

6COSC019W  
Cyber Security Coursework  
Awais khan  
w18076815

## Table of Contents

Building Company Scenario .....	2
A. Information Gathering.....	2
1. Open-Source Intelligence (OSINT) activities .....	2
2. Reconnaissance .....	10
i. TheHarvester .....	10
ii. SpiderFoot.....	12
3. Port Scanning and Enumeration .....	18
Fingerprinting for services .....	20
UDP scan .....	21
Threats an open port can potentially causes .....	22
B. Server-side exploits .....	23
i. Data tampering .....	23
1. Data tampering vulnerability .....	25
2. SQL injection .....	26
3. XSS Scripting.....	30
4. Other OWASP vulnerable machine vulnerabilities exploited. ....	33
C. Client-side exploits .....	37
1. Man in the Middle Attack (MiTM).....	37
2. Social engineering attack .....	39
D. Denial of Service attacks .....	40
1. DoS the web server.....	40
E. Recommendations to protect the scenario company server.....	42
References .....	47

## **Building Company Scenario**

A fledgling firm named "Green Grocers" engaged my business to perform a penetration test. The business operates an online marketplace where users may buy local farmers' fresh products. Customers may explore the available items, place orders, and make payments on the website <https://greengrocers.com>. Farmers may register and post their produce for sale on the platform as well. The database that underpins the backend of the website has data about customers, orders, and farmers. Twenty people work remotely for the startup Green Grocers from various places. To provide clients with a variety of fresh goods, the business has teamed up with regional farmers around the UK. The website keeps track of private data such as client names, addresses, phone numbers, and payment information. Additionally, the database contains facts on farmers, including their names, residences, bank account information for payments, and the produce they are selling. Customers and farmers are the two different user kinds on the website. To place orders and make payments, customers can create accounts. To register their goods for sale and manage their inventory, farmers can form accounts. Access to the backend of the website is available to Green Grocers staff employees for managing orders and customer service.

## **A. Information Gathering**

### **1. Open-Source Intelligence (OSINT) activities**

From the examples below we have undertaken OSINT vulnerabilities activities on a OWASP machine under Damn vulnerable Web Application. We can see a menu on the left; this menu contains links to all the vulnerabilities such as Brute Force, Command Execution, SQL Injection, and so on. We undertaken three activities as shown below where we could obtain vulnerable information on the machine hence easily attacked.

kali-linux-2022.3B-UoW-VBox-amd64 [Running] - Oracle VM VirtualBox

FileMachineViewInputDevicesHelp

1234


16:00

kali@kali: ~

Kali Linux x owaspbwa OWASP Broke x +

192.168.230.102

CSE Tech WikiUniversity of Westmin...Blackboard Learn



# owaspbwa

## OWASP Broken Web Applications Project

Version 1.2

This is the VM for the [Open Web Application Security Project \(OWASP\) Broken Web Applications](#) project. It contains many vulnerable web applications, which are listed below. More information about this project can be found in the project [User Home Page](#).

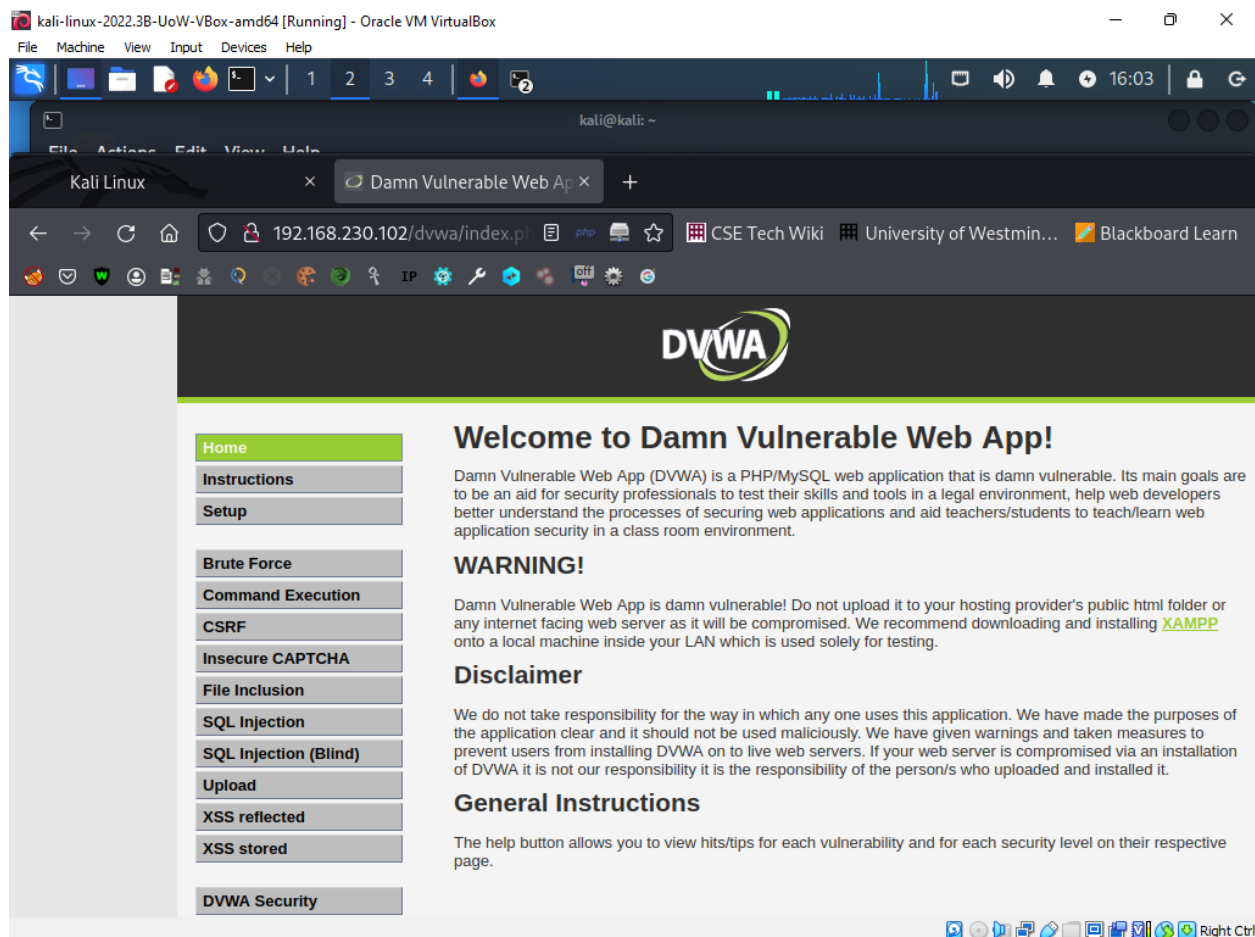
For details about the known vulnerabilities in these applications, see [https://sourceforge.net/p/owaspbwa/tickets/?limit=9&sort=\\_severity+asc](https://sourceforge.net/p/owaspbwa/tickets/?limit=9&sort=_severity+asc).

!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

TRAINING APPLICATIONS

www.owasp.org

Right Ctrl



The first vulnerability activity was the command execution. By inspecting the Damn Vulnerable Web App (DVWA) and performing command injection attacks, an attacker may gain unauthorized access to the underlying systems of the web application and perform malicious activities.

Specifically, an attacker can execute arbitrary commands on the server hosting the DVWA by pasting commands into vulnerable input fields such as search fields, login forms, or other input fields that have not been properly sanitized or validated.

Some of the data that an attacker can achieve while executing a command injection assault on DVWA includes:

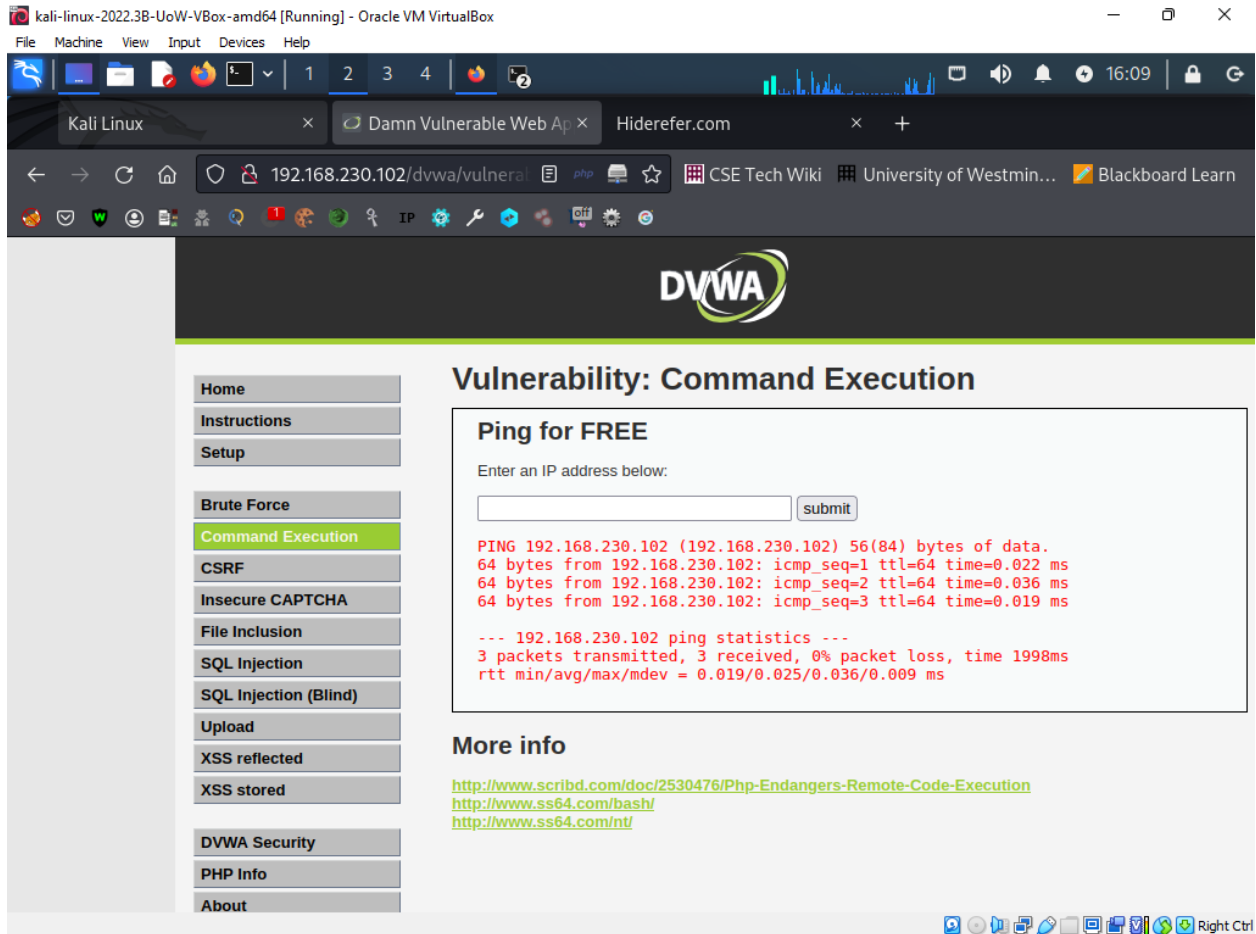
System data: The attacker can retrieve machine data along with the working machine, version, and configuration of the server web website hosting the DVWA.

User credentials: If the attacker profits get right of entry to to the underlying machine, they could doubtlessly achieve person credentials and use them to get right of entry to different structures or amplify their privileges.

File machine get right of entry to: The attacker can traverse the report machine and get right of entry to documents and directories that they may be now no longer legal to view, modify, or delete.

Network data: The attacker can achieve data approximately the community configuration, gadgets related to the community, and doubtlessly get right of entry to different structures at the identical community.

Overall, command injection assaults can result in extreme results along with facts theft, unauthorized get right of entry to, and machine compromise, making it important to nicely sanitize and validate person enter fields to save you such assaults.



The second activity was Cross Site Request Forgery (CSRF).

By scanning the Damn Vulnerable Web App (DVWA) and performing a Cross Site Request Forgery (CSRF) attack, the attacker can obtain different information and perform different actions depending on the vulnerability exploited. increase.

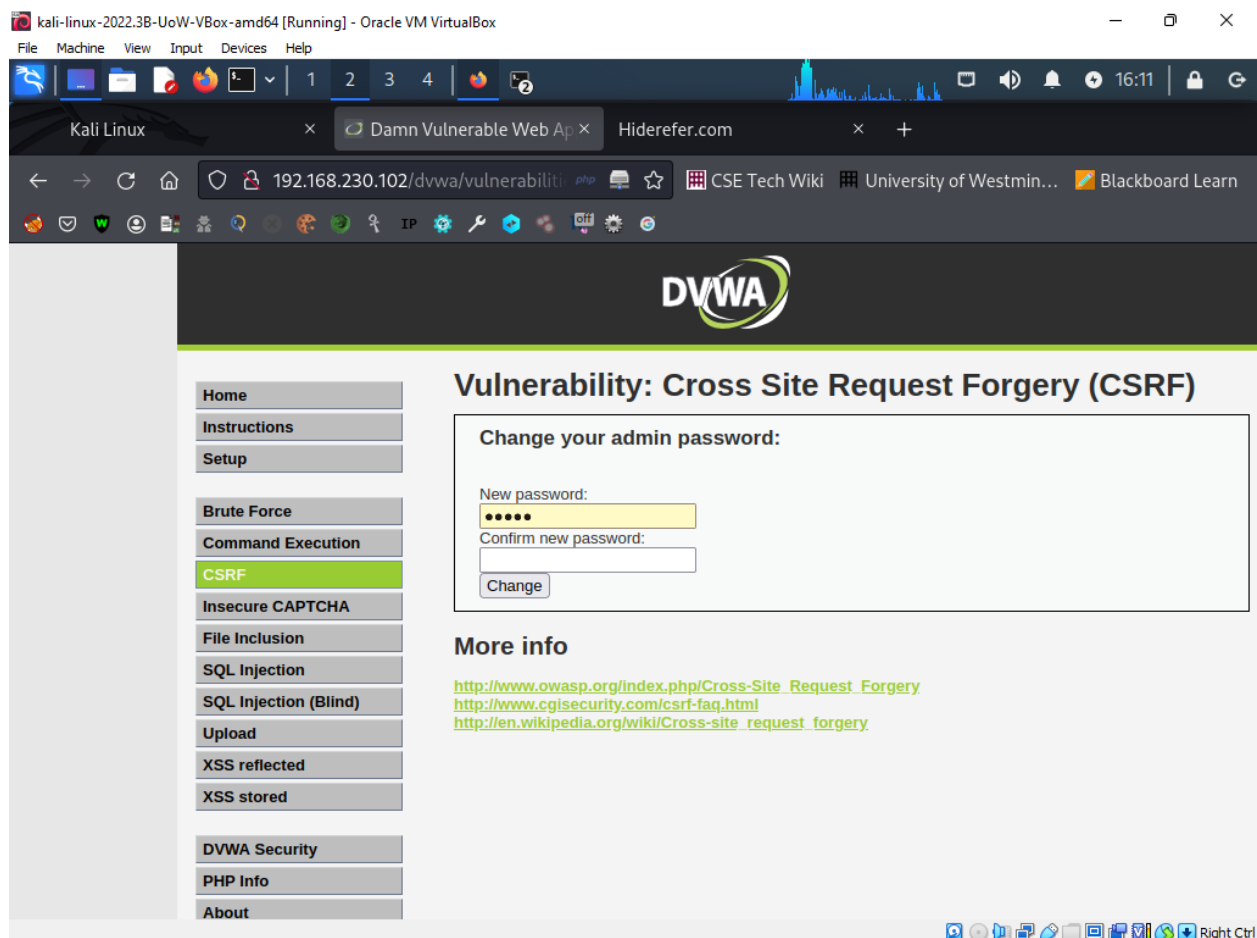
When a CSRF attack is successful, the attacker is often able to carry out illegal tasks on behalf of a victim user who has previously authenticated to a weak online application (Dokman, and Ivanjko, 2020). For instance, an attacker may persuade a victim user to click a malicious link that sends an impersonation request to a weak web application, causing the victim user to carry out an activity they did not intend.

