**SQL Injection Testing Script**

**Overview**

The SQL Injection Testing Script, developed by Raja Muhammad Awais, is a Python tool designed to assess web applications for SQL injection vulnerabilities. SQL injection is a critical security flaw that allows attackers to manipulate SQL queries through user inputs, potentially gaining unauthorized access to databases. This script aids in identifying and validating these vulnerabilities by injecting carefully crafted SQL payloads and analyzing the application's responses.

**Features**

* **Comprehensive Testing**: Tests both GET and POST requests with a range of SQL injection payloads.
* **Vulnerability Detection**: Detects potential vulnerabilities based on common SQL error patterns.
* **Logging and Reporting**: Logs results to files (sql\_injection\_results.json, sql\_injection\_results.csv) for further analysis.
* **Customizable Payloads**: Easily customizable with additional or modified SQL injection payloads.

**Requirements**

* Python 3.x
* Requests library (pip install requests)

**Usage**

1. **Clone the Repository**:

bash

Copy code

git clone https://github.com/your\_username/sql-injection-testing.git

cd sql-injection-testing

1. **Install Dependencies**:

Ensure Python 3.x is installed. Install the required requests library:

bash

Copy code

pip install requests

1. **Run the Script**:

Execute the script with Python, providing the base URL of the web application you want to test:

bash

Copy code

python sql\_injection\_test.py

1. **Enter Base URL**:

When prompted, enter the base URL of the web application. Ensure it starts with http:// or https://.

1. **Review Results**:

The script will systematically test the provided URL using a variety of SQL injection payloads. Results will indicate potential vulnerabilities found in the application's responses.

1. **Save and Analyze Results**:

Results are automatically saved in sql\_injection\_results.json and sql\_injection\_results.csv files, facilitating detailed analysis and reporting.

**Disclaimer**

* **Use Responsibly**: This script is intended for authorized security testing purposes only. Ensure you have permission before testing any web application.
* **No Guarantees**: Detection of vulnerabilities depends on various factors. A lack of detected vulnerabilities does not imply absolute security of the application.

**Support**

For questions, issues, or suggestions regarding the SQL Injection Testing Script, please contact **Raja Muhammad Awais** via email at muhammadawaisturk@gmail.com.