utilises file inclusion to access forbidden employees, the **Confidentiality** tenant will be breached. However supposing that they make changes to existing files or run malicious commands the systems, the **Integrity** tenant will be compromised.

Chapter C: Client-side Exploits

C.1: Man in the Middle Attack

C.1.1: Ettercap

The author utilised ettercap in an attempt to sniff traffic from one target which is the server (192.168.56.102) and another target that is a client (192.168.56.103).



The login credentials of the client was sniffed and was successfully captured.

C.1.2: Scenario Assessment

This exploit presents a serious threat to the HR management system, as it will provide the attacker with the credentials of an employee that would give them unauthorised access to their personal information. Furthermore, if an HR staff members' credentials are compromised, then appraisals can be manipulated in favour of a specific employee.

The **Confidentiality** tenant is violated because the login details of an employee are exposed, and the Integrity tenant is violated as the attacker can manipulate appraisals and edit employee data.

C.2: Social Engineering Attack

C.2.1: Examples of Social Engineering Attack

C.2.2.1: Social-Engineer Toolkit

Using the Social-Engineer Toolkit tool the author was able to clone a website for a credential harvester attack.

```
[*] Cloning the website: https://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. It puts the pieces together by including all remaining
[*] 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...]

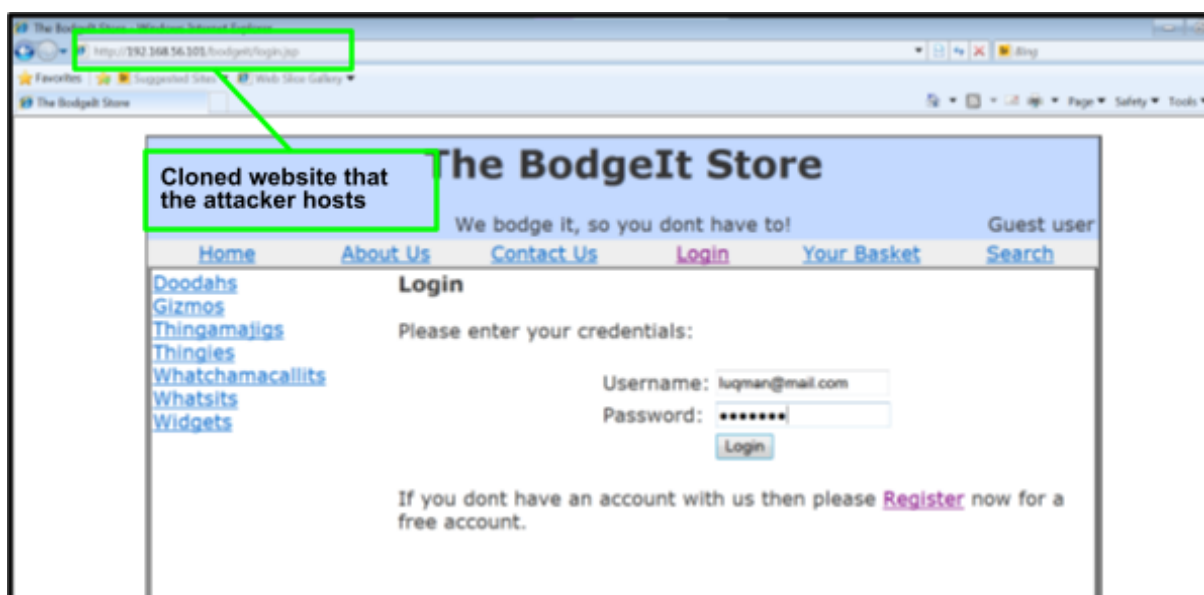
Array
(
    [username] => admin
    [password] => admin
)
```

