NAME : Shrishti Vishwakarma

CLASS : BVOC (First year) Sem 2

TITLE : Python-Based Vulnerability Scanner

INSTRUCTOR : Shubham sir

Table Of Content

INTRODUCTION

In today's digitally connected world, websites are frequent targets of cyberattacks. To proactively detect and mitigate security threats, organizations rely on vulnerability scanners that automate the identification of potential weaknesses in their web applications.

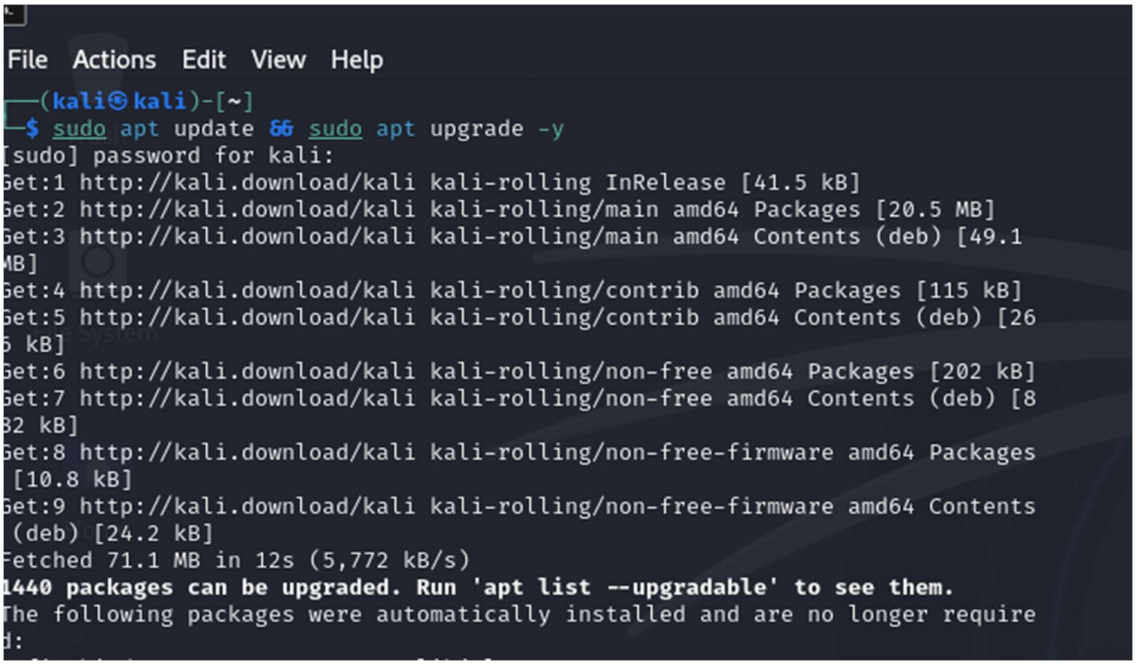
This project, titled "Python-Based Vulnerability Scanner (Web Vuln Scanner 1.0)", is a custom-built tool developed using Python. It is designed to scan websites for common and high-risk security vulnerabilities such as:

- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Open Redirects
- File Inclusion
- Cross-Site Request Forgery (CSRF)

The scanner performs intelligent crawling of the target website, analyzes parameters, and attempts various payloads to test for exploitable conditions.

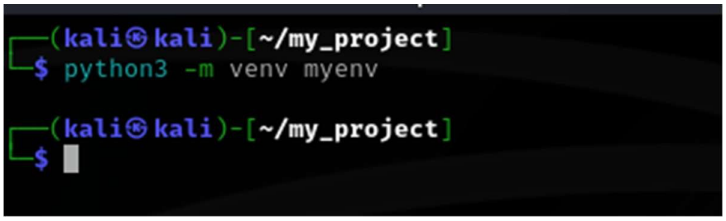
Result And Screenshot

1. using “sudo apt update && sudo apt upgrade -y” command to ensure if the system is updated.

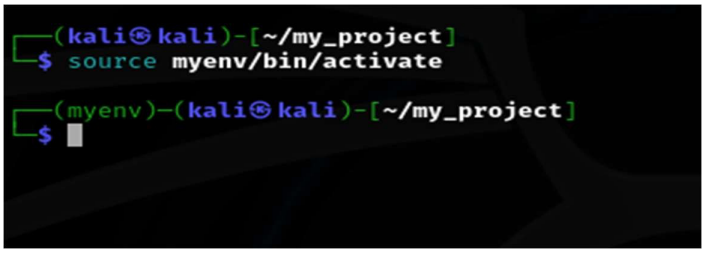


2. using “sudo apt install python3-venv” command to install python packages to create a virtual environment.

4. using “python3 -m venv myenv” command to create a folder in virtual environment.



5. using “source myenv/bin/activate” command to Activate the virtual environment to isolate your Python environment:



The (myenv) indicates that the virtual environment is active.

7. creating Using Sudo Nano a python file

```
┌──(myenv)─(kali㉿kali)-[~]
└─$ sudo nano scanner.py
```

8. Final Output

```
┌──(myenv)─(kali㉿kali)-[~]
└─$ python scanner.py http://testphp.vulnweb.com

[+] Starting scan of http://testphp.vulnweb.com
[*] Scan started at 2025-04-11 10:00:59.356185
[*] Verifying target...
[*] Crawling website...
```

After Scanning Result:

```
Web Vulnerability Scan Report
==================================================
Target: http://testphp.vulnweb.com
Date: 2025-04-10 13:48:01
Vulnerabilities Found: 38

[High] SQL Injection
URL: http://testphp.vulnweb.com/listproducts.php?cat='
Description: Parameter 'cat' appears vulnerable with payload: '
Timestamp: 2025-04-10 13:48:15
--------------------------------------------------
[High] SQL Injection
URL: http://testphp.vulnweb.com/product.php?pic='
Description: Parameter 'pic' appears vulnerable with payload: '
Timestamp: 2025-04-10 13:48:16
--------------------------------------------------
[High] SQL Injection
URL: http://testphp.vulnweb.com/listproducts.php?cat='
Description: Parameter 'cat' appears vulnerable with payload: '
Timestamp: 2025-04-10 13:48:16
--------------------------------------------------
[High] SQL Injection
URL: http://testphp.vulnweb.com/listproducts.php?artist='
Description: Parameter 'artist' appears vulnerable with payload: '
Timestamp: 2025-04-10 13:48:16
--------------------------------------------------
[High] SQL Injection
URL: http://testphp.vulnweb.com/product.php?pic='
Description: Parameter 'pic' appears vulnerable with payload: '
Timestamp: 2025-04-10 13:48:19
--------------------------------------------------
[High] SQL Injection
URL: http://testphp.vulnweb.com/product.php?pic='
Description: Parameter 'pic' appears vulnerable with payload: '
Timestamp: 2025-04-10 13:48:19
--------------------------------------------------
[High] SQL Injection
URL: http://testphp.vulnweb.com/listproducts.php?artist='
Description: Parameter 'artist' appears vulnerable with payload: '
Timestamp: 2025-04-10 13:48:19
```

TOOLS USED

1. Kali linux
2. Windows 11(host)
3. VMware
4. Google chrome

CONCLUSION

The Python-Based Vulnerability Scanner is a simple yet effective tool for detecting common web vulnerabilities like SQLi, XSS, and CSRF. It automates scanning, crawling, and reporting, making it useful for basic security assessments. This project highlights the importance of web security and the role of automation in identifying potential threats early.