Web Vulnerability Scanner - Project Report

-By Prakanth V

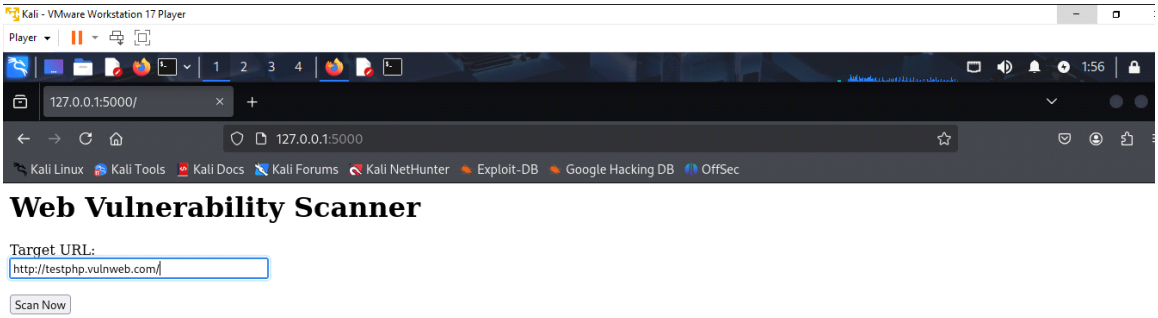
Objective

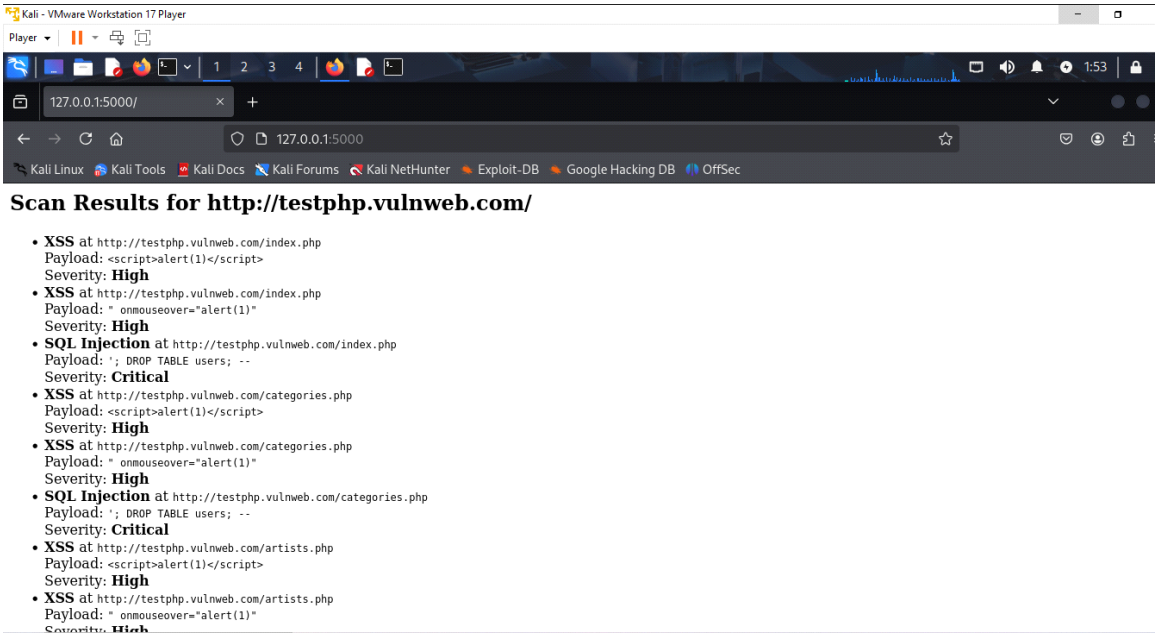
Build a Python-based web vulnerability scanner that identifies common web application vulnerabilities such as Cross-Site Scripting (XSS) and SQL Injection (SQLi). The scanner uses a web interface for scanning URLs and displaying results in real-time.