For example, in a successful CSRF attack against DVWA, an attacker can access the following details and perform the following actions: from your account.

Send messages on behalf of victims: Attackers can send messages on behalf of victims through vulnerable web applications. This can be exploited to propagate malware and phishing scams.

Modification of victim's account information: An attacker can modify a victim's account information, such as her email address and personal information such as password and username. This can be used for identity theft and other malicious activities.

Money transfer: A CSRF attack may be used by an attacker to transfer money from the victim's account to the attacker's account, costing the victim money.



The third activity was Brute Force.

Depending on your attack scenario, you can get some information from Damn Vulnerable Web App (DVWA) inspection and brute force execution.

First, the brute force attack itself reveals whether the target system implements appropriate security measures to prevent such an attack. A successful attack and the acquisition of credentials can give

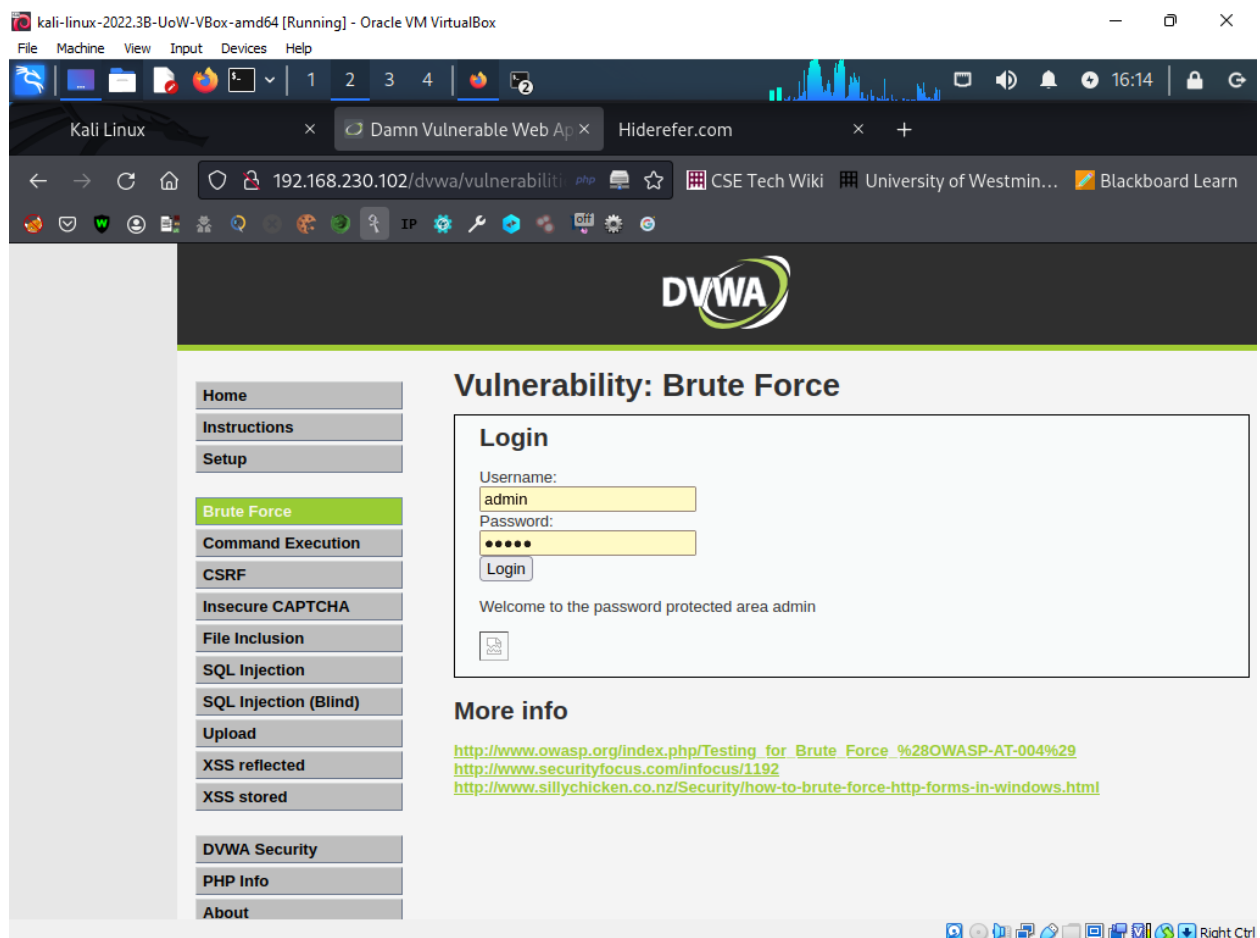


access to sensitive information such as: B. User Personal Data, Financial Information, and Sensitive Business Data. An attacker could also perform unauthorized actions on the system, such as: Adding, Deleting, or Modifying Data.

Specifically, for DVWA, an attacker can successfully brute force the login page and gain access to the management console. The administrative console contains sensitive information such as user credentials and configuration settings. A hacker might alter these settings, get access to more data or resources, or infect the machine with malware or other harmful software.

An attacker might potentially learn about particular system vulnerabilities in the case of DVWA, in addition. The system can be further penetrated or other assaults launched using this knowledge.

All things considered, it is essential to implement all required security safeguards to prevent unauthorized access and to routinely test systems for vulnerabilities to find any security holes before they can be exploited.



## **How OSINT can be effective**

Open Source Intelligence (OSINT) is the process of collecting and researching publicly available data in order to learn more about companies or specific individuals. This is an important part of penetration testing and can be used to learn more about target networks, systems and people.

The following are some justifications for why OSINT might be useful in penetration testing:

1. Finding suitable targets: OSINT may be used to learn about the resources, people, and infrastructure of an organization. The penetration tester can focus on regions that are more likely to be vulnerable using this information to find possible targets for penetration testing.
2. Reconnaissance: OSINT may assist penetration testers in doing reconnaissance on the target company to learn more about the operating systems, online applications, and network topology in use. The penetration testing procedure may be planned in accordance with this information to discover potential attack vectors.
3. Social engineering: OSINT can be used to compile data on people inside the target company, including their names, positions held, and email addresses. This knowledge may be utilized to create more successful social engineering schemes or convincing phishing emails.
4. Reporting: OSINT can assist penetration testers in creating thorough reports that summarize the results of the testing procedure. Utilizing this data, the target organization can be advised on remediation steps to take in order to identify vulnerabilities.

OSINT is frequently one of the first tasks performed by penetration testers throughout the testing process. This is so that later phases of the testing process may be informed by the abundance of information that OSINT can supply about the target company. Penetration testers can more efficiently design their testing approach by conducting OSINT early in the process to discover probable targets.

In conclusion, OSINT is a useful tool for penetration testers since it may provide important information about the target company and point out possible weaknesses. It is frequently one of the first tasks completed throughout the testing process and might provide information for later phases.

## **Scenario assessment**

If the wrong people get their hands on the material gathered via OSINT investigative efforts for the assigned scenario, it might be dangerous. The website keeps records of information on clients, including their names, addresses, phone numbers, and means of payment, as well as information about farmers, including their names, addresses, and bank account details for payments. Identity theft, financial fraud, and other security breaches may arise from unauthorized access to sensitive information.

Moreover, if adequate security measures are not in place, the website's backend, which is accessed by Green Grocers staff, may be open to attacks. For example, if a hacker obtains access to the backend, they could be able to alter orders, examine customer and farmer data, and jeopardize the website's security.

To prevent future security breaches, it is important to properly protect your website and databases with strong passwords, frequent security updates, and data encryption. Frequent security audits and risk assessments are also important to quickly find and remediate potential vulnerabilities.

