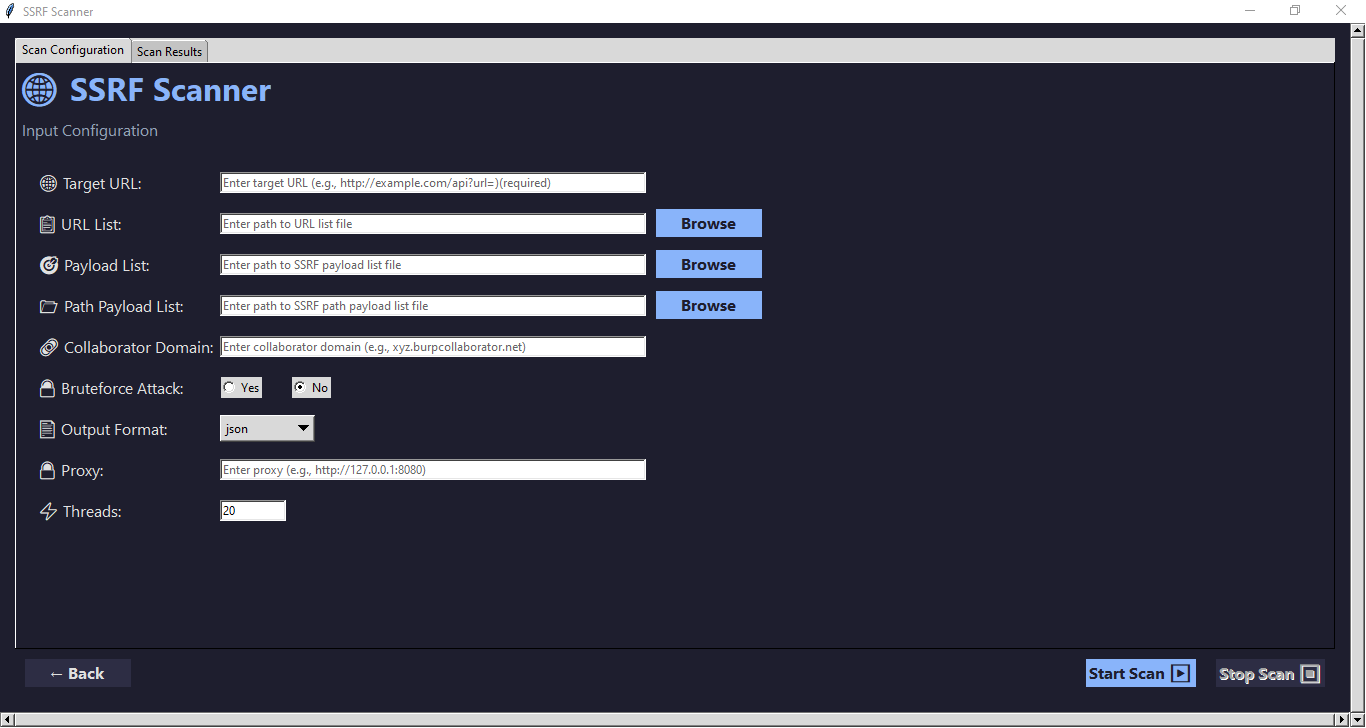
SSRF Scanner GUI

The SSRF Scanner GUI is a Python-based graphical interface for a Server-Side Request Forgery (SSRF) scanning tool. It provides an intuitive interface for configuring and running SSRF vulnerability scans against web applications.

Scan Configuration



Target URL: Single URL to scan (e.g., http://example.com/api?url=)

URL List: File containing multiple URLs to scan

Payload List: File containing SSRF payloads to test

Path