PYTHON PENTESTING TOOL FOR WEB APPLICATION

This tool is tailored testing for Web Application is builed on Flask/ React/ PostgreSQL/ Docker/ Nginx Proxy Manager stack, running on ParrotOS (Security Edition).

* Core Features: Original tests (port scanning, SQL injection, XSS, brute-force, JWT validation, etc.) with NVD CVE integration, version matching, and caching.
* ParrotOS Integration: Integration with sqlmap, nikto, and Tor for enhanced testing, leveraging ParrotOS’s security tools.
* Additional Features: Modular design, CLI interface, Docker support, forensic reporting, and compliance checks.
* Reporting: CSV, HTML, and PDF reports with severity, CVE references, and remediation suggestions.
* Optimizations: Caching, version matching, and dynamic dependency detection.

Directory Structure

|  |
| --- |
| pentest\_tool/  ├── pentest.py # Main script  ├── report\_template.html # HTML report template  ├── requirements.txt # Python dependencies  ├── config.json # Configuration file  └── cve\_cache.json # Cached CVE data (auto-generated) |

I – FEATURE AND FUNCTION

|  |  |
| --- | --- |
| TOOL FEATURE AND FUNCTIONS | |
| TYPE | DETAILS |
| Core Tests | Port scanning |
| Endpoint exposure |
| SQL injection |
| XSS |
| Brute-force |
| JWT validation |
| Fuzzing |
| HTTPS stripping |
| Subdomain enumeration |
| CSRF |
| Directory listing |
| Enhanced Tests | Flask debug mode |
| PostgreSQL exposure |
| Nginx security |
| SSTI |
| Docker security |
| Sensitive data exposure |
| ParrotOS Integrations | sqlmap |
| nikto |
| Tor-based anonymous testing |
| Forensic reporting |
| FEATURES | |
| CVE Integration | NVD API with version matching and caching |
| Reporting | CSV, HTML, and PDF with severity, CVE references, and suggestions. |
| Usability | CLI interface, modular design, dynamic version detection. |

II – BRIEF LIST TO SETUP TO USE

* Software Requirements:
  + ParrotOS Security Edition
  + python3 and python3-pip
  + git
* Documents Requirements:
  + config.json
  + report\_template.html
  + NVD API Key from nvd.nist.gov
* Dictionaries Requirements:
  + Username and Password dictionaries (Eg: passwords.txt)
  + Payload Dictionaries (Eg: payloads.txt)
  + Subdomain Lists

III – SETUP AND USAGE

1. Install ParrotOS

Hardware Requirements Recommended:

CPU: Quad-core processor (e.g., Intel i5 or better)

RAM: 16 GB (to handle multiple tests and virtual machines)

Storage: 50 GB+ (for ParrotOS, tool data, and reports)

Network: High-speed broadband (for large-scale scans)

* Use ParrotOS Security Edition.
* Update: sudo apt update && sudo apt upgrade.
* Install dependencies: sudo apt install python3 python3-pip tor nmap sqlmap nikto docker.io

1. Set Up the Tool

* Create the directory: mkdir /home/parrot/pentest\_tool && cd /home/parrot/pentest\_tool.
* Save pentest.py, report\_template.html, requirements.txt, and config.json.
* Create a virtual environment: python3 -m venv venv && source venv/bin/activate.
* Install dependencies: pip install -r requirements.txt.