## **2. Reconnaissance**

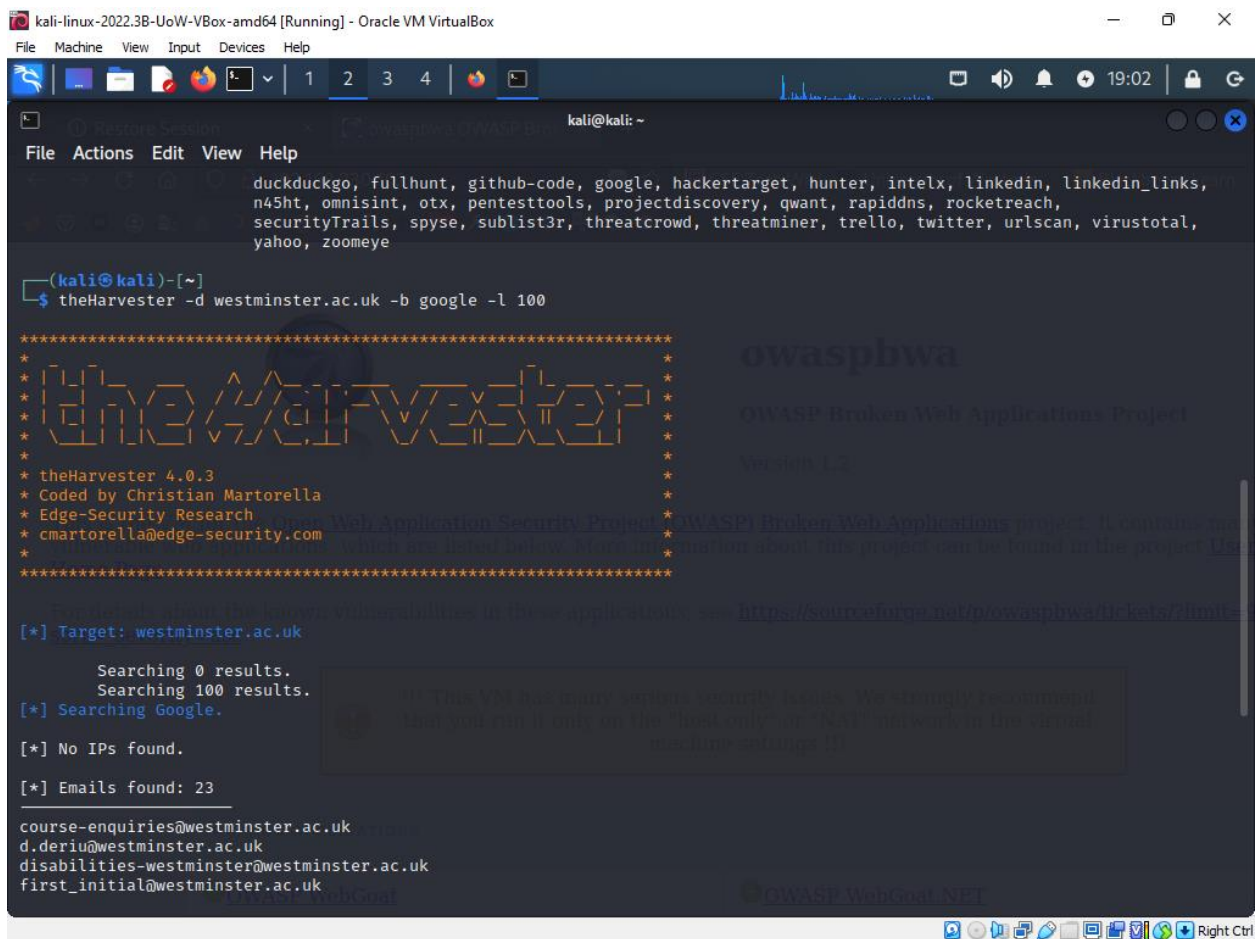
### **i. TheHarvester**

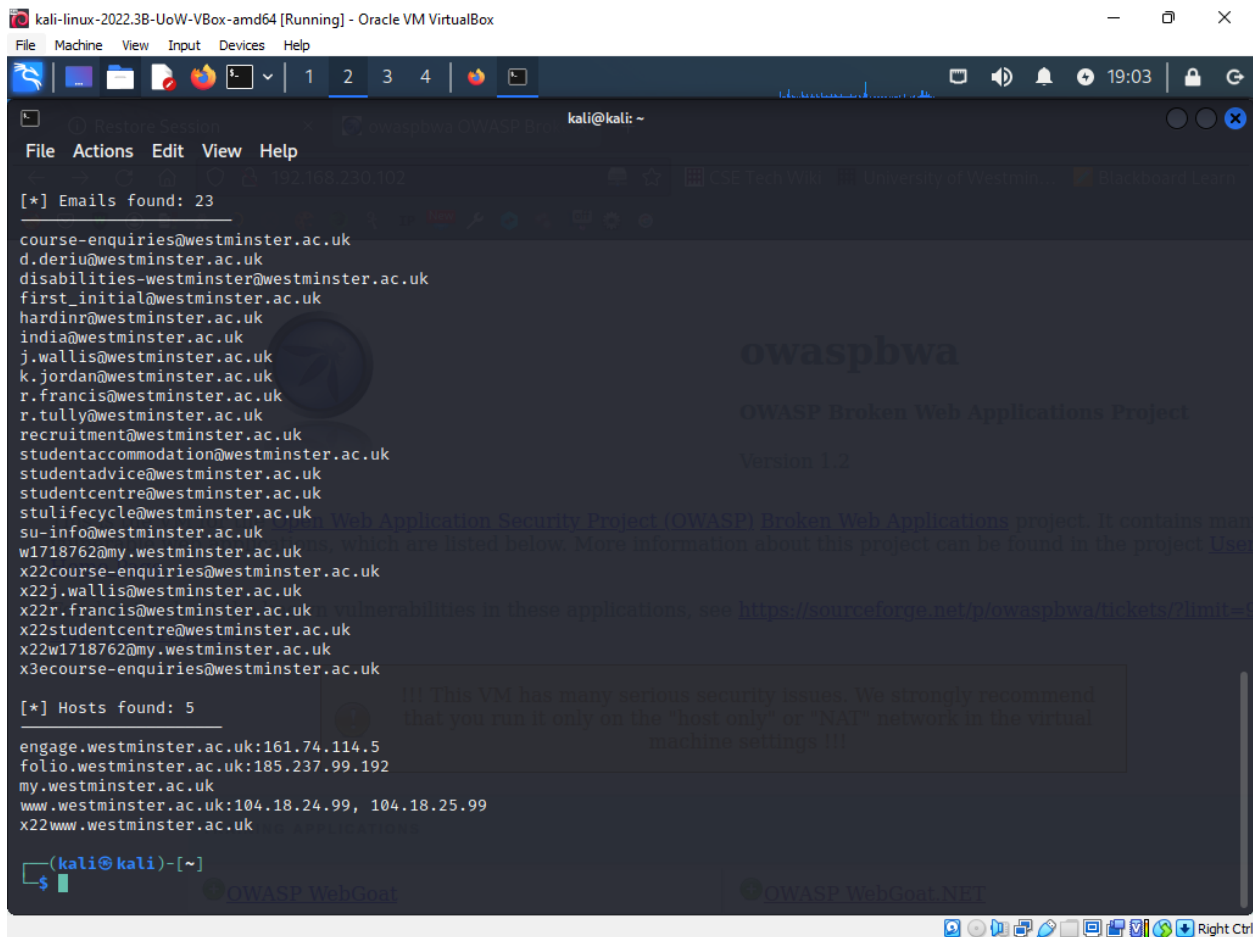
TheHarvester is a passive scouting tool that gathers information from various public databases, social media sites and search engines. An attacker can use her TheHarvester to find her IP address, hostname, username, subdomain, and email address for her targeted web application or company.

TheHarvester can steal a variety of essential information, including:

- Email addresses of the company's partners, clients, and staff
- Hostnames and subdomains connected to the web application
- Social media profiles connected to the business or its workers
- IP addresses of the equipment or servers used by the company
- Publicly accessible data or papers pertaining to the organization

This information can be used to carry out targeted phishing attacks, localize potential weaknesses in your infrastructure, or access sensitive data.





## ii. SpiderFoot

A well-known open-source tool for learning more about a target domain or IP address is called SpiderFoot. Using SpiderFoot, you can quickly find out details like:

DNS data, including IP addresses, subdomains, and MX records

Email addresses - by searching email search engines for addresses connected to the target domain or by scanning web pages for email addresses

Social media accounts - by looking up relevant accounts on social media search engines or by scouring web sites for social media links

You may find out additional information about the web server and the organization that runs the website by verifying the SSL/TLS certificates for the target domain.

Whois information - by searching WHOIS databases for facts on the domain owner, the date of registration, and their contact information.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ spiderfoot -I 127.0.0.1:5001  
usage: sf.py [-h] [-d] [-l IP:port] [-m mod1,mod2, ...] [-M] [-C scanID] [-s TARGET] [-t type1,type2, ...]  
            [-u {all,footprint,investigate,passive}] [-T] [-o {tab, csv, json}] [-H] [-n] [-r] [-S LENGTH] [-D DELIMITER]  
            [-f] [-F type1,type2, ...] [-x] [-q] [-V] [-max-threads MAX_THREADS]  
sf.py: error: unrecognized arguments: -I 127.0.0.1:5001  
  
(kali@kali)~  
$ spiderfoot -l 127.0.0.1:5001  
2023-05-02 08:25:07,346 [INFO] sf : Starting web server at 127.0.0.1:5001 ...  
2023-05-02 08:25:07,507 [WARNING] sf :  
*****  
Warning: passwd file contains no passwords. Authentication disabled.  
Please consider adding authentication to protect this instance! See one of the following. SpiderFoot will automatically detect the target type based on the format.  
Refer to https://www.spiderfoot.net/documentation/#security.  
*****  
*****  
Scan Target                                Domain Name: e.g. example.com                E-mail address: e.g. bob@example.com  
                                           IPv4 Address: e.g. 1.2.3.4                    Phone Number: e.g. +12345678901 (E.164 format)  
*****0.4700.4700:1111                      Human Name: e.g. "John Smith" (must be in quotes)  
Use SpiderFoot by starting your web browser of choice and browse to http://127.0.0.1:5001/  
                                           Username: e.g. "smith2000" (must be in quotes)  
*****                                           Network ASN: e.g. 1234  
                                           Subnet: e.g. 1.2.3.0/24  
                                           IP Address: e.g.  
                                           1HesYUSP1CqpyPEhCQvzBL1wujnNC67R  
  
By Use Case      By Required Data      By Module  
All              Get anything and everything about the target.  
  
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.  
  
Follow SpiderFoot on Twitter for the latest updates.
```

kali-linux-2022.3B-UoW-VBox-amd64 [Running] - Oracle VM VirtualBox

FileMachineViewInputDevicesHelp

127.0.0.1:5001/scaninfo?id=5D74557F

CSE Tech WikiUniversity of Westmin...Blackboard Learn

spiderfoot

New ScanScansSettings

Light M

spiderfoot

FINISHED

SummaryCorrelationsBrowseGraphScan SettingsLog

Scan Status

Total407Unique186StatusFINISHEDErrors252

Correlations

High2Medium0Low2Info5

Data Types

Unique Elements

987

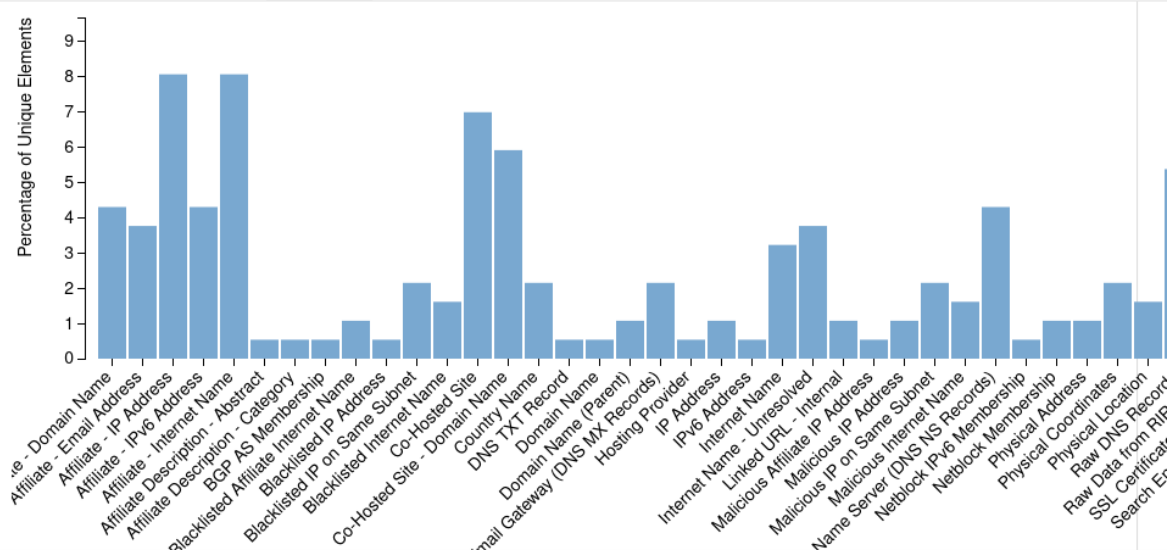
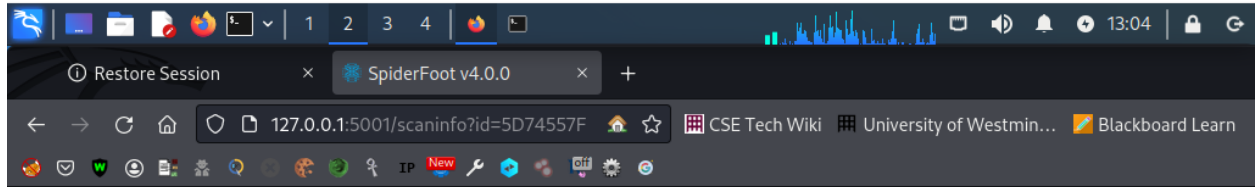
8

8

7

Want more OSINT automation capabilities? Check out SpiderFoot HX.

Right Ctrl



Want more OSINT automation capabilities? Check out SpiderFoot HX.



kali-linux-2022.3B-UoW-VBox-amd64 [Running] - Oracle VM VirtualBox

FileMachineViewInputDevicesHelp

1234

13:05

Restore SessionSpiderFoot v4.0.0

127.0.0.1:5001/scaninfo?id=5D74557FCSE Tech WikiUniversity of Westmin...Blackboard Learn

IPNew

spiderfootNew ScanScansSettings

Light

spiderfoot

FINISHED

- Summary
- Correlations
- Browse
- Graph
- Scan Settings
- Log

Correlation	Risk	Data Elements
Entity considered malicious by multiple sources: 2001-08d8-100f-f000-0000-0000-02b6.elastic-ssl.ui-r.com	HIGH	6
Entity considered malicious by multiple sources: 217.160.0.219	HIGH	3
Host found only in certificate transparency: autodiscover.cwscenario.site	LOW	7
Host found only in certificate transparency: www.cwscenario.site	LOW	9
Outlier country found: Montenegro	INFO	1
Outlier country found: United Kingdom	INFO	1
Outlier hostname found: 2001-08d8-100f-f000-0000-0000-02b6.elastic-ssl.ui-r.com	INFO	1
Outlier hostname found: 217-160-0-219.elastic-ssl.ui-r.com	INFO	1
Outlier hostname found: adsreidir.ionos.info	INFO	2

Want more OSINT automation capabilities? Check out SpiderFoot HX.

kali-linux-2022.3B-UoW-VBox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

Restore Session SpiderFoot v4.0.0

127.0.0.1:5001/scaninfo?id=5D74557F CSE Tech Wiki University of Westmin... Blackboard Learn

spiderfoot New Scan Scans Settings Light M

spiderfoot **FINISHED**

Summary Correlations Browse Graph Scan Settings Log Search...

Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Domain Name	8	20	2023-05-02 08:57:59
Affiliate - Email Address	7	8	2023-05-02 08:52:33
Affiliate - IP Address	15	15	2023-05-02 08:57:59
Affiliate - IPv6 Address	8	8	2023-05-02 08:57:59
Affiliate - Internet Name	15	41	2023-05-02 08:58:47
Affiliate Description - Abstract	1	1	2023-05-02 08:55:08
Affiliate Description - Category	1	1	2023-05-02 08:55:08
BGP AS Membership	1	5	2023-05-02 08:51:31
Blacklisted Affiliate Internet Name	2	2	2023-05-02 08:57:13

Want more OSINT automation capabilities? Check out SpiderFoot HX.

Right Ctrl

## Assessment scenario

Testing online apps can reveal flaws that could possibly be used to access a company's web services without authorization. For instance, if a penetration tester finds a SQL injection vulnerability in the database of the website, they may use this weakness to extract sensitive data from the database, such as client names, addresses, phone numbers, and payment information. The company's online services may potentially be the subject of a focused assault using this information.

In the case of Green Grocers, if a penetration tester finds a weakness in the website's login mechanism, they may be able to access the website's backend, which has private data about the company's clients and farmers. Furthermore, they had access to the database that held data on customers and orders. If this information is utilized to launch a targeted assault on the company's

online services, the security of the platform's users, including both customers and farmers, might be put in danger.

Additionally, if the penetration tester finds a flaw in the payment system, they might be able to use it to access the payment information of Green Grocers' clients, which they might then use to carry out fraudulent transactions. Customers and the business might suffer money losses as well as reputational harm as a result of this.

### **3. Port Scanning and Enumeration**

Security experts employ port scanning and enumeration techniques to find open ports on a network or system and learn more about the services that are using those ports. Once open ports have been located, attackers can use the flaws in those ports to gain unauthorized access to a network or system.

Open ports frequently have vulnerabilities like the following:

- Unpatched software: A service may be vulnerable to known vulnerabilities or attacks if it is using an open port and an out-of-date or unpatched software version.
- Some services might make use of default usernames and passwords, which are well-known to hackers and can be quickly exploited to gain access to the system.
- Access controls that have been improperly set might allow an attacker to access confidential data or take illegal activities on the system.
- A service may be subject to buffer overflow attacks, in which attackers submit more data than the service can manage, causing it to crash or run malicious code, if it is not correctly designed to handle unexpected input.
- SQL injection: Attackers can insert erroneous SQL instructions into user input fields of services that connect with databases, giving them access to or control over sensitive data in the database.

```
kali@kali: ~  
File Actions Edit View Help  
$ nmap -sn 192.168.230.102  
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-02 04:28 EDT  
Nmap scan report for 192.168.230.102  
Host is up (0.0033s latency).  
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds  
  
$ nmap 192.168.230.102  
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-02 04:29 EDT  
Nmap scan report for 192.168.230.102  
Host is up (0.0016s latency).  
Not shown: 991 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
139/tcp   open  netbios-ssn  
143/tcp   open  imap  
443/tcp   open  https  
445/tcp   open  microsoft-ds  
5001/tcp  open  complex-link  
8080/tcp  open  http-proxy  
8081/tcp  open  blackice-icecap  
  
Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds  
  
$
```

Now, we'll instruct Nmap to inquire about the server's service versions and infer the operating system based on those results. The version is determined by the banner header or self-identification that -sV requests for each open port that is discovered. Using data gathered from open ports and version numbers, the -O flag instructs Nmap to attempt to identify the operating system running on the target.

