Title: Advanced Web Vulnerability Scanner

Introduction:

The Advanced Web Vulnerability Scanner is a powerful Python-based security tool designed to identify and analyze vulnerabilities in live websites. Developed with the goal of supporting OWASP Top 10 vulnerability categories, this scanner allows penetration testers and security professionals to perform real-time assessments across various severity levels, including custom-defined scanning depths.

Abstract:

The project implements a modular scanner capable of conducting reconnaissance, vulnerability detection, and reporting in multiple formats (TXT, JSON, CSV, HTML). It integrates WAF bypass mechanisms, proof-of-concept (PoC) generators, AI-driven fix recommendations, and a CLI interface. Target analysis includes WHOIS, DNS, ports, banners, CMS, and screenshot capturing with Selenium.

Tools Used:

- Python 3.x
- Requests, BeautifulSoup, Selenium, argparse
- socket, hashlib, threading, whois, ipwhois
- fpdf (for PDF reports), json, csv, HTML generation

Steps Involved in Building the Project:

1. Reconnaissance Modules: Subdomain enumeration, port scanning, DNS and WHOIS data gathering.
2. Scanner Engine: Core logic to identify vulnerabilities like XSS, SQLi, CSRF, RCE, SSRF, LFI, etc.
3. WAF Bypass and PoC Generation: Encoded payloads, HTML/cURL/Bash/JS-based PoCs.

4. AI Fix Recommendations: Severity classification, detailed remediation suggestions.

5. Reporting Modules: Generate TXT, JSON, CSV, and HTML reports. Screenshot capture and HAR log collection.

6. CLI Interface: Complete command-line integration with argument parsing for mode and output control.

Conclusion:

This project showcases an end-to-end web security scanner suitable for both educational and professional use. It provides actionable insights, integrates advanced attack simulation techniques, and delivers comprehensive reports. Its modularity, extensibility, and full CLI support make it a flexible addition to any pentesting toolkit.