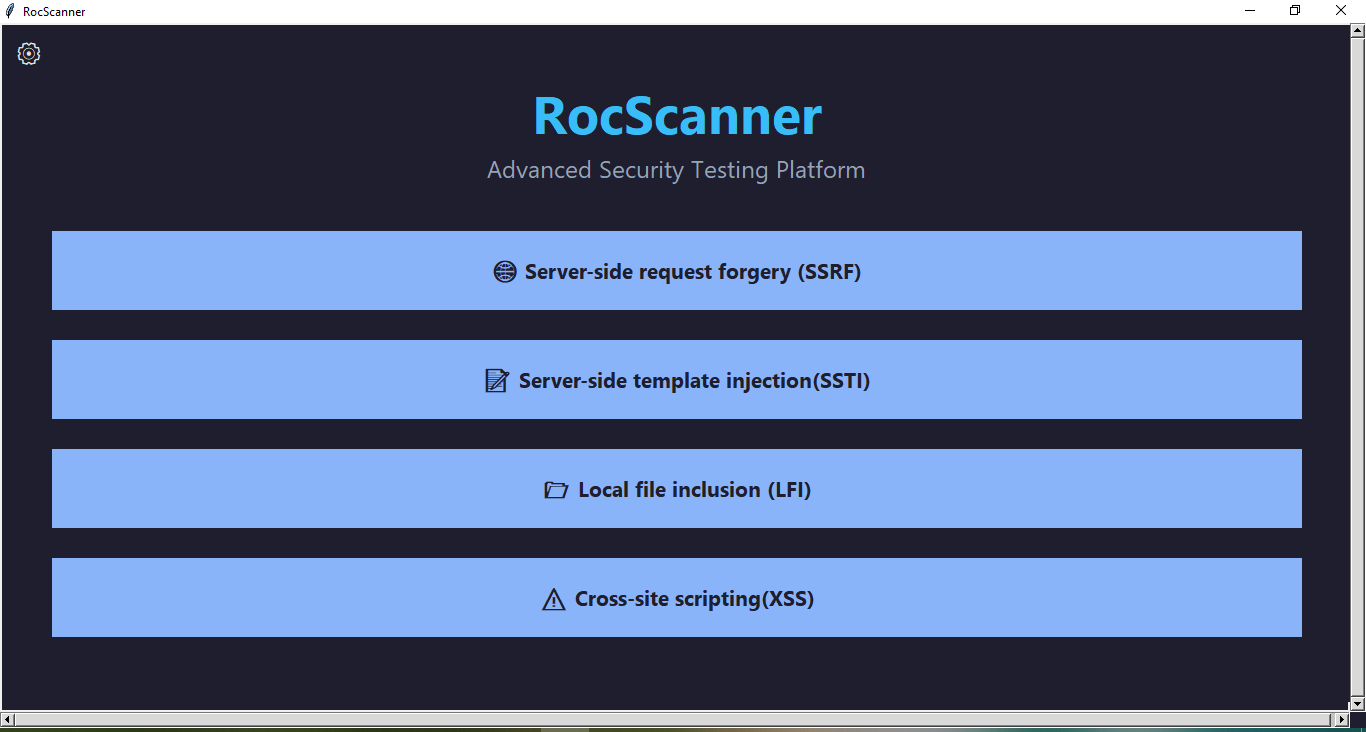
GUI Documentation: Vulnerability Scanner Application

The GUI.py file contains the main graphical user interface for the Vulnerability Scanner application. It provides a modern, dark-themed interface with four main vulnerability scanning options and additional help/about windows.



Main Window Structure

1. Main Menu

Title : "RocScanner" displayed prominently at the top.

Subtitle : "Advanced Security Testing Platform" to describe the tool's purpose.

