🛡️ Web Vulnerability Scanner – Project Report

📌 Description:

A simple Python tool with a web interface (Flask) that scans a given URL for **XSS** and **SQL Injection** vulnerabilities by detecting and testing form inputs.

⚙️ Features:

- **Form Detection**: Extracts all forms from the target webpage.
- **XSS Scan**: Injects <script>alert(1)</script> and checks if it's reflected.
- **SQLi Scan**: Uses common payloads like ' OR 1=1 -- to detect SQL errors.
- **HTML Output**: Displays vulnerabilities, payloads used, and sample response.

🛠️ Tech Used:

- Python, Flask
- Requests
- BeautifulSoup
- Regex (re)

🚀 How to Run:

1. Install dependencies:

```
pip install flask requests beautifulsoup4
```

2. Run the app:

```
python scanner.py
```

3. Open in browser:

http://127.0.0.1:5000

✅ Output Example:

```
Vulnerability: SQL Injection

URL: http://target.com/login

Payload: ' OR '1'='1

Evidence: SQL syntax error detected...
```
