SSTI Scanner GUI

The SSTIScannerWindow class provides a graphical user interface (GUI) for scanning and exploiting Server-Side Template Injection (SSTI) vulnerabilities. This window is implemented as a Toplevel widget in Tkinter and features a modern, user-friendly design with multiple tabs for different functionalities.

Features

Scan Configuration: Configure scan parameters including target URLs, proxies, and threading

Scan Results: View scan results in multiple formats (JSON, CSV, XML)

Interactive Shell: Execute commands on vulnerable systems after successful detection

Responsive Design: Maximized window with scrollable content areas

Modern UI: Custom styling with accent colors and placeholder text handling

UI Components

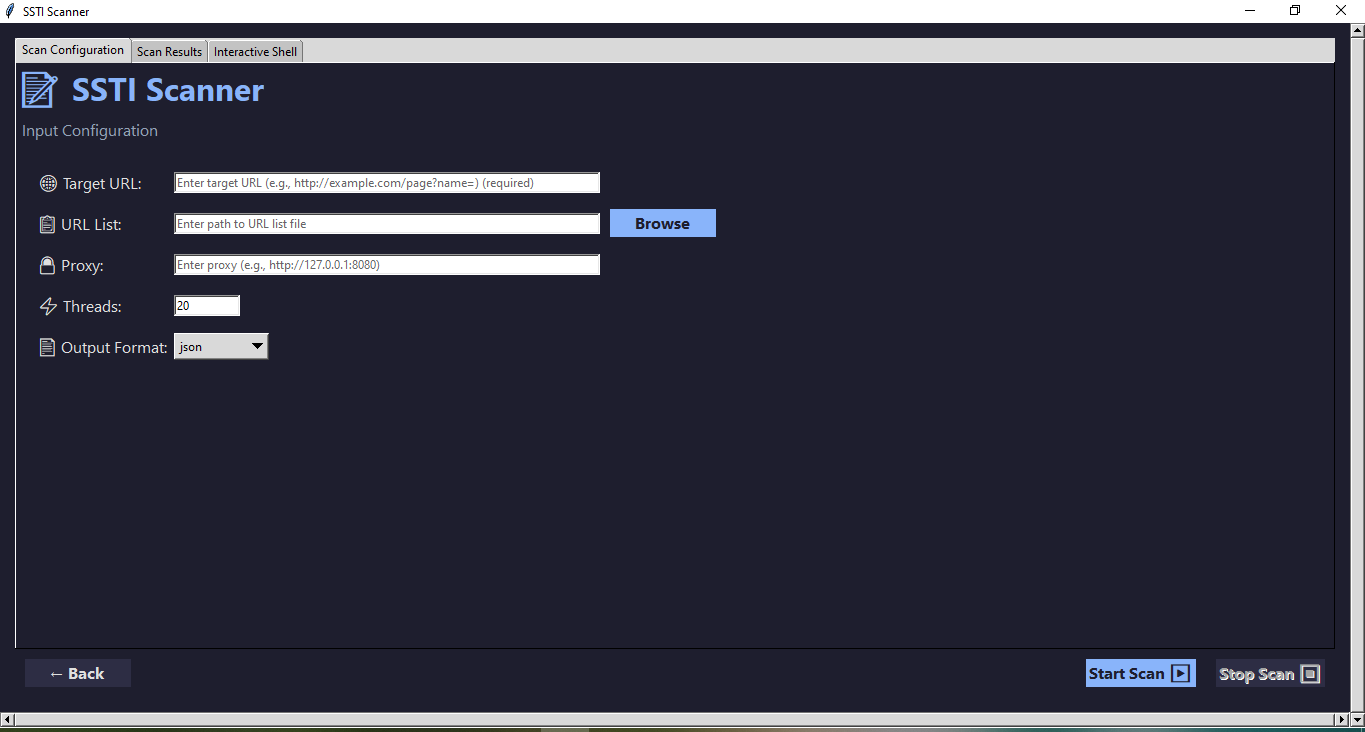
Main Window

Starts maximized (zoomed state)

Uses custom styling with dark theme

Contains a notebook widget with three tabs

Scan Configuration Tab



Input Fields:

Target URL (single URL or file containing multiple URLs)

Proxy configuration

Thread count (default: 20)

Output format selection (JSON, CSV, XML)