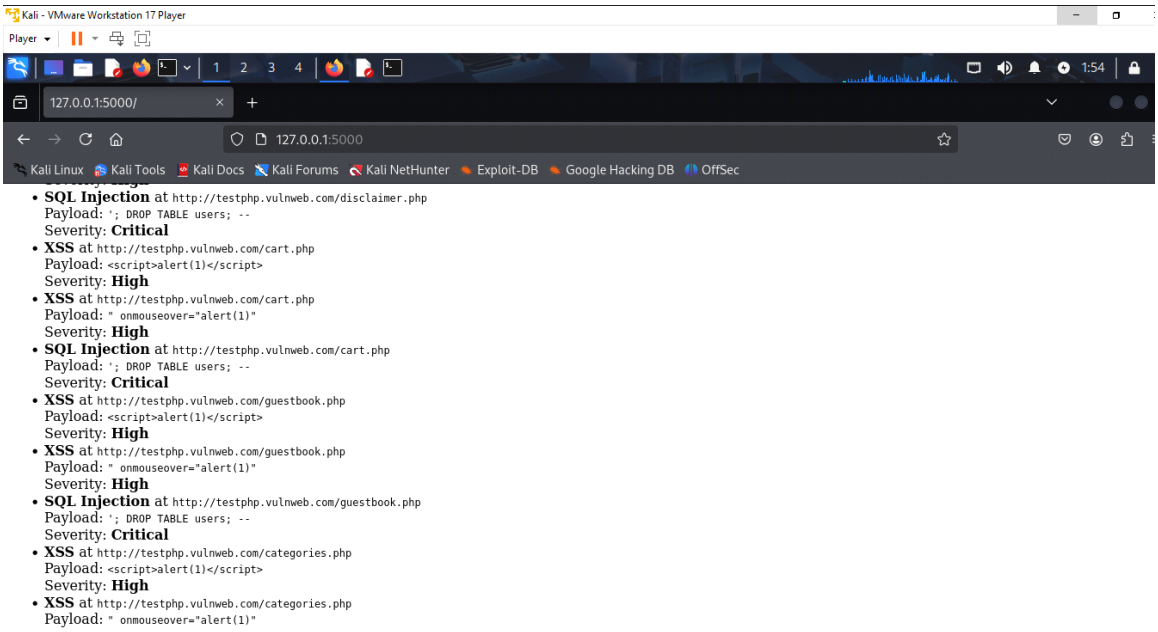
Tools & Technologies

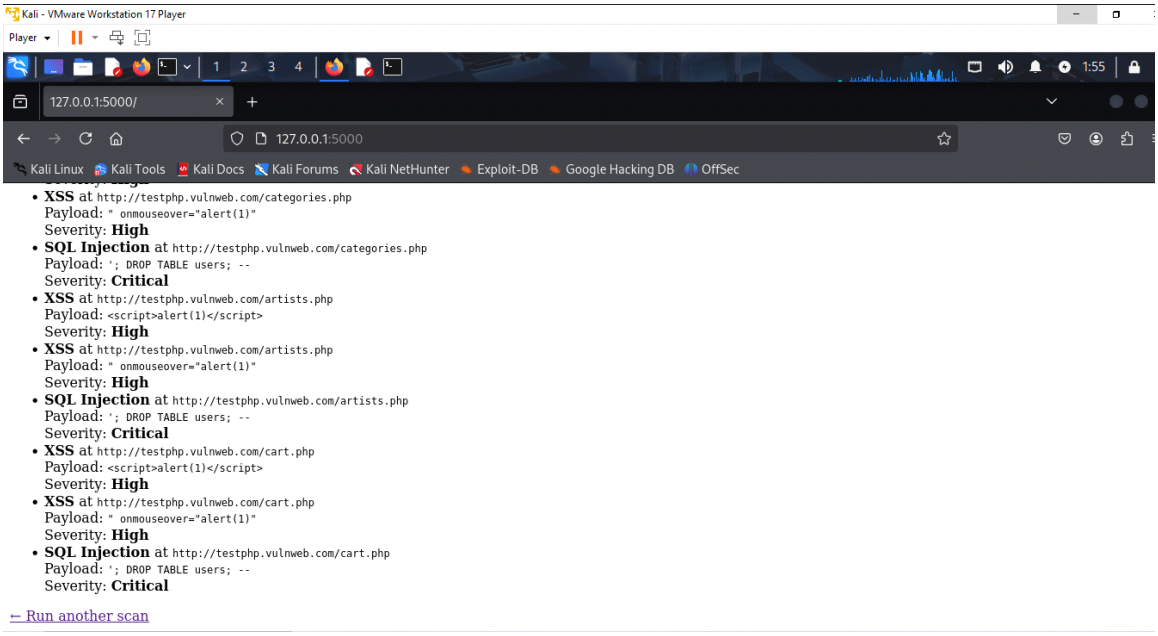
Tool	Purpose
Python 3.8+	Core scripting language
Flask	Web framework
Requests	HTTP request handling
BeautifulSoup	HTML parsing and crawling
Regex	Pattern matching for error detection

Screenshots









How It Works

1. User inputs a URL.
2. The crawler finds all internal links and form elements.
3. Payload injection occurs in form inputs.
4. Responses are analyzed for reflection or error signatures.

5. Detected vulnerabilities are displayed in a table.

Vulnerability Testing

XSS (Cross-Site Scripting)

Payload: <script>alert(1)</script>
Detection: If payload is reflected in HTML response.

SQL Injection

Payload: ' OR 1=1 --
Detection: If response contains SQL errors (e.g., SQL syntax error).

Example Report Entry

Type	URL	Payload	Severity
SQL Injection	http://test.com/search	' OR 1=1 --	Critical
XSS	http://test.com/comment	<script>alert(1)</script>	High

Ethical Notice

⚠ This tool is for educational purposes only. Only scan domains you own or are authorized to test.