**How to Use Your Vulnerability Scanner**

**🔹 1. Install Required Packages in your linux**

Before running the script, ensure you have the necessary Python libraries installed. Open a terminal or command prompt and install them using:

**pip install requests logging**

**🔹 2. Save the Script**

* Copy the full Python scanner code into a file or download it from git link

**🔹 3. Run the Scanner**

Execute the script using:

**python vulnerability\_scanner.py**

**🔹 4. Modify Targets**

* Change **target\_ip** to the actual IP address or hostname of the target system.
* Change **target\_url** to the actual web application you want to test.

Example:

**target\_ip = "192.168.1.105"**

**target\_url = "http://example.com/product"**

**🔹 5. Review Scan Results**

The script automatically logs findings into files:

* open\_ports.txt → Lists open ports.
* sql\_vulnerabilities.txt → Shows SQL injection risks.
* xss\_vulnerabilities.txt → Displays XSS vulnerabilities.
* scan\_results.log → Contains the full scan summary.

You can open these files to review the results