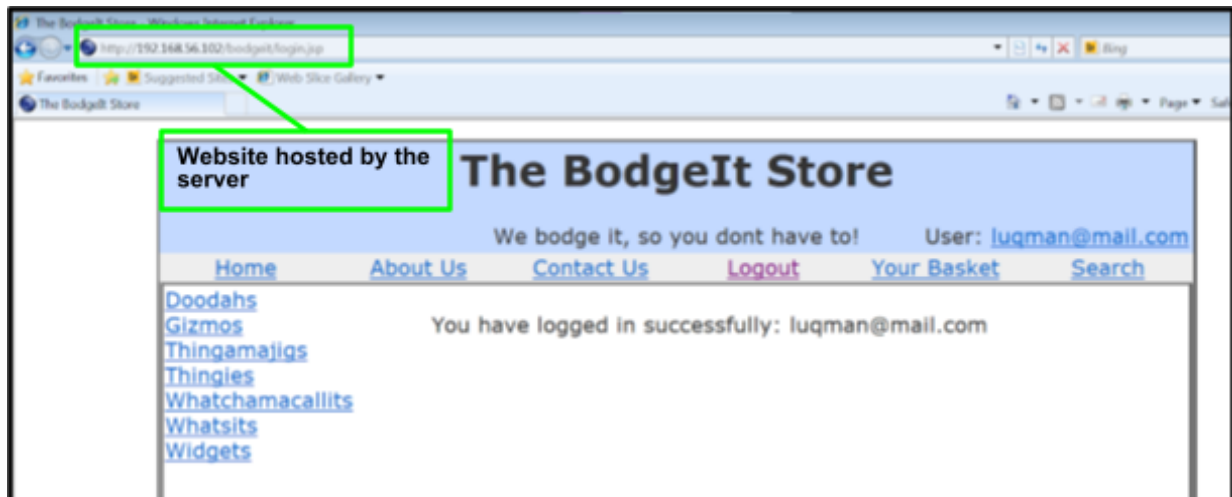
The user was tricked into entering their credentials in the cloned website, their credentials were then harvested as can be seen in the above screenshot.

C.2.2.2: Phishing Site

A phishing attack can also fool vigilant users into entering their login details. Because unlike the previously used method where users could be sceptical when they are redirected to the same page after signing-in, phishing would clone the full-page and can mimic the website more legitimately and would allow almost full site navigation. This would make it difficult for even more experienced users to spot the deception here.

In the below screenshot, the cloned website that is hosted by the perpetrator can be seen, the user has entered some credentials.





After clicking the login button, the website is then redirected to the legitimate site and the credentials of the user are stored in the attackers machine as seen below.

```
(kali@kali)-[~]
$ cat /var/www/html/bodgeit/labpasswords.txt
Array
(
    [username] => luqman@mail.com
    [password] => pass123
)
```

C.2.2: Scenario Assessment

The impact would more or less be the same as caused by the MitM attack. The employee data in the HR system as well as the fairness of employee appraisals would be damaged, since the perpetrator can modify this data.

The **Confidentiality** tenant is breached since the employee data and status of appraisals can be sabotaged, furthermore the **Integrity** tenant is breached as the user is directed to a replica of the original HR management site.

