Web Application Vulnerability Scanner.
By: Rithika Swami
Project Type: Vulnerability Scanning (Cybersecurity)

Objective:

Build a Python-based vulnerability scanner that detects Cross-Site Scripting (XSS) vulnerabilities in web applications by crawling .php pages and testing them with basic XSS payloads.

Tools & Technologies Used:

Python

Requests :- to make HTTP requests

BeautifulSoup :-to parse HTML and extract internal links

Colorama :- to make terminal output colorful and readable

urljoin :- to handle relative/absolute URL combinations

Text File Output :- to save scan results in a .txt file

Project Overview:

This scanner goes through a target website, collects all .php links, and then checks each one for possible XSS vulnerabilities using a simple payload (<script>alert('XSS')</script>). If the payload is reflected in the response, it indicates a potential vulnerability.

Sample Output in Terminal:

[+] Found 15 internal links. Starting XSS scan...

[-] No XSS at: http://testphp.vulnweb.com/index.php
[-] No XSS at: http://testphp.vulnweb.com/cart.php
...

All scan results were also saved to scan_results.txt.

Output File:

scan_results.txt :- stores all scan results

Can be easily attached or used as part of an audit report

Final Notes:

This is a basic web vulnerability scanner meant to demonstrate scanning logic. It's useful for learning and can be extended with:

SQLi detection

Authentication bypass attempts

Better payload fuzzing techniques