```
kali-linux-2022.3B-UoW-VBox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ sudo nmap -sV -O 192.168.230.102
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-02 04:32 EDT
Nmap scan report for 192.168.230.102
Host is up (0.0013s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 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_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=5/2%Time=6450CA9B%P=x86_64-pc-linux-gnu%r(NUL
SF:L,4,"\xac\xed\x05");
MAC Address: 08:00:27:5F:D4:AD (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 30.12 seconds

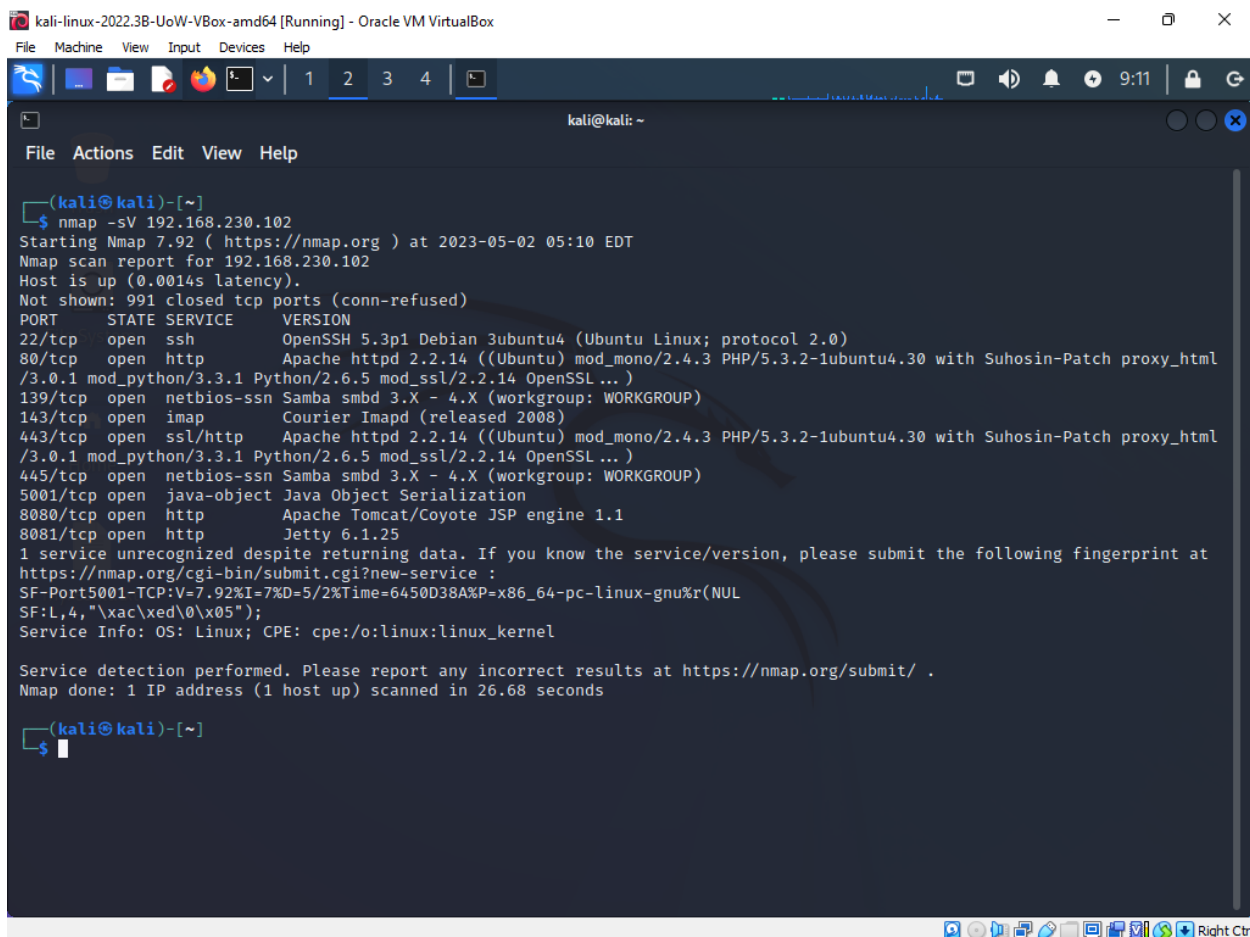
(kali@kali)-[~]
$
```

## Fingerprinting for services

On the target host with the IP address 192.168.230.102, service version identification is carried out using the nmap command "nmap -sV 192.168.230.102". In other words, nmap will make an effort to identify the precise applications and version numbers running on any open ports discovered throughout the scan.

Depending on the individual program and version discovered, open ports and services may have vulnerabilities. Once the software and version are identified, a vulnerability assessment can be carried out to see if the software and version have any known vulnerabilities.

A vulnerability assessment might find, for instance, that the target host is running Apache HTTP Server version 2.4.29, which is known to have a vulnerability (CVE-2017-15715) that could allow an attacker to run arbitrary code or inflict a denial of service.



```
kali-linux-2022.3B-UoW-VBox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ nmap -sV 192.168.230.102
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-02 05:10 EDT
Nmap scan report for 192.168.230.102
Host is up (0.0014s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 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_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=5/2%Time=6450D38A%P=x86_64-pc-linux-gnu%r(NUL
SF:L,4,"xac\xed\x05");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

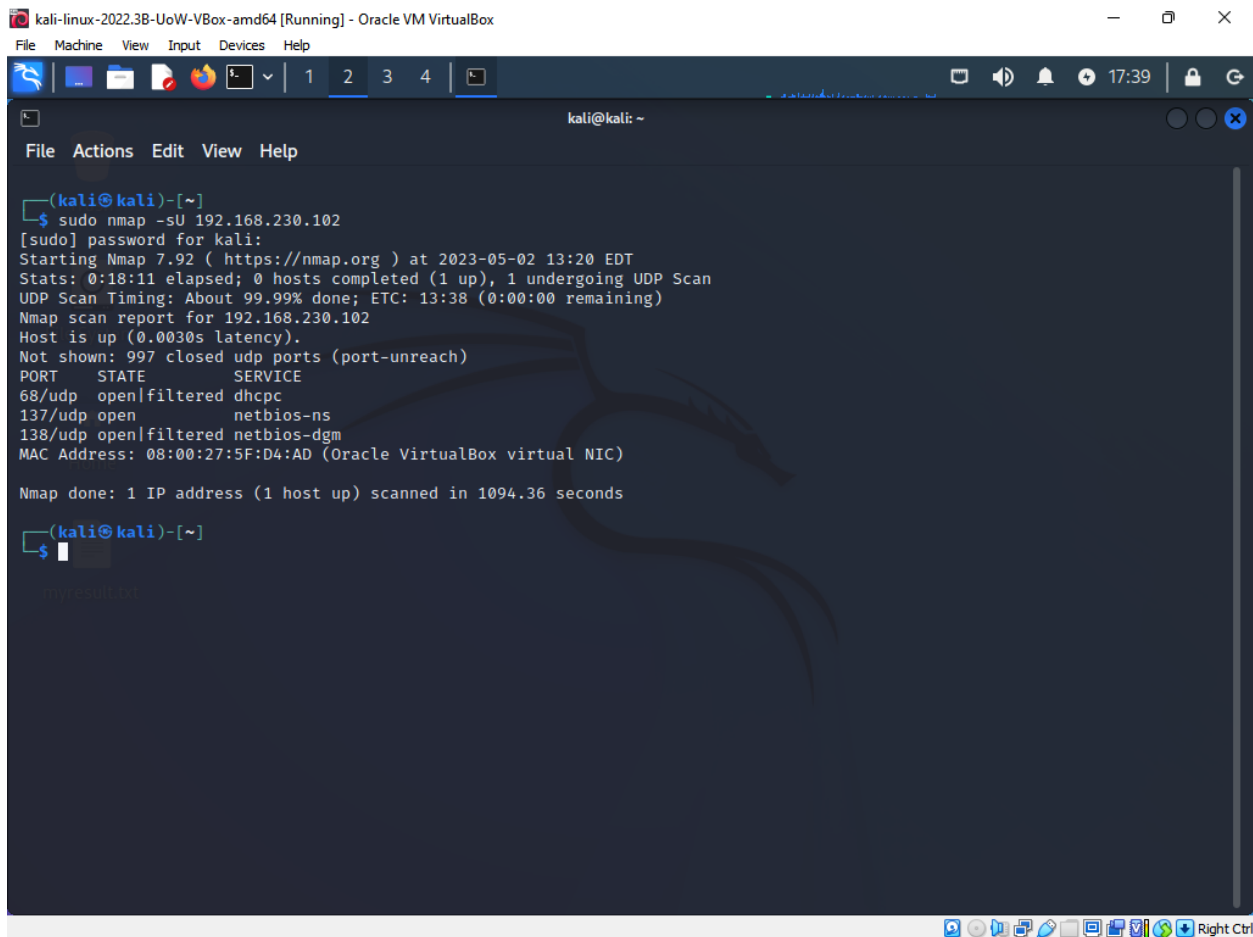
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.68 seconds
(kali@kali)-[~]
$
```

## UDP scan

Open UDP ports on the target machine may be discovered using UDP scanning. UDP, in contrast to TCP, lacks a handshake phase and is therefore a connectionless protocol, which makes it more challenging to identify available ports. As a result, UDP scans can aid in locating possible attack vectors, such as the existence of open services that listen on UDP ports.

Numerous vulnerabilities can result from open UDP ports, including:

Attackers can launch distributed denial of service (DDoS) attacks on target systems by saturating them with traffic by sending a lot of requests to open DNS servers, which then send responses to the target system.

A screenshot of a Kali Linux terminal window. The window title is 'kali-linux-2022.3B-UoW-VBox-amd64 [Running] - Oracle VM VirtualBox'. The terminal shows the execution of the command 'sudo nmap -sU 192.168.230.102'. The output includes the Nmap version (7.92), the start time (2023-05-02 13:20 EDT), and the scan results for 192.168.230.102. The results show that the host is up, with 997 closed UDP ports. Open ports are listed: 68/udp (open/filtered, dhcpc), 137/udp (open, netbios-ns), and 138/udp (open/filtered, netbios-dgm). The MAC address is 08:00:27:5F:D4:AD (Oracle VirtualBox virtual NIC). The scan took 1094.36 seconds.

```
(kali@kali)-[~]
$ sudo nmap -sU 192.168.230.102
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-02 13:20 EDT
Stats: 0:18:11 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 13:38 (0:00:00 remaining)
Nmap scan report for 192.168.230.102
Host is up (0.0030s latency).
Not shown: 997 closed udp ports (port-unreach)
PORT      STATE      SERVICE
68/udp    open/filtered dhcpc
137/udp   open       netbios-ns
138/udp   open/filtered netbios-dgm
MAC Address: 08:00:27:5F:D4:AD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1094.36 seconds

