User Manual for ASIS:

An SQL Injection Scanner

Contents

Introduction

ASIS (A SQL Injection Scanner) is a tool designed to identify potential SQL injection vulnerabilities in source code files within a specified directory. It provides a user-friendly interface to scan codebases and detect vulnerabilities that could be exploited by SQL injection attacks, helping developers secure their applications.

System Requirements

- **Operating System:** Windows or Kali Linux
- **Python Version:** Python 3.6+
- **Python Libraries:** Tkinter, OS, re

Installation

1. **Install Python:** Ensure Python 3.6+ is installed on your system. You can download it from Python's official website.
2. **Download ASIS:** Download the asis.py file and save it to a directory of your choice.
3. **Install Required Libraries:** Open a terminal or command prompt and run the following commands to install the required Python libraries: ‘pip install tk’.

Usage

Launching the Application

1. Open a terminal or command prompt.
2. Navigate to the directory where you saved asis.py.
3. Run the following command: ‘python asis.py’

Selecting a Directory

1. Upon launching the application, you will see the main interface.
2. Click the "Browse" button to open a file dialog.
3. Select the directory containing the source code files you want to scan.

Scanning for Vulnerabilities

1. After selecting the directory, click the "Scan" button to start the scanning process.
2. The application will recursively scan each file in the selected directory for predefined SQL injection patterns.

Understanding the Results

1. The results of the scan will be displayed in the large grey box on the main interface.
2. If vulnerabilities are detected, they will be listed with the file names and specific line numbers where issues were found.
3. If no vulnerabilities are found, a corresponding message will be displayed.

Troubleshooting

- **Error Message:** "Please select a directory."
    - Ensure you have selected a directory before clicking the "Scan" button.
- **Error Message:** "An error occurred while scanning [file path]."
    - This indicates an issue with reading or scanning the specified file. Ensure the file is not corrupted and try again.

FAQs

Q1: What types of SQL injection vulnerabilities does ASIS detect?

- ASIS detects various types of SQL injection vulnerabilities including escape character misuse, dynamic SQL type handling, direct concatenation, exec/execute commands, string-based injection, insert statement injection, update statement injection, delete statement injection, LIKE clause injection, numeric-based injection, and IN clause injection.

Q2: Can ASIS scan subdirectories within the selected directory?

- Yes, ASIS recursively scans all subdirectories within the selected directory.

Q3: Is there any limitation on the file types that ASIS can scan?

- ASIS scans all files within the selected directory regardless of the file type. However, it is optimized for scanning source code files.

Q4: Can I use ASIS on macOS?

- While ASIS is primarily tested on Windows and Kali Linux, it should work on macOS if Python and the required libraries are properly installed.

Repository Link

For the source code and additional documentation, please visit the ASIS repository on GitHub:

https://github.com/hw044/ASIS