# Web Application Vulnerability Scanner

## Introduction

_This project is a lightweight web application vulnerability scanner written in Python. It is designed to detect basic vulnerabilities in web applications such as SQL injection, cross-site scripting (XSS), missing security headers, and exposed directories.

## Objective:

To automate the process of identifying common web vulnerabilities for educational or testing purposes.

### Features:

- Scans for SQL Injection vulnerabilities
- Detects reflected Cross-site Scripting (XSS)
- Checks for missing HTTP security headers
- Identifies exposed directories
- Generates an HTML report with summary and charts

### Technologies Used:

- Python 3
- requests
- BeautifulSoup4
- urllib.parse
- Chart.js (for report visualization)

### Setup Instructions:

1. Clone or copy the project folder
2. Create and activate a virtual environment (optional)
3. Run `pip install -r requirements.txt` to install dependencies

### How It Works

1. Takes a URL as input
2. Checks for security headers
3. Parses and tests form inputs for SQLi and XSS

4. Attempts to access common sensitive directories
5. Generates a styled HTML report (report.html)

## Code Explanation:

- check_security_headers(): Inspects HTTP headers for security best practices
- scan_sqli(): Injects SQL payloads into form inputs and looks for error patterns
- scan_xss(): Injects XSS scripts and checks for reflection
- check_directories(): Tries to access common directories like /admin or /backup
- generate_html_report(): Creates a styled HTML report with charts

## Sample Scan and Output:

Run the tool with: `python3 scanner.py`
Input the target URL when prompted.
The scanner logs progress and creates a `report.html` file in the same directory.

## Limitations:

- Only tests for reflected XSS and basic SQLi patterns
- Does not perform authenticated scans
- Cannot crawl entire websites
- Depends on network access and target availability

## Conclusion:

This scanner is a basic yet useful tool for learning about automated web vulnerability testing. It is extendable and ideal for beginners in cybersecurity.