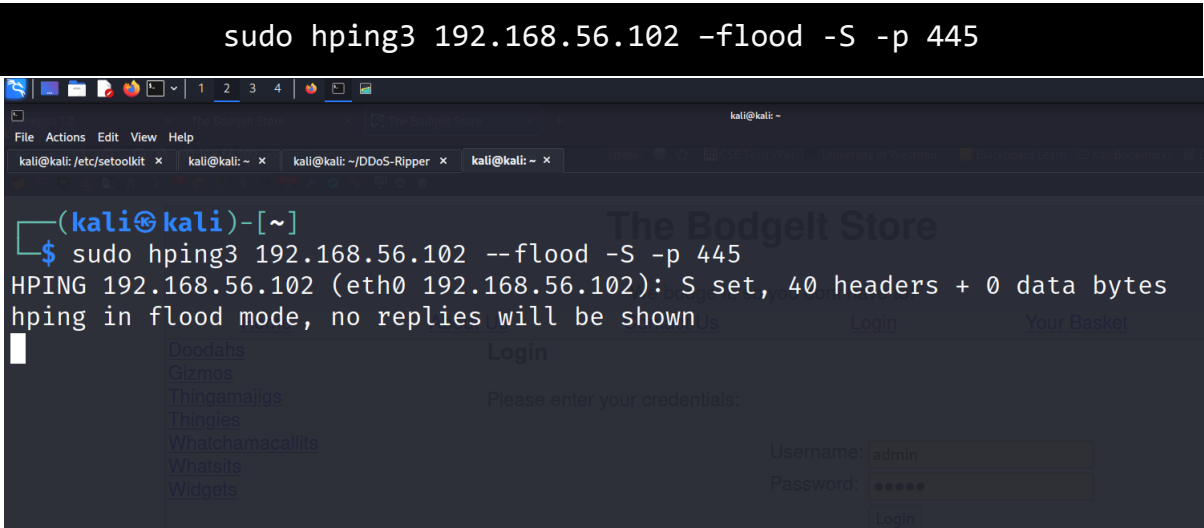
Chapter D: Denial of Service Attacks

D.1: DoS Attack

D.1.1: Examples of DoS Attacks

D.1.1.1: TCP SYN Flood

By executing the below command the author is using hping3 to send a bunch of SYN messages to an open port in the server but no ACK messages are returned, leading to the server's buffer being overwhelmed and potentially crashing it.



The image shows the output of the `top` command. The system is running with 2 users and a load average of 0.00, 0.11, 1.02. The CPU usage is 0.3% user, 3.2% system, 0.0% idle, 96.5% total. The memory usage is 1026132k total, 539872k used, 486260k free, 82316k buffers. The swap usage is 397304k total, 0k used, 397304k free, 229012k cached. The table below shows the process list with CPU and memory usage highlighted in green.

PID	USER	PR	NI	VRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
2340	root	20	0	2548	1280	920	R	3.8	0.1	0:23.75	top
6	root	20	0	0	0	0	S	0.3	0.0	0:02.95	events/0
1	root	20	0	2800	1636	1188	S	0.0	0.2	0:00.33	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
4	root	20	0	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/0
5	root	RT	0	0	0	0	S	0.0	0.0	0:00.00	watchdog/0

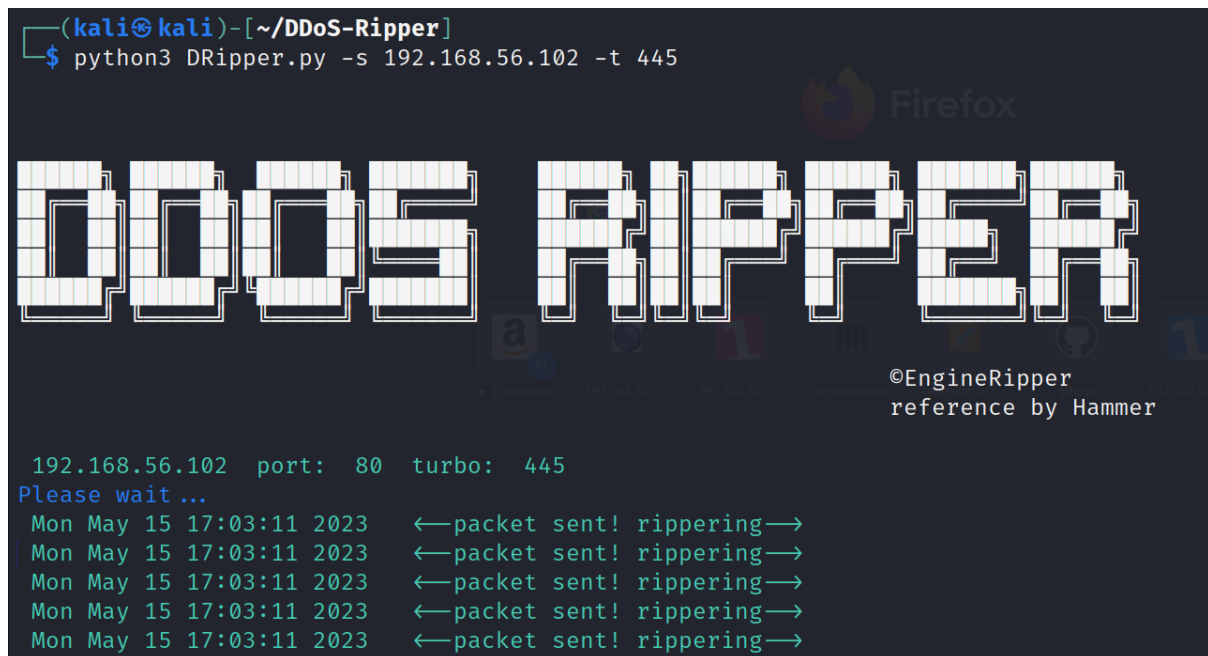
Before running this DoS attack the system resources of the server are not utilised heavily, after executing this attack the usage of server's hardware increases significantly as exhibited in the below image.