(kali@kali)-[~]
$
```

## Threats an open port can potentially causes

A port is a communication endpoint in networking that allows several processes to connect with one another on a computer or network. A network port that is open on a computer is one that is watching for incoming network traffic. A port being open indicates that a particular service or application is active and ready to receive incoming traffic on that port.

A network or computer system may be at risk of security breach due to open ports. Open ports can be used by attackers to gain unwanted access to a machine or network. An attacker may, for example, use a port scanner program to look for open ports on a target network before utilizing that information to start an attack. If an attacker finds an open port attached to a service or application, they may be able to use that vulnerability to gain unauthorized access to the system.

Additionally, denial of service attacks (DoS) can be launched against networks or systems through open ports. An attacker could flood the network by flooding the network with traffic sent to an

open port, causing the system to become unresponsive. Malware may also interact with distant servers over open ports or proliferate throughout a network.

## **Scenario assessment**

Because they offer a potential point of entry for attackers to access a network or system, open ports can be risky. A port that is open indicates that a certain service is active and watching for incoming connections on that port. Unauthorized access to the system may be possible as a result of a flaw in the service.

For example, a web server listening on port 80, the default port for HTTP, could be attacked if a port is open. It is possible for an attacker to execute arbitrary code on the web server if it has a defect that permits remote code execution.

Many open ports were discovered during a port scan in the context of the Green Grocers scenario, the risk would depend on the particular services that were using those ports and whether or not they had any known vulnerabilities that might be exploited. For instance, port 3306, the default port for MySQL, was open, a hacker may try to use a known weakness in MySQL to access the Green Grocers database and steal customer and farmer data.

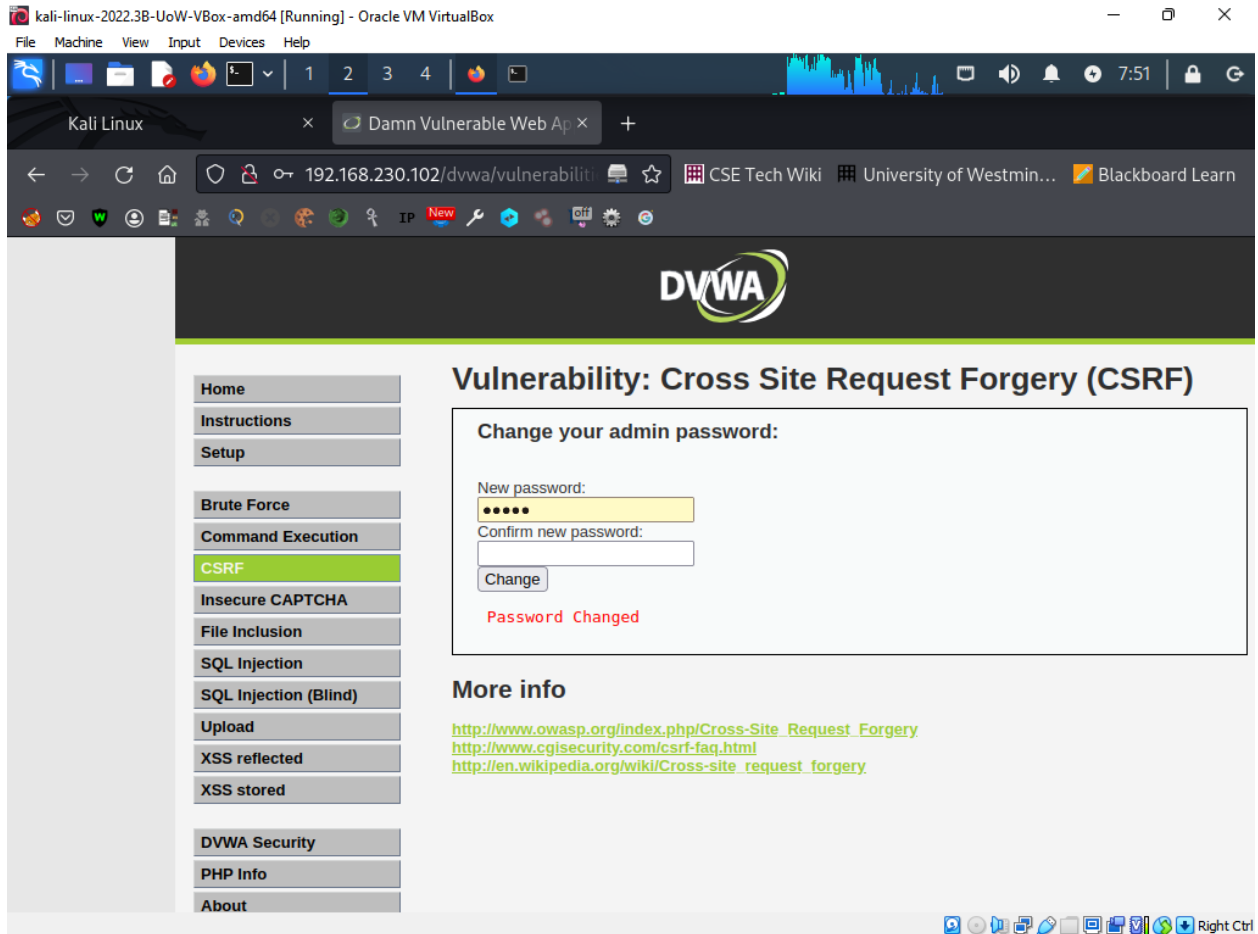
## **B. Server-side exploits**

### **i. Data tampering**

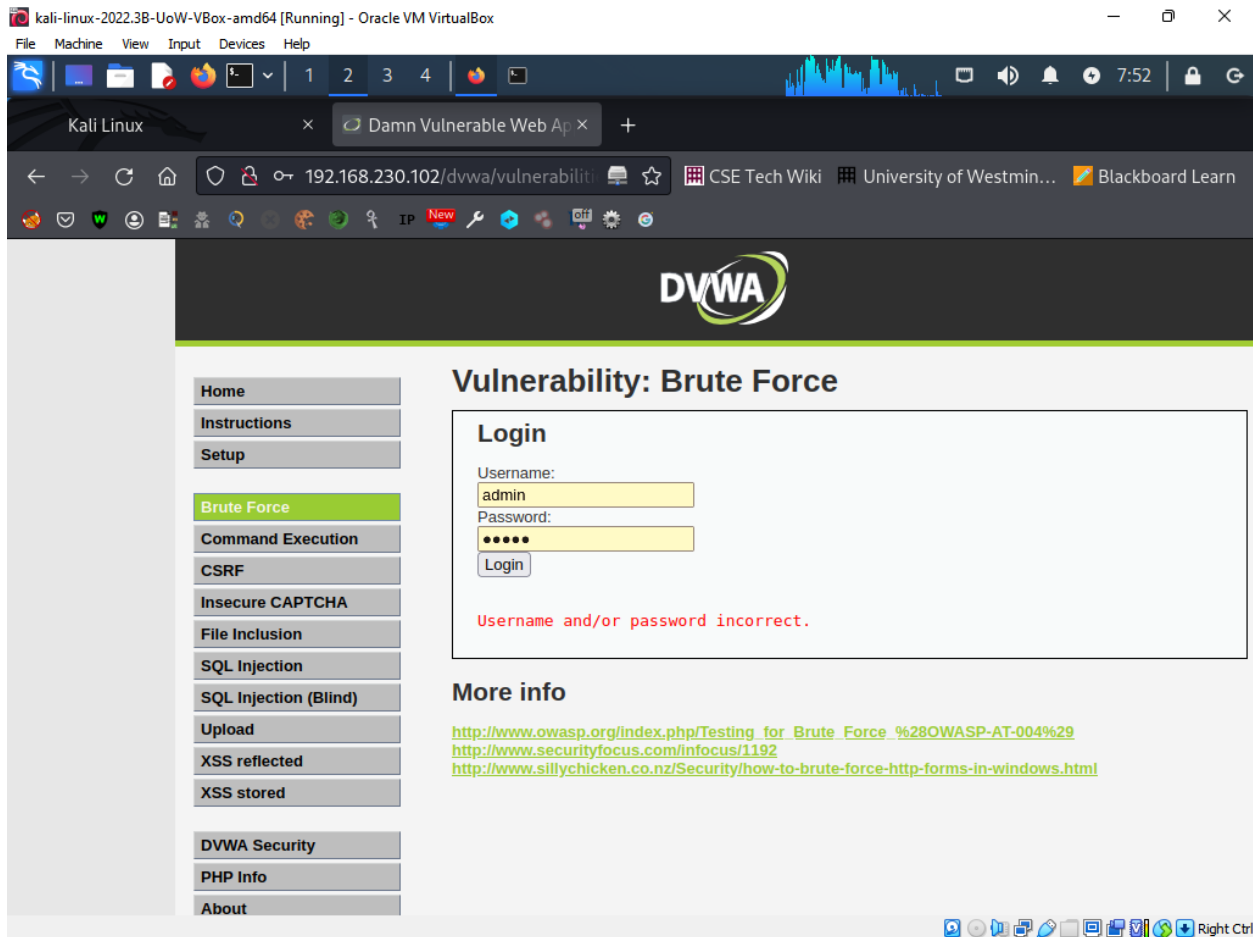
The application is vulnerable to data tampering because from the Cross-Site Request Forgery (CSRF) screenshot, one can change a user password hence kicking the legal user from accessing the intended information.

The attacker is often able to carry out illegal tasks on behalf of a victim user who has previously authenticated to a weak online application. When the password is changed then the intruder is able to tamper with the data such that the processes are no longer working as intended.





We go in a extent of verifying if the password is truly changed and for sure the previous password of the admin is no longer correct hence the admin cannot access the application anymore. This shows that the intruder now has access to the application as an administrator hence can change any data or protocols set.



## 1. Data tampering vulnerability

Data tampering, a type of cyberattack, entails the modification or change of data in order to undermine the intended functionality of a system or service. Data can be altered at any time, whether it's being transferred, currently at rest, or after it's been added to the system.

Attacks that alter data can have major repercussions, including erroneous choices, financial losses, and even bodily injury. For instance, tampering with medical records by an attacker might lead to inaccurate diagnoses or treatment choices.

The integrity tenet of cyber security is broken when data is tampered with. Data and systems must be shielded from unauthorized alteration or erasure, according to the integrity concept. Attacks on data integrity violate its integrity by altering information in ways that weren't intended, in violation of the integrity tenet.

To prevent efforts at data manipulation, organizations can employ a range of security measures, such as encryption, access limits, and intrusion detection systems. The implementation of rules

and processes for preventing and countering such attacks, as well as user education on the risks of data tampering, are also essential. By taking these safeguards, organizations may lower the risk of data manipulation and protect the integrity of their systems and data.

### **Scenario assessment**

Customers' names, addresses, phone numbers, and payment information, as well as farmers' names, addresses, and bank account information for payments, are among the vulnerable information for data tampering that attackers may access in this situation. Attackers have the ability to change this data or introduce false information, such as altering payment information to reroute payments to their own accounts or altering farmer information to reroute orders to their own items.

Such assaults may have serious repercussions for greengrocers. For instance, attackers can steal payment information and dollars from customers if they alter payment data. Green Grocers might suffer reputational harm and financial losses if they falsify farmer information and trick consumers into purchasing false goods. Additionally, if attackers alter customer data, this may violate privacy laws, cause customers to lose faith in the business, and hurt its reputation and bottom line.

## **2. SQL injection**

Attackers might use SQL injection vulnerabilities to access and change databases in unanticipated ways, potentially revealing sensitive data and jeopardizing the security of both the application and the system as a whole. From the below evidence, the attacker is able to obtain sensitive information on users stored in the database such that he knows the user ID, First name, and surname. This leads unauthorized data access whereby hackers can access private information contained in the database, such as user passwords, personally identifiable information (PII), and financial information, by using SQL injection.



- Home
- Instructions
- Setup

### Instructions

### Instructions

### Setup

## Brute Force

## Command Execution

CSRF

## Insecure CAPTCHA

## File Inclusion

## SQL Injection

## SQL Injection (Blind)

**Upload**

XSS reflected

XSS stored

## DVWA Security

PHP Info

## About

