

**NAME : Shrishti Vishwakarma**

**CLASS : BVOC (First year) Sem 2**

**TITLE : Python-Based Vulnerability Scanner**

**INSTRUCTOR : Shubham sir**

---

*Table Of Content*

---

**Introduction**

**Result and screenshots**

**Tools used**

**Conclusion**

---

## 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)

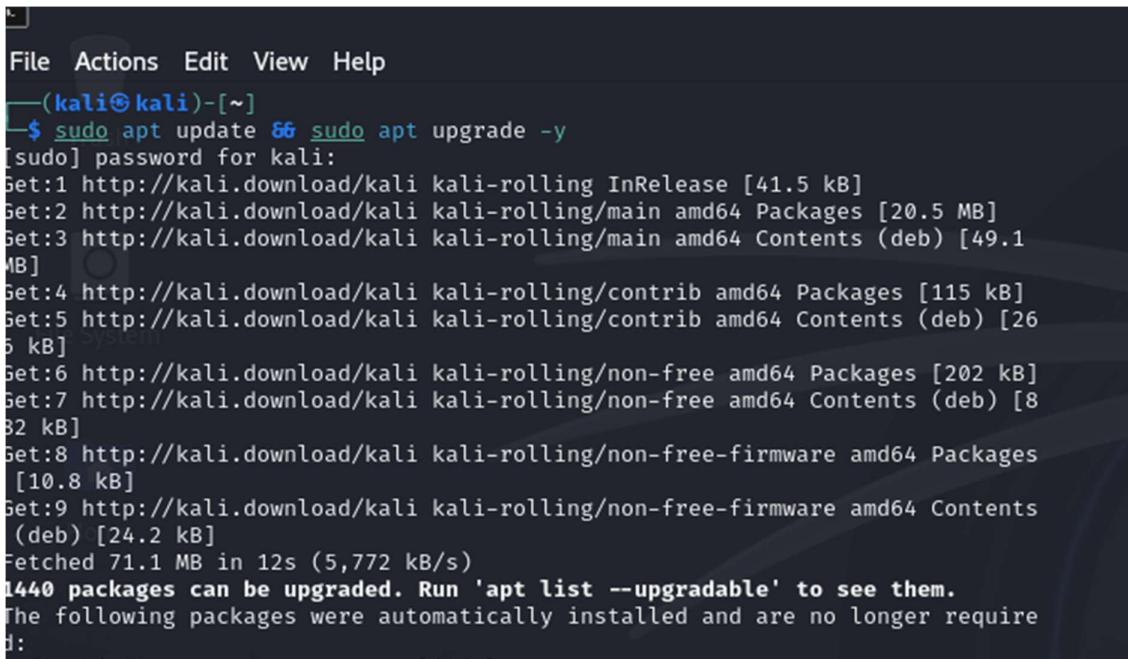
The scanner performs intelligent crawling of the target website, analyzes parameters, and attempts various payloads to test for exploitable conditions.

---

## *Result And Screenshot*

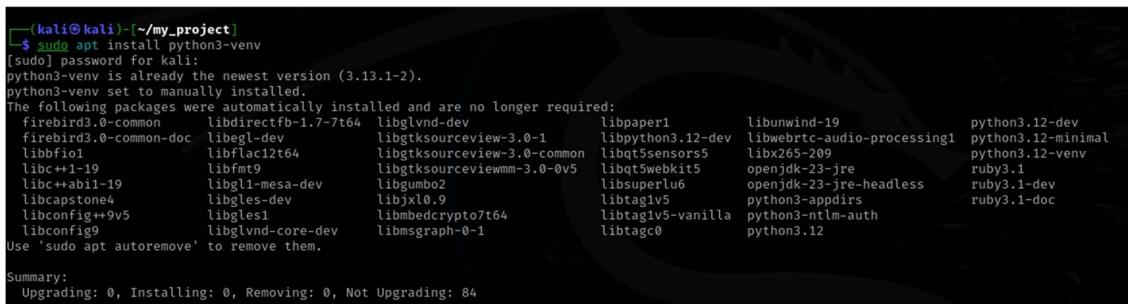
---

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



```
File Actions Edit View Help
└──(kali㉿kali)-[~]
$ sudo apt update && sudo apt upgrade -y
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.5 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.1
MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [26
5 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [202 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [8
32 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages
[10.8 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents
(deb) [24.2 kB]
Fetched 71.1 MB in 12s (5,772 kB/s)
1440 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer require
d:
```