Scanner Buttons : Four main buttons representing different vulnerability scanners:

A)Server-side Request Forgery (SSRF)

B)Server-side Template Injection (SSTI)

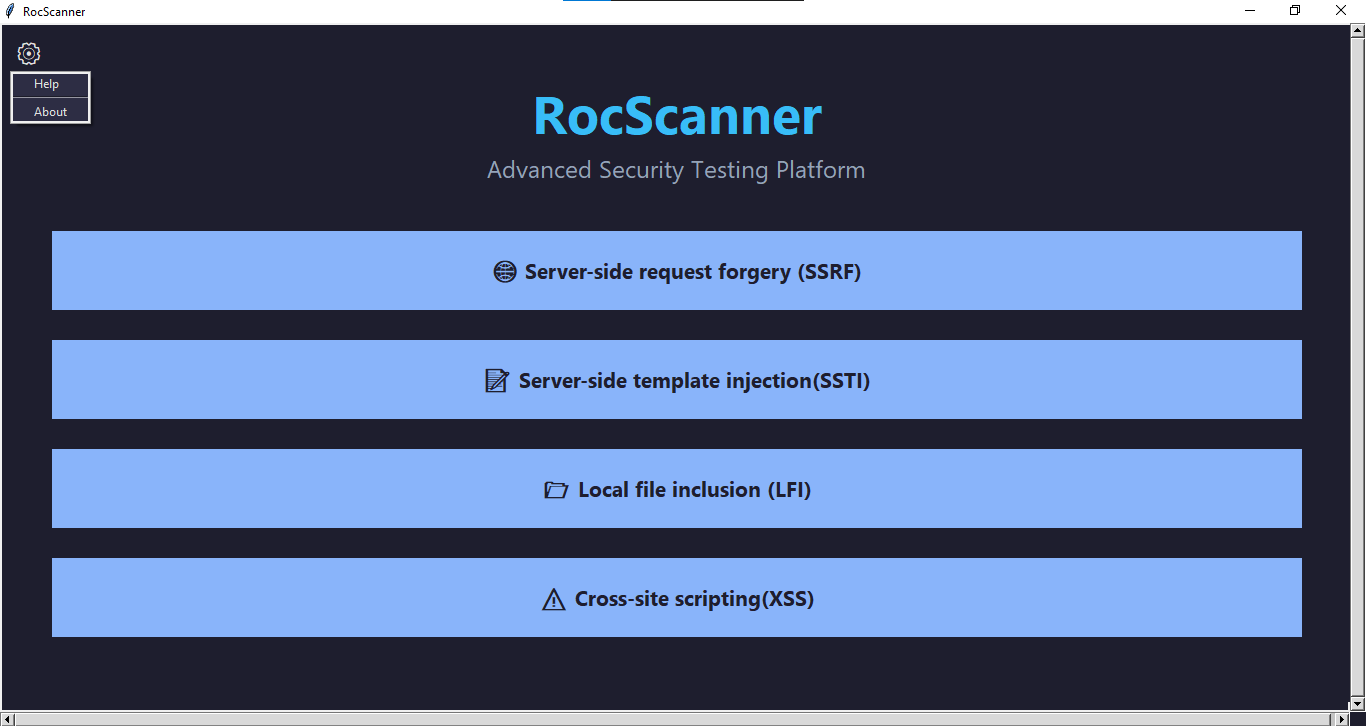
C)Local File Inclusion (LFI)

D)Cross-site Scripting (XSS)

Each button opens its respective scanner window when clicked.

2. Settings Button

Located in the top-left corner



Opens a dropdown menu with two options:

A)Help – opens the help guide window.



B)About – opens the about information window.



Scanner Windows

When a vulnerability type is selected from the main menu, a dedicated scanner window opens for that specific test. These windows are implemented in separate classes (e.g., LFIScannerWindow, XSSScannerWindow, etc.).

Each scanner window includes:

1)A title corresponding to the selected vulnerability.

2)Input fields for target URLs or file paths.

3)Configuration options for scanning parameters.

4)Start scan button to initiate the vulnerability assessment.

5)Stop scan button Used to stop the scan

6)Output area to display scan results or logs.

7)Clear Results button Used to clear the scan results window.

8)Save Output button It is used to save the results in a location of the user's choice and in any format he wants.