The image shows the output of the `top` command after the DoS attack. The system is running with 2 users and a load average of 0.00, 0.11, 1.02. The CPU usage is 32.5% user, 17.2% system, 4.6% idle, 54.3% total. The memory usage is 1026132k total, 539872k used, 486260k free, 82316k buffers. The swap usage is 397304k total, 0k used, 397304k free, 229012k cached. The table below shows the process list with CPU and memory usage highlighted in green.

PID	USER	PR	NI	VRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
2340	root	20	0	2548	1280	920	R	32.5	0.1	0:34.14	top
4	root	20	0	0	0	0	S	17.2	0.0	0:03.60	ksoftirqd/0
6	root	20	0	0	0	0	S	4.6	0.0	0:03.74	events/0
1588	root	20	0	283n	69n	14n	S	2.2	6.9	0:08.73	java
1649	root	20	0	664n	88n	18n	S	0.4	8.8	0:09.74	java

D.1.1.2: Smurf DoS Attack

DDoS Ripper allows the author to perform a smurf DoS attack, this involves sending multiple ICMP echo requests with spoofed source IP's to the server which causes all the hosts in the LAN to respond to the target which would overload the system.



```
(kali㉿kali)-[~/DDoS-Ripper]
$ python3 DRipper.py -s 192.168.56.102 -t 445

DDoS RIPPER

©EngineRipper
reference by Hammer

192.168.56.102 port: 80 turbo: 445
Please wait ...
Mon May 15 17:03:11 2023 ←packet sent! ripping→
Mon May 15 17:03:11 2023 ←packet sent! ripping→
Mon May 15 17:03:11 2023 ←packet sent! ripping→
Mon May 15 17:03:11 2023 ←packet sent! ripping→
Mon May 15 17:03:11 2023 ←packet sent! ripping→
```

The author noticed a delay of 15.22 seconds to load the index page during the Smurf DoS attack.

D.2: What Tenant does DoS violate?

The Accessibility tenant is breached here since the accessibility of the HR management site is impeded with a flood of network requests the system will lag and possibly even stop functioning.

D.3: Scenario Assessment

If the perpetrator successfully launches a DoS attack there would have a moderate impact on the HR process of the company as the HR staff will not be able to maintain employee information and management appraisals resulting in significant operational delays.

Since this company is a medium sized company and as this system is not for customers, there is not going to be as much of an impact, thus there won't be any costs. However it would affect the productivity of the HR department during

downtime and would bring a bad reputation to the company (Sansone, 2021). This is because the company develops IT solutions. Customers who may learn about such an attack taking place on this internal HR site would make them think twice about signing a contract and existing contracts can be affected.

Chapter E: Recommendations to Solve Vulnerabilities

E.1: Mitigation for A.2

The robots.txt file should be protected using access controls since it contains sensitive data, furthermore such data must be encrypted. The file upload size must also be specified to an appropriate limit, rate limiting must also be implemented.