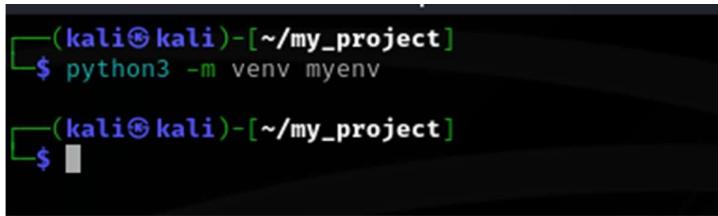
**2.** using “`sudo apt install python3-venv`” command to install python packages to create a virtual environment.



```
└──(kali㉿kali)-[~/my_project]
$ sudo apt install python3-venv
[sudo] password for kali:
python3-venv is already the newest version (3.13.1-2).
python3-venv set to manually installed.
The following packages were automatically installed and are no longer required:
 firebird3.0-common   libdirectfb-1.7-7t64  libglvnd-dev      libpaper1      libunwind-19    python3.12-dev
 firebird3.0-common-doc libegl-dev       libgtsourceview-3.0-1   libpython3.12-dev  libwebrtc-audio-processing1 python3.12-minimal
 libffiol             libflac12t64    libgtsourceview-3.0-common libqt5sensors5  libx265-209    python3.12-venv
 libc++1-19           libfmt9        libgtsourceviewmm-3.0-0v5  libqt5webkit5  openjdk-23-jre   ruby3.1
 libc++abi1-19        libgli-mesa-dev libgumbo2        libsuperlu6    openjdk-23-jre-headless ruby3.1-dev
 libcapstone4         libgles-dev     libjxl0.9       libtag1v5      python3-appdirs  ruby3.1-doc
 libconfig++9v5        libgles1       libmbcrypto7t64   libtag1v5-vanilla python3-nlml-auth
 libconfig9           libglvnd-core-dev libmsgraph-0-1    libtagc0       python3.12
Use 'sudo apt autoremove' to remove them.

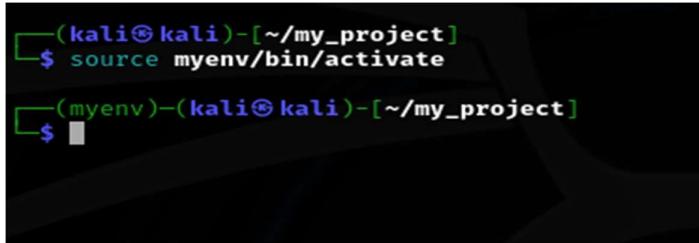
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 84
```

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



```
(kali㉿kali)-[~/my_project]
$ python3 -m venv myenv
(kali㉿kali)-[~/my_project]
$
```

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



```
(kali㉿kali)-[~/my_project]
$ source myenv/bin/activate
(myenv)@(kali㉿kali)-[~/my_project]
$
```

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:

```
1 Web Vulnerability Scan Report
2 =====
3 Target: http://testphp.vulnweb.com
4 Date: 2025-04-10 13:48:01
5 Vulnerabilities Found: 38
6
7 [High] SQL Injection
8 URL: http://testphp.vulnweb.com/listproducts.php?cat='
9 Description: Parameter 'cat' appears vulnerable with payload: '
10 Timestamp: 2025-04-10 13:48:15
11 -----
12 [High] SQL Injection
13 URL: http://testphp.vulnweb.com/product.php?pic='
14 Description: Parameter 'pic' appears vulnerable with payload: '
15 Timestamp: 2025-04-10 13:48:16
16 -----
17 [High] SQL Injection
18 URL: http://testphp.vulnweb.com/listproducts.php?cat='
19 Description: Parameter 'cat' appears vulnerable with payload: '
20 Timestamp: 2025-04-10 13:48:16
21 -----
22 [High] SQL Injection
23 URL: http://testphp.vulnweb.com/listproducts.php?artist='
24 Description: Parameter 'artist' appears vulnerable with payload: '
25 Timestamp: 2025-04-10 13:48:16
26 -----
27 [High] SQL Injection
28 URL: http://testphp.vulnweb.com/product.php?pic='
29 Description: Parameter 'pic' appears vulnerable with payload: '
30 Timestamp: 2025-04-10 13:48:19
31 -----
32 [High] SQL Injection
33 URL: http://testphp.vulnweb.com/product.php?pic='
34 Description: Parameter 'pic' appears vulnerable with payload: '
35 Timestamp: 2025-04-10 13:48:19
36 -----
37 [High] SQL Injection
38 URL: http://testphp.vulnweb.com/listproducts.php?artist='
39 Description: Parameter 'artist' appears vulnerable with payload: '
40 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.