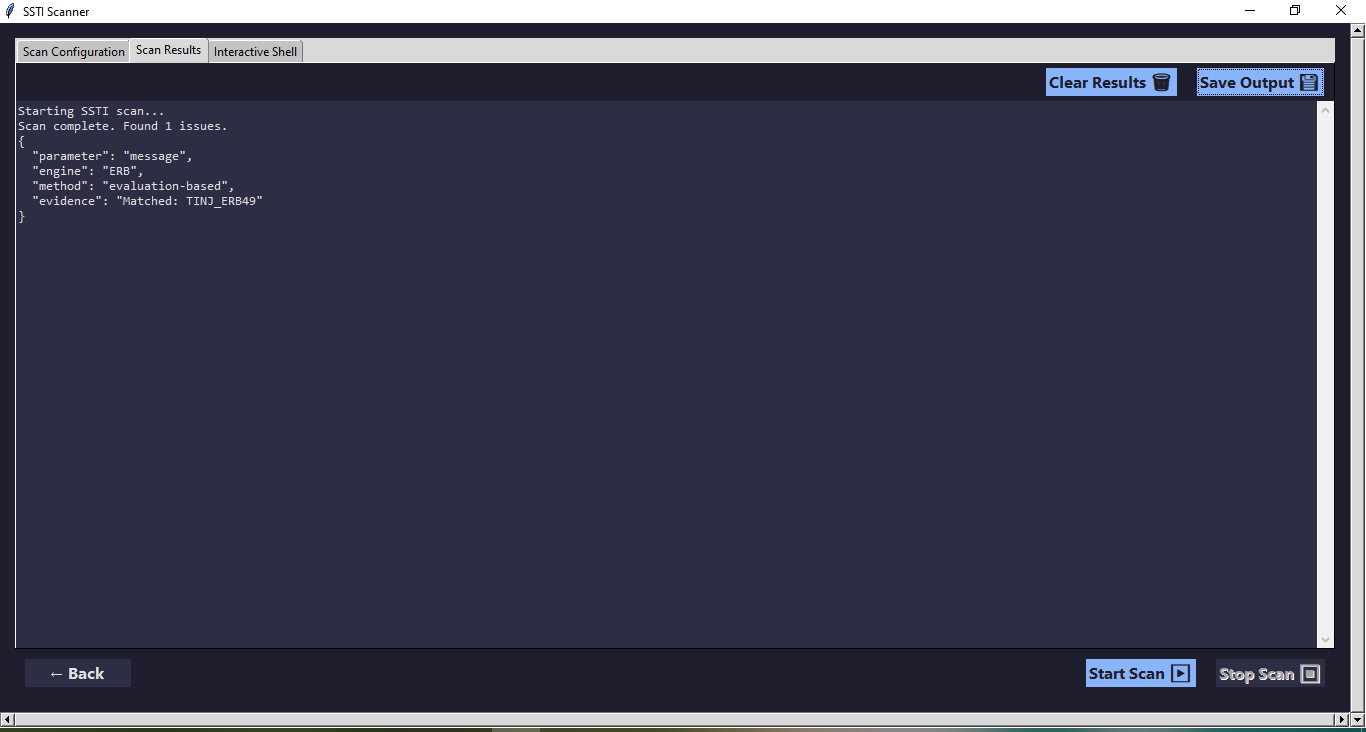
Buttons:

Start Scan: Initiates the scanning process

Stop Scan: Allows stopping an ongoing scan

Back: Returns to the parent window

Scan Results Tab



Text Area:

Displays scan results in the selected format

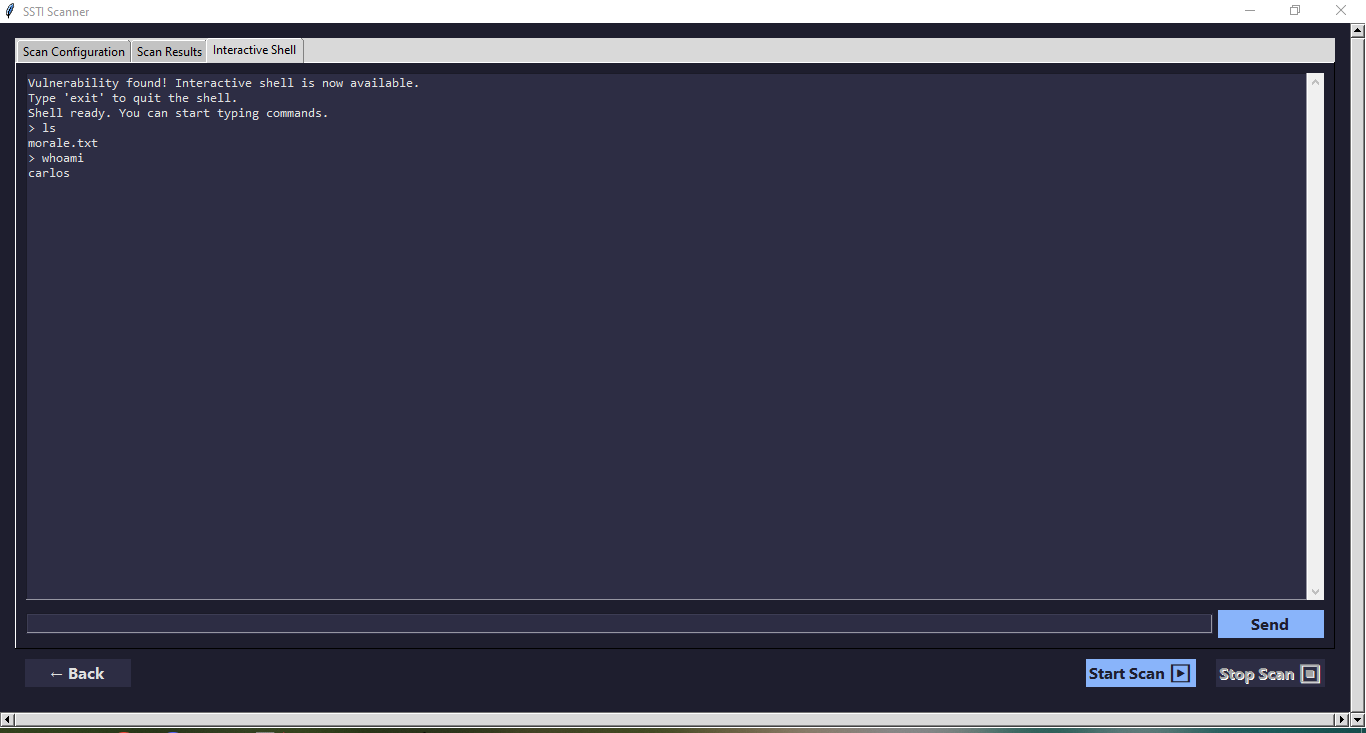
Scrollable with syntax highlighting

Buttons:

Save Output: Exports results to a file

Clear Results: Clears the results display

Interactive Shell Tab



Components:

Output area: Displays command execution results

Input field: For entering commands to execute

Send button: Triggers command execution

Functionality:

Automatically enabled when vulnerabilities are found

Supports basic command execution

Type 'exit' to quit the shell