The author also recommends the removal of unwanted services or applications, setting up access control, ensuring sensitive data is not stored in web-accessible directories, hardening server configurations and using a WAF to block malicious requests from attackers. It is also suggested that the HR system is patched regularly.

E.2: Mitigation for A.3

Port	Service	Mitigation
22	SSH	To minimise the threat that is associated with the SSH port, strong and complex passwords must be used. Furthermore after a certain number of failed attempts, SSH access must be disabled for a certain period of time.
80	HTTP	Confidential employee data such as credentials, address, contact numbers and such must never be sent over HTTP, rather such traffic must be redirected to HTTPS.
443	HTTPS	The company must update the server's SSL/TLS configuration often to mitigate the threats related to outdated protocols.
139	NetBIOS-SSN	It is recommended to block this port over TCP/IP if not required due to the threat of its vulnerabilities.

445	Microsoft-DS	To mitigate this threat, it's crucial to keep the running the system running the server updated and also to setup strong firewall rules/
8080	HTTP-Proxy	Make sure the HTTP proxy server and the applications running on it are well configured and updated.

E.3: Mitigation for B.2

The author suggests that input is sanitised, a regular expression to only allow letters, numbers, and spaces can stop any unwanted characters from passing into the form to avoid SQL Injection (What is SQL Injection?, no date).

E.4: Mitigation for B.3

The same mitigation used in E.3 should be done here, in no circumstances should the input data from the form be output onto the browser, there must be strong input validation (What is Cross-site Scripting and How Can You Fix it?, no date).

Moreover a Content Security Policy (CSP) can be implemented to reduce the sources of content that the browser could execute (West and Medley, 2020), this in turn helps prevent the execution of malicious code injected by attackers.

E.5: Mitigation for C.1

To protect against MitM attacks, the author endorses several approaches that can be employed. The utilisation of strong encryption protocols like HTTPS as well as the use of VPNs would make intercepted data unreadable to perpetrators.

Another suggestion is to acquire an IDS, it would help monitor the traffic in the network and would mark suspicious activities. Any attempts by the attack to exploit vulnerabilities would be blocked before they are breached (What is IDS and IPS? | Juniper Networks US, no date).

E.6: Mitigation for C.2

One of the most important tasks that must be done to solve social-engineering attacks is to ensure that staff members using the HR management system are

educated to acknowledge the common indicators of such attacks, validating the source for any communication will help prevent falling victim to phishing emails and spoofed hyperlinks (Ways to avoid social engineering attacks, 2023).

Additionally a strong way to minimise the risk of falling prey to this attack is to enable 2FA (Two-Factor Authentication), the attacker then would have the added task of figuring that out else they cannot proceed to gain unauthorised access.

E.7: Mitigation for D.1

To handle DoS attacks, the author advises that the company implements these measures. Firstly, the use of firewalls or IDSs will aid in identifying malicious activity and in dropping packets that are associated with the attack (mimecast, 2021).

A well-defined response plan to a DoS attack that covers communication, mitigation and recovery would be a lifesaver in the case that such an attack arises.

E.8: Intrusion Detection and Prevention Systems

E.8.1: Examples of firewall and iptable Rules

```
root@owaspbwa:~# sudo iptables -A INPUT -p tcp --dport 143 -j ACCEPT
WARNING: All config files need .conf: /etc/modprobe.d/vmware-tools, it will be i
gnored in a future release.
root@owaspbwa:~# sudo iptables -A INPUT -p tcp --dport 445 -j ACCEPT
root@owaspbwa:~# _
```

```
root@owaspbwa:~# sudo ufw allow from 192.168.56.101 to any port 5001
Rules updated
root@owaspbwa:~# iptables -A INPUT -p tcp --dport 80 -m limit --limit 30/minute
--limit-burst 100 -j ACCEPT
root@owaspbwa:~# _
```

The first screenshot shows the author using iptables to allow traffic for specific ports, and the other screenshot displays the use of ufw to allow traffic for the port 5001 and also the next command shows how DoS attacks can be limited using ufw by setting a limit.

E.8.2: Which Firewall Tool should the Company use?

When deciding an appropriate firewall for the HR management system, a multitude of factors must be considered. The network that is running the site does not seem to be that complex (*Hypothetical*), and the company does not have a solid team of systems administrators. By assessing the previous statements, the author recommends that **ufw** is used as a firewall tool due to its easy to use interface compared to **iptables** that is normally used for more complex systems and requires expert admins to configure it (How to work with your firewall, 2022).

E.8.3: What are the differences between an Intrusion Detection System and an Intrusion Prevention System?

	IDS	IPS
Scope	Network packet comparison and monitoring tool	A Control-based solution that approves or denies network packets.
Location	Operators by covering the entire network	Positioned in the same network as a firewall.
Intervention	It can manually stop threats through human intervention.	It can automatically stop threats before any further damage happens.
Configuration	It can be configured to operate in-line or logging mode.	Positioning to block or allow packets in-line.
Type	Host-based IDS, Network-based IDS	Host-based IPS, Network-based IPS, Wireless IPS

(Ashtari, 2022)

E.8.4: Scenario Assessment

By taking a close look at the differences between an IPS and IDS, the author advises the company to go with an IPS as it can even prevent detected threats unlike IDS. It also is autonomous and will not need a staff member to manually intervene, this is convenient as the company is medium and the application is for an internal system unlike a client application.

Bibliography

Ashtari, H. (2022). IDS vs. IPS: Key Difference and Similarities. *Spiceworks*. Available from <https://www.spiceworks.com/it-security/network-security/articles/ids-vs-ips/> [Accessed 16 May 2023].

Buffer Overflow | OWASP Foundation. (2022). Available from https://owasp.org/www-community/vulnerabilities/Buffer_Overflow [Accessed 16 May 2023].

How to work with your firewall. (2022). Available from <https://webdock.io/en/docs/how-guides/security-guides/how-work-your-firewall-ufw-uncomplicated-firewall> [Accessed 16 May 2023].

Kapsamer, R. (2022). The undetectable Cyber Security Threat: Data Tampering. *Tributech*. Available from <https://www.tributech.io/blog> [Accessed 15 May 2023].

Kelleher, S. (2020). OSINT: Common Tools and How to use them Safely. Available from <https://www.bu.edu/tech/files/2020/08/BU-Security-Camp-2020-OSINT.pdf>.

mimecast. (2021). DoS Attack | What Is A Denial-of-Service Attack (DoS). *Mimecast*. Available from <https://www.mimecast.com/blog/what-is-dos-attack-and-how-to-prevent-it/> [Accessed 16 May 2023].

Sansone, I. (2021). Why DDoS Attacks are So Damaging | Corero Network Security Blog. *Corero*. Available from <https://www.corero.com/the-damaging-impacts-of-ddos-attacks/> [Accessed 16 May 2023].

Tyas Tunggal., A. (2023). What is an Open Port? | Definition & Free Checking Tools for 2023 | UpGuard. Available from <https://www.upguard.com/blog/open-port> [Accessed 15 May 2023].

Ways to avoid social engineering attacks. (2023). *www.kaspersky.com*. Available

from

<https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks> [Accessed 16 May 2023].

West, M. and Medley, J. (2020). Content security policy. *web.dev*. Available from <https://web.dev/csp/> [Accessed 16 May 2023].

What is Cross-site Scripting and How Can You Fix it? (no date). *Acunetix*. Available from <https://www.acunetix.com/websitesecurity/cross-site-scripting/> [Accessed 16 May 2023].

What is IDS and IPS? | Juniper Networks US. (no date). Available from <https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html> [Accessed 16 May 2023].

What is SQL Injection? (no date). *StackHawk*. Available from <https://www.stackhawk.com/blog/what-is-sql-injection/> [Accessed 16 May 2023].

What is XSS | Stored Cross Site Scripting Example | Imperva. (no date). *Learning Center*. Available from <https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/> [Accessed 16 May 2023].

