

DarkNET_Scanner will be a RESTful API designed to support authorized penetration testing and network security scanning. This API will provide cybersecurity enthusiasts with tools to conduct various tests, evaluate vulnerabilities, and analyze security risks within a controlled, secure, and ethical framework.

Network and Web App Testing Tools

- **Network Scanning:** Perform port scanning, service detection, and OS identification on specified IPs.
- **Web Vulnerability Testing:** Test web endpoints for vulnerabilities such as SQL Injection, XSS, and Remote Code Execution (RCE).
- **Authentication Strength Testing:** Evaluate the robustness of authentication mechanisms, including password strength and session management.

Technical Stack

- **Backend Framework:** FastAPI (Python)
- **Database:** PostgreSQL
- **Security Libraries:** PyJWT, Authlib
- **Testing Libraries:** Scapy (network scanning), SQLMap (SQL Injection testing), and OWASP ZAP (web vulnerability testing)
- **Logging and Monitoring:** Elasticsearch, Logstash, Kibana