```
ID: 1
First name: admin
Surname: admin
```

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>  
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

kali-linux-2022.3B-UoW-VBox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Kali Linux x Damn Vulnerable Web App x +

192.168.230.102/dvwa/vulnerabilities/s CSE Tech Wiki University of Westmin... Blackboard Learn

**DVWA**

**Vulnerability: SQL Injection**

Home  
Instructions  
Setup

Brute Force  
Command Execution  
CSRF  
Insecure CAPTCHA  
File Inclusion  
**SQL Injection**  
SQL Injection (Blind)  
Upload  
XSS reflected  
XSS stored

DVWA Security  
PHP Info  
About

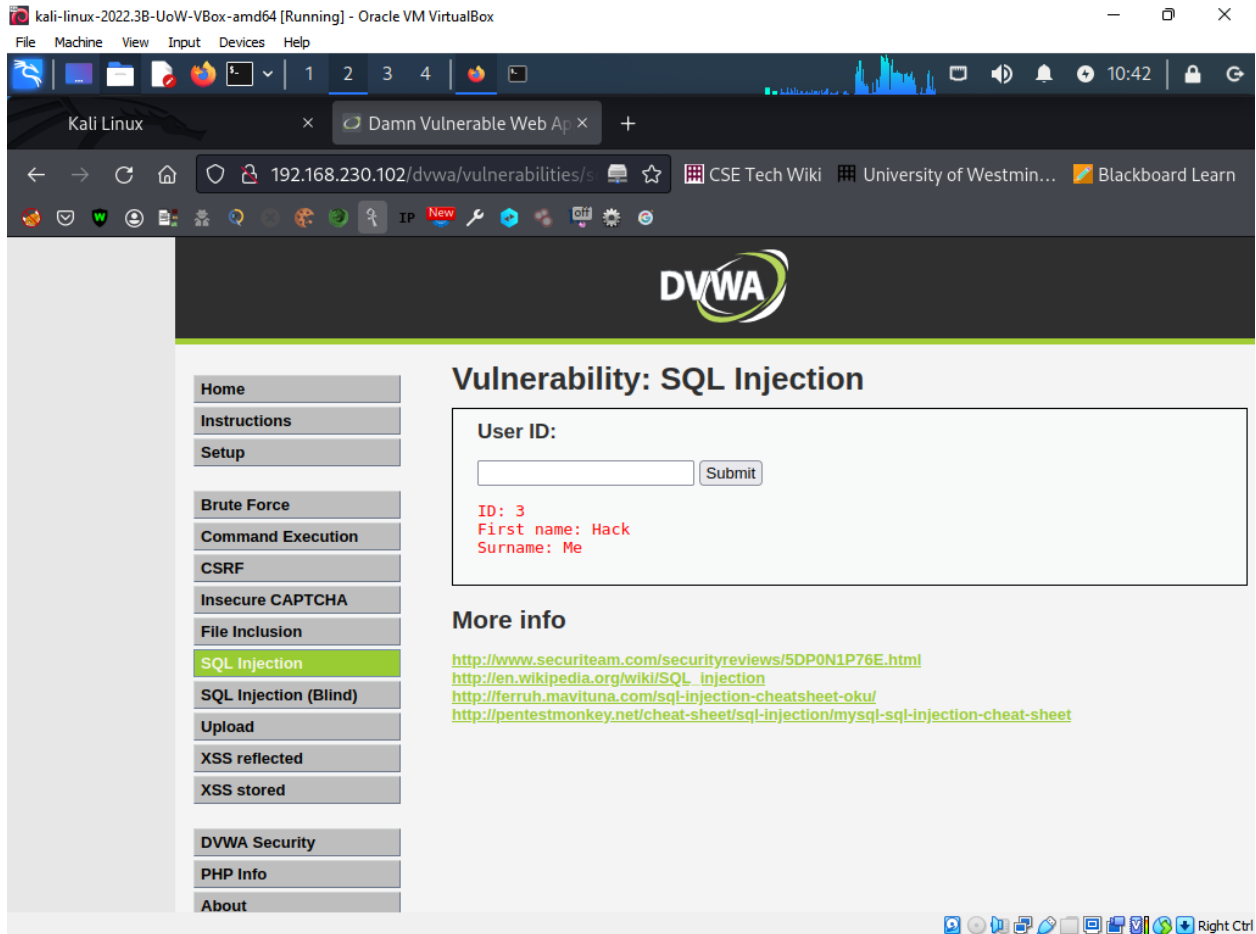
**User ID:**

ID: 2  
First name: Gordon  
Surname: Brown

**More info**

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>  
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Right Ctrl



## SQL Injection Vulnerability

The security flaw known as SQL injection occurs when an attacker inserts malicious SQL code into an application's input fields to access and take control of the database. A vulnerability occurs when an application doesn't properly sanitize or check the user's input before sending it to the database.

Attackers can manipulate or remove data, steal sensitive information, and run unauthorized instructions on the application's database via SQL injection. They can take advantage of this weakness to get access to the application's backend, get through authentication safeguards, and compromise the whole system.

The CIA (Confidentiality, Integrity, and Availability) triangle of cyber security principles is broken by SQL injection. Because it makes it possible for attackers to manipulate and change the data stored in the application's database, jeopardizing its accuracy and dependability, it violates

the Integrity tenet. Additionally, it violates the confidentiality tenet by giving attackers access to private information stored in the database, including login credentials, financial information, and personal data. SQL injection also violates the Availability tenet since it can lead to a denial of service (DoS) attack that makes the system inaccessible to authorized users.

### **Scenario assessment**

Attackers may be able to access sensitive data from the company's database, including customer information, order specifics, and farmer information, if the Green Grocers website is susceptible to SQL injection attacks. Attackers may get access to and change the company's database by using SQL injection techniques to get beyond authentication and authorization checks, which might result in data theft, data manipulation, or website defacement.

If attackers are successful in using SQL injection flaws in the case of Green Grocers, they will have access to the database that contains information on customers, including names, addresses, phone numbers, and payment information, as well as information about farmers, including names, addresses, and bank account information for payments. These details may be used by the attackers for illegal activities including identity theft, financial fraud, or the sale of the data on the dark web.

Additionally, hackers have the ability to change or remove data from the database, which could cost the business money or harm its reputation. To redirect payments to their own account, an attacker, for instance, may alter the cost of the goods or the farmers' bank account information.

### **3. XSS Scripting**

Attackers can insert harmful scripts into a trustworthy website when it is susceptible to XSS (Cross-Site Scripting) assaults, and unwary visitors can then execute the scripts while they browse the page. This may lead to a variety of information and vulnerabilities. Our application is vulnerable since we are able to inject some messages in to the website and it signed the message to the guestbook. This means if it was a malicious script, then the website could be attacked,

kali-linux-2022.3B-UoW-VBox-amd64 [Running] - Oracle VM VirtualBox

FileMachineViewInputDevicesHelp

1234

17:12

Kali Linux × Damn Vulnerable Web Ap × +

192.168.230.102/dvwa/vulnerability...CSE Tech WikiUniversity of Westmin...Blackboard Learn

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

format this computer

Sign Guestbook

Name: test  
Message: This is a test comment.

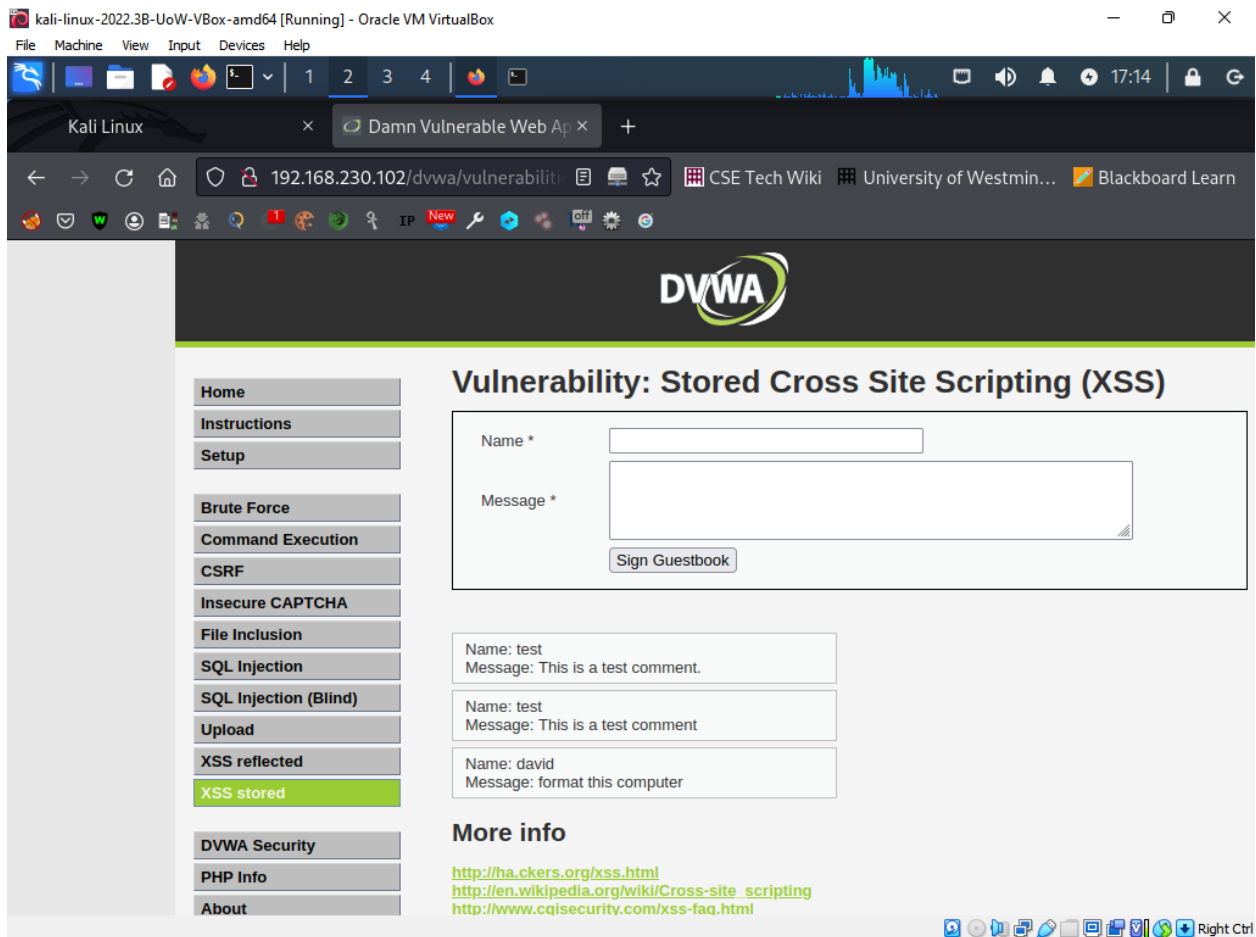
Name: test  
Message: This is a test comment

### More info

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

Right Ctrl





## XSS scripting vulnerability

Attacks that inject malicious code into web pages that other users are viewing are known as XSS (Cross-Site Scripting) or XSS. If an application fails to properly validate user input and output, attackers can inject their own code that runs in the context of other users' browsers.

The two types of XSS are stored XSS and reflected XSS. The malicious code that an attacker installs into a website is stored permanently on the server and executed each time a user views that page. Stored XSS is what this is. When a user is duped into clicking on a link that includes malicious code, the malicious code is then run in the user's browser, resulting in reflected XSS.

XSS vulnerabilities may be used to obtain login credentials, session tokens, and contact information from other users. Additionally, attackers can use XSS to alter a web page's content, send users to risky websites, and perform other nefarious deeds.

The cyber security principles of Confidentiality and Integrity are broken by XSS. By enabling attackers to obtain private information from other users and by enabling them to alter web page content without authorization, it breaches both confidentiality and integrity.

### **Scenario assessment**

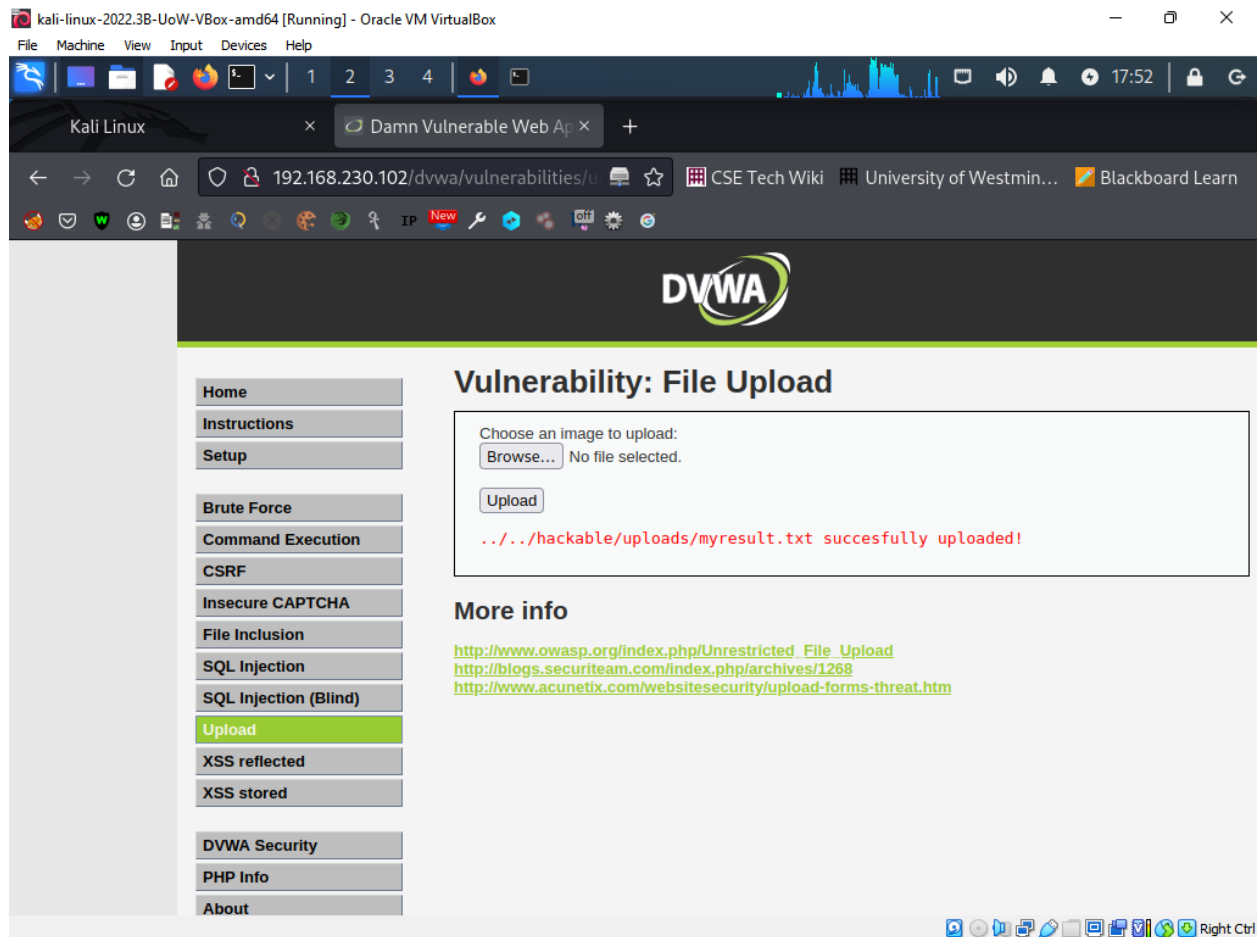
For instance, a hacker may include a script that takes the login information from customers or farmers who input it on the harmed page. The attacker might then access the victim's account using these credentials, get their personal information and payment information, and perhaps engage in fraudulent activity.

An XSS attack might provide hackers access to session cookies, which the website uses to identify and authenticate users, in addition to login information. An attacker might successfully impersonate the victim and do activities on their behalf, such placing orders or changing their account information, with the use of a stolen session cookie.

Overall, a significant XSS vulnerability in the Green Grocers website might result in identity theft, financial loss, and harm to the company's reputation, which would be bad for both consumers and farmers. Therefore, it is crucial for the business to guarantee that XSS attacks are prevented and its website is secure.

## **4. Other OWASP vulnerable machine vulnerabilities exploited.**

Other vulnerability exploited was file upload vulnerability whereby an attacker can upload a Delivery of malware: Attackers have the ability to upload harmful files like viruses, worms, or Trojan horses that can infect the server or the devices of other users, compromising data and systems. Attackers may upload enormous files that suck up server resources, slowing down or crashing the server and denying access to legitimate users. This is known as a denial-of-service attack. In our case we uploaded a file and was successfully uploaded to the server.



Another vulnerability exploited is Insecure CAPTCHA. An application's CAPTCHA mechanism is not safe and is readily circumvented by attackers if it is exposed to an insecure CAPTCHA flaw. As a result, attackers are able to access the application without authorization, launch automated assaults like brute-force attacks, and engage in a variety of destructive actions.



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

## Vulnerability: Insecure CAPTCHA

reCAPTCHA API key NULL in config file.

Please register for a key from reCAPTCHA at <https://www.google.com/recaptcha/admin/create> and set the key in the file `/owaspbwa/dvwa-svn/config/config.inc.php`

New password:

.....

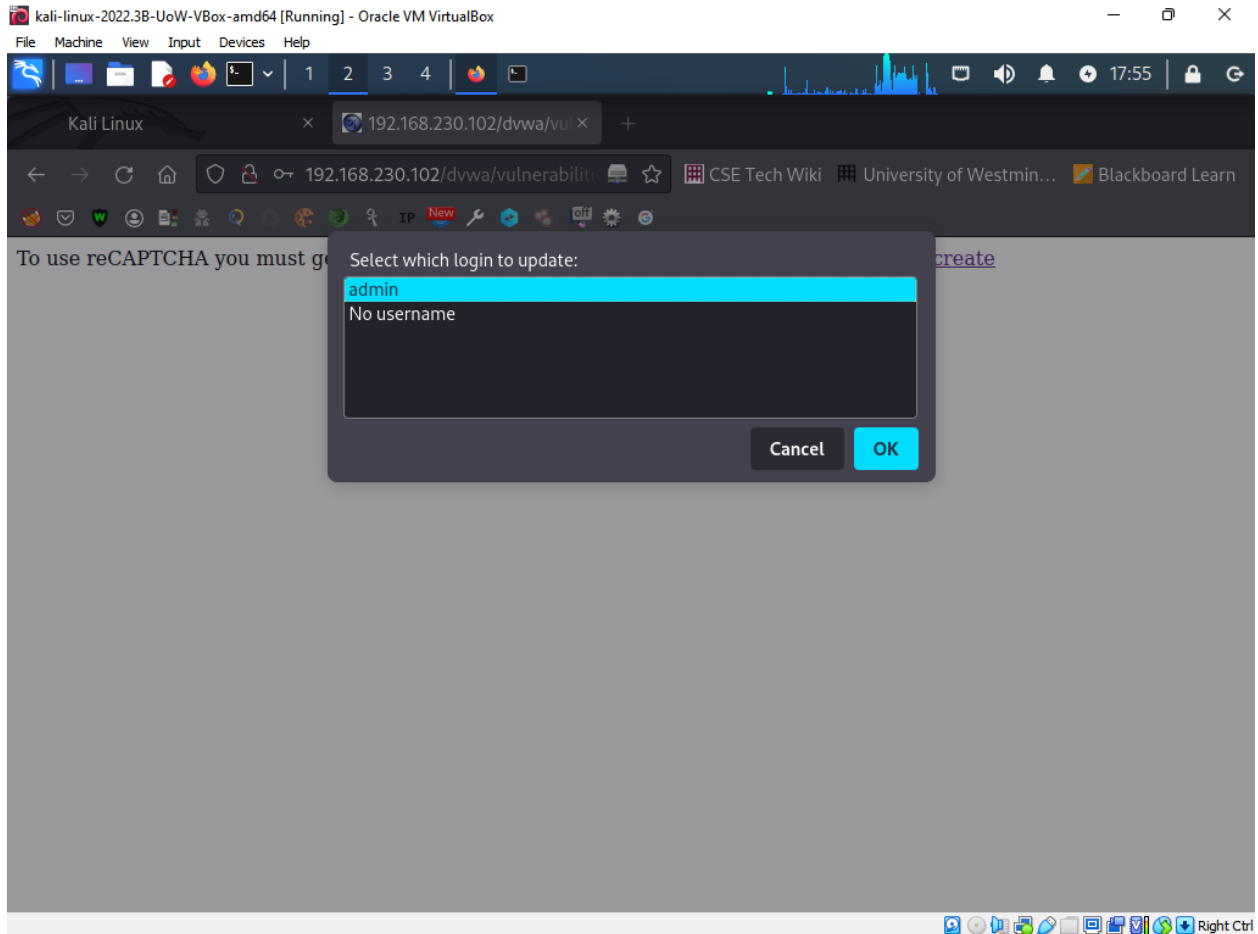
Confirm new password:

.....

Change

### More info

<http://www.captcha.net/>  
<http://www.google.com/recaptcha/>



## Scenario assessment

**Insecure CAPTCHA implementation:** If the website uses a CAPTCHA that is not secure, automated bots may be able to get around the authentication procedure and make phony accounts and orders. Financial losses and reputational harm to the business may result from this.

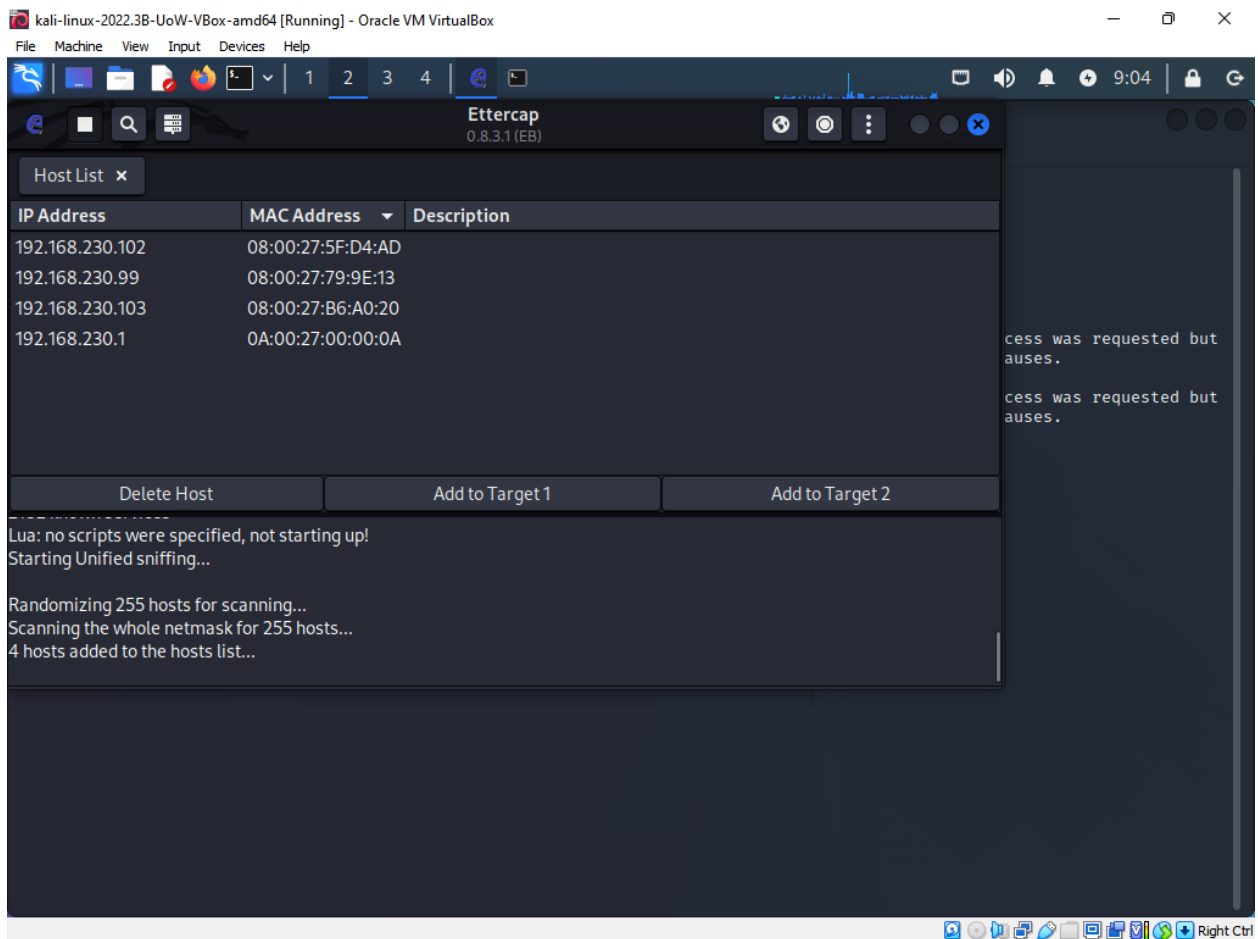
**File Upload Vulnerabilities:** Attackers may upload harmful files to the website, such as malware or web shells, thanks to file upload vulnerabilities. These files have the potential to steal confidential information, interfere with website functionality, or provide unwanted access to the website's backend.

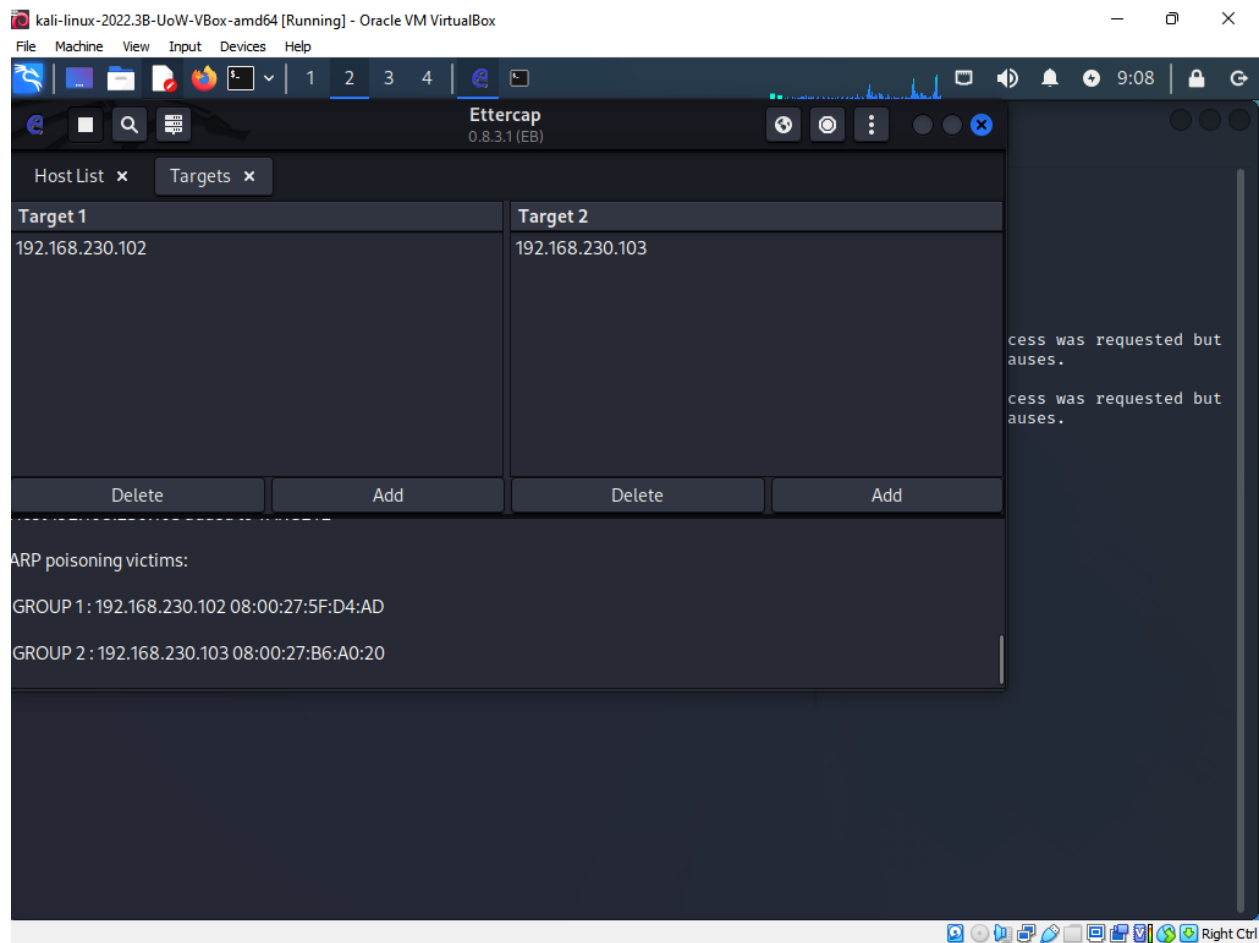
## C. Client-side exploits

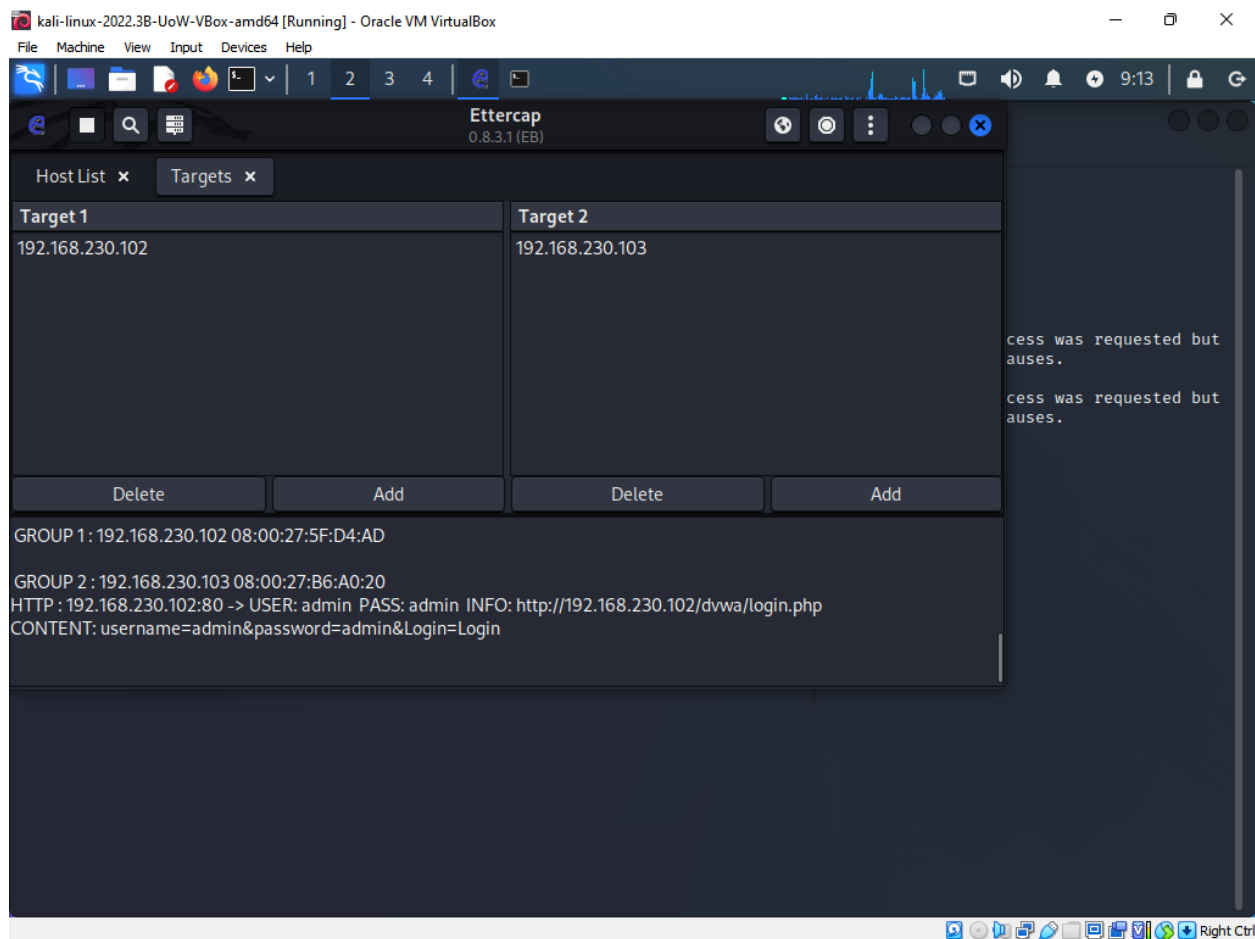
### 1. Man in the Middle Attack (MiTM)

A Man-in-the-Middle (MiTM) attack involves the attacker intercepting two parties' communications in order to listen in, steal data, or change the flow. Here's how an attacker may intercept traffic from a session between a legitimate user and the application's server side:

For our case we are able to steal sensible data such that we are able to identify the username and password for the OWASP VM.







## 2. Social engineering attack

"Phishing" is a popular social engineering technique that an attacker might employ to seduce a regular user to their computer rather than the server machine. An email or message that pretends to be from a reliable source, such the victim's bank or an online service provider, is sent to them by the attacker in a phishing assault (Salahdine and Kaabouch 2019). The message often contains a link that directs the user to a fake website that mimics the actual one.

The moment the victim clicks the link and enters their login information or other sensitive data, the attacker can get hold of that information and use it to either steal the victim's identity or get unauthorized access to their account.

"Baiting" is a different type of social engineering technique that an attacker might employ to entice a person to their computer. A USB drive or other physical object may be left in a public area with a label or message that tempts the victim to pick it up and insert it into their computer in a baiting



attack. By doing this, the victim gives the attacker access to their computer, giving them the opportunity to steal sensitive information or introduce malware.

In both scenarios, the attacker seeks to exploit the victim's trust or curiosity in order to breach their security.

### **Scenario assessment**

Social engineering attacks might be used in the Green Grocers scenario to persuade consumers to divulge private information like login passwords or financial information. For instance, a potential attacker may phone consumers and claim to be from Green Grocers while requesting their account details to address a purported issue with their purchase. The attacker may also impersonate Green Grocers in phishing emails, asking recipients to click a link to update their account information.

Social engineering assaults have the potential to do the company and its clients serious harm if they are successful. Attackers could get into client accounts, take their money, and use it to make fraudulent purchases. They could also sell data on the dark web, utilize it for phishing schemes, or steal people's identities.

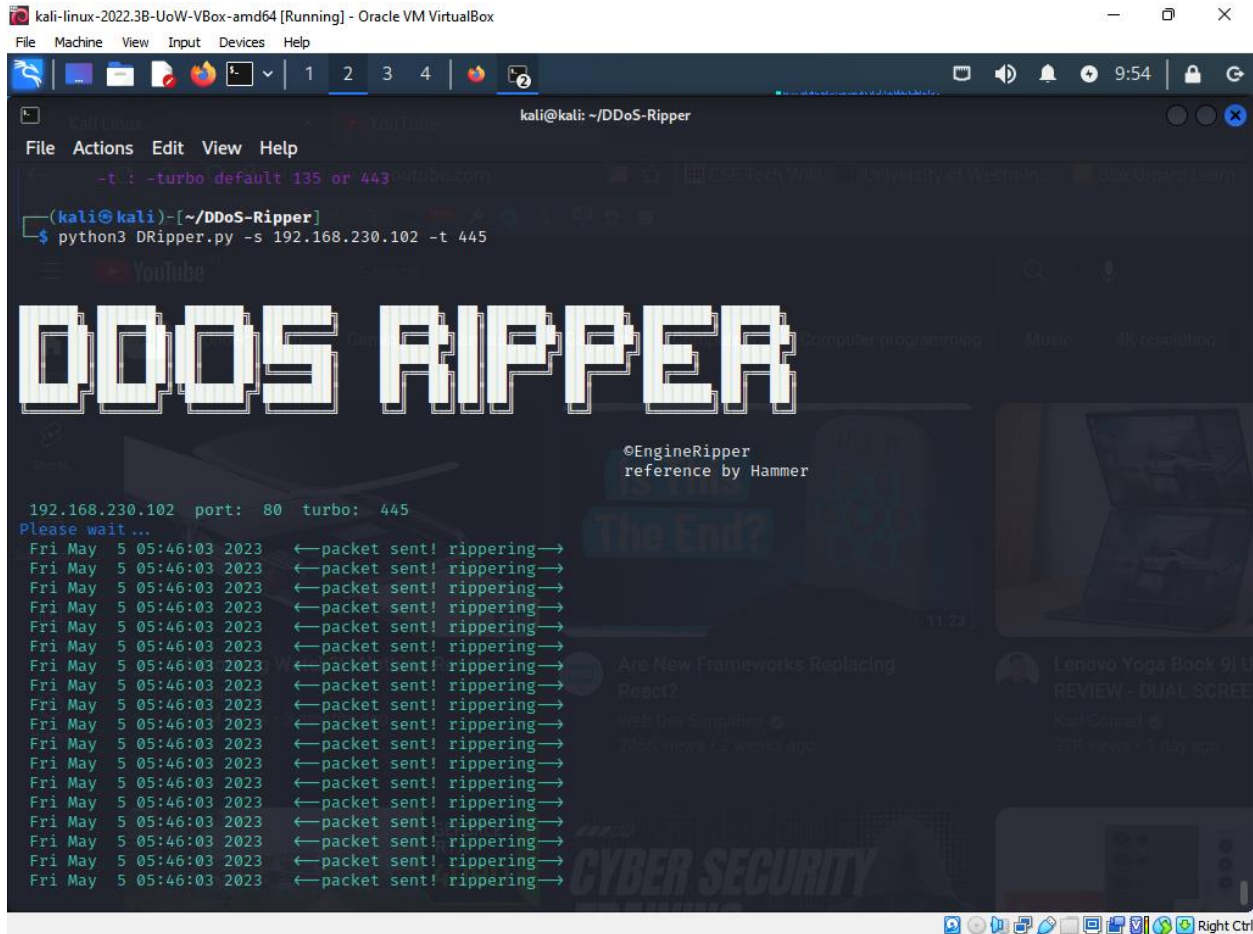
Additionally, social engineering assaults can harm Green Grocers' brand, losing the company customers' confidence and eventually damaging its bottom line. In order to safeguard against social engineering attacks, the business must put in place safeguards including staff education and awareness training, two-factor authentication, and email filtering systems to identify and prevent phishing emails.

## **D. Denial of Service attacks**

### **1. DoS the web server**

Here are a few techniques an attacker may use to launch a DoS attack on a web server:

**Ping Flood Attack:** In this form of DoS attack, the target server is bombarded with many ping requests from the attacker. The website will become inaccessible as a result of the server's inability to respond to valid requests since it will be too busy handling these requests. As for our case one can launch the attack on the webserver as such:



Attacks that cause a denial of service breach the cybersecurity principle of availability, which guarantees that authorized users have timely and uninterrupted access to the data and services they require.

## Scenario assessment

A Ping Flood Attack on Green Grocers' web server might have a major effect on the business. Customers could be unable to access the website, make purchases, or send money, and farmers might be unable to submit their goods or control their inventory. Customers and farmers may lose faith in the platform's dependability and security as a result of the website's outage, harming the company's image. The sensitive data kept in the database, such as client payment information, may also be compromised if the attack ends in a data breach, resulting in financial loss and reputational harm.

## **E. Recommendations to protect the scenario company server**

When testing a web application, the following actions may be performed to reduce risks to the findings from the reconnaissance phase:

1. Watch the website: Monitoring the website's traffic and activity will enable you to notice any odd or unlawful behaviour.
2. Encrypt all correspondence: All connections between a website and a user should be secured using secure protocols like HTTPS to prevent data eavesdropping and manipulation.
3. Use two-factor authentication, third. Two-factor authentication can assist in preventing unauthorized access to the website and its backend by demanding an additional form of identification in addition to a username and password.

By permitting access to network services only after a predetermined series of connection attempts to a set of restricted ports has been successful, port knocking is a technique used to secure network services. In other words, the method necessitates a specified order of port knocks before allowing access to a given service. The knock code is the name given to this pattern. By obscuring open ports and services and making it harder for attackers to find them, port knocking can aid in preventing unwanted access to a network (Jeanquier, 2006). Attackers find it more challenging to target vulnerabilities when they cannot readily determine which services are operating on the network because the ports are blocked and unreachable until the proper knock code is supplied.

You may put the following precautions into practice to safeguard your database from SQL injection:

1. Make use of a web application firewall (WAF): By examining incoming traffic and use patterns, a WAF may detect and prevent attempts at SQL injection. A WAF can aid in defending against further assaults.
2. Keep software up to current: To make sure that known vulnerabilities are patched, keep your database and application software up to date. To find and categorize vulnerabilities in your system, use security software (Wei et al. 2006).

3. Regularly test your program: Check your application frequently for security holes, such as SQL injection. Use techniques like code reviews and penetration testing to find vulnerabilities and repair them before attackers can take advantage of them.

There are several approaches to protect a web application from Cross-Site Scripting (XSS) attacks:

1. The first step in preventing XSS attacks is sanitizing and verifying user input. This is performed server-side. This entails reviewing every input data to make sure it complies with expectations and eliminating any potentially injected harmful code.
2. Encoding all output data before presenting it to the user is another efficient method of preventing XSS attacks. Encoding transforms special characters into their equivalents in HTML or JavaScript, making it more challenging for attackers to insert harmful code (Nithya et al. 2015).
3. Web developers may determine which content sources, such as stylesheets and scripts, are trusted by using the Content Security Policy (CSP) security mechanism. By limiting the execution of material to only those from reliable sources, this can help avoid XSS attacks.

Several actions may be taken by a security analyst to thwart or lessen the effects of a Man in the Middle (MITM) attack. Among these activities are:

1. Encryption: Securing communications using encryption is one of the best ways to defend against MITM attacks. This entails encrypting data in transit using secure protocols like HTTPS, SSL/TLS, and IPsec. A successful MITM attack is less likely if encryption is used since attackers won't be able to intercept and read sensitive data.
2. Implementing a Public Key Infrastructure (PKI) can assist defend against MITM attacks. The legitimacy of each party taking part in a communication is verified and authenticated by a PKI, which is a system of digital certificates, certificate authorities, and other registration authorities (Ekparinya et al. 2018). This can lessen the likelihood of an MITM attack by assisting in preventing attackers from posing as trustworthy sources.
3. Two-Factor Authentication (2FA): Using 2FA can lessen the impact of an MITM attack and assist prevent unwanted access to systems. This entails confirming a user's identification using both something they possess and something they know (such a mobile phone or a password). Even if the user's password is intercepted by an attacker, they won't be able to get into the system without the second factor.

The following steps should be taken by businesses to protect themselves from social engineering attacks:

1. Implement strong authentication safeguards: Use multi-factor authentication (MFA) to confirm that users are who they claim to be. This can prevent an attacker from accessing systems and data even if they have the user's password.
2. Maintain current software and hardware: Ascertain that the most recent security patches and upgrades are installed on all systems and applications. By doing this, attackers may be deterred from using known vulnerabilities.
3. Conduct routine security audits: To find and fix weaknesses in systems and procedures, conduct routine security audits. Through the detection and correction of security infrastructure weak points, this can assist avoid social engineering attacks (Salahdine and Kaabouch 2019).

Businesses may defend their online services from DoS attacks by putting in place a number of preventive measures.

1. Implement network-level security measures: Network-level security measures can assist in traffic filtering and blocking traffic from known malicious sources (Mahjabin et al. 2017). Examples include firewalls, intrusion prevention systems (IPS), and load balancers. These precautions can aid in preventing the web service from being overloaded by the attack traffic before it ever reaches it.
2. Utilize Content Delivery Networks (CDNs): By distributing traffic across several servers, CDNs stop an assault from swamping any one server. Additionally, a CDN can offer traffic filtering and DDoS protection as extra security measures.
3. Implement rate limitation to prevent attackers from deluging the service with a huge number of requests. Rate limiting restricts the number of requests that may come from a single IP address.

#### Intrusion Detection and Prevention systems

The following are a few examples of firewall and iptables rules that help defend Green Grocers from the aforementioned attacks:

1. Data tampering: The following iptables rule may be used to prevent data tampering attacks by limiting access to the server's port for unapproved IPs:

```
iptables -A INPUT -p tcp --dport 80 -s ! 192.168.230.102/24 -j DROP
```

2. SQL injection: To stop incoming SQL requests, you can use firewall rules to prevent SQL injection attacks. (Šimon et al. 2015):

```
sudo ufw deny from any to any port 3306
```

3. XSS scripting: To stop XSS assaults, incoming JavaScript code can be blocked by a firewall rule:

```
sudo ufw deny from any to any port 80 proto tcp
```

4. Man-in-the-middle: To stop Man-in-the-middle attacks, a firewall rule may be used to prohibit non-authorized IPs from accessing the server's port:

```
iptables -A INPUT -p tcp --dport 443 -s ! 192.168.230.102/24 -j DROP
```

Firewall and iptables evaluation:

Iptables and firewalls are both effective defenses against assaults on web services. Iptables, on the other hand, is more adaptable and offers more flexibility over the rules that may be used (Šimon et al. 2015). It also allows for the development of complex rule sets that protect against a range of threats and is more adaptive. However, firewalls often have an easier to use interface and are more straightforward to utilize. Iptables would be better appropriate for a company like Green Grocers owing to its flexibility and increased control.

IDS and IPS distinctions include:

Although both IDS and IPS are used for network security, their capabilities vary. An IDS is a device that scans network traffic for indications of malicious activity and issues alarms when it does (Ashoor and Gore 2011). It is a passive device that does not purposefully obstruct traffic. However, when it discovers harmful behavior, an IPS is a program that actively stops communications. Compared to an IDS, it is a more proactive tool.

## **Scenario assessment**

It is advised for Green Grocers to utilize both IDS and IPS to defend against the discovered attacks. An IPS can actively restrict traffic when it detects harmful behavior, but an IDS can monitor the website's traffic and provide notifications when it finds any dangerous activity. This will offer a multi-layered security strategy and assist in reducing the effect of any successful assaults. To make sure the system is safe and up to date with the most recent security updates, frequent vulnerability scans and penetration tests should also be performed.

## References

- Dokman, T. and Ivanjko, T., 2020. Open source intelligence (OSINT) issues and trends. *The Future of Information Sciences*, 1(2020), p.191.
- Ekparinya, P., Gramoli, V. and Jourjon, G., 2018, October. Impact of man-in-the-middle attacks on ethereum. In *2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS)* (pp. 11-20). IEEE.
- Jeanquier, S., 2006. *An Analysis of Port Knocking and Single Packet Authorization MSc Thesis* (Doctoral dissertation, PhD thesis).
- Mahjabin, T., Xiao, Y., Sun, G. and Jiang, W., 2017. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, 13(12), p.1550147717741463.
- Nithya, V., Pandian, S.L. and Malarvizhi, C., 2015. A survey on detection and prevention of cross-site scripting attack. *International Journal of Security and Its Applications*, 9(3), pp.139-152.
- Salahdine, F. and Kaabouch, N., 2019. Social engineering attacks: A survey. *Future Internet*, 11(4), p.89.
- Šimon, M., Huraj, L. and Čerňanský, M., 2015. Performance evaluations of IPTables firewall solutions under DDoS attacks. *Journal of Appli*
- Wei, K., Muthuprasanna, M. and Kothari, S., 2006, April. Preventing SQL injection attacks in stored procedures. In *Australian Software Engineering Conference (ASWEC'06)* (pp. 8-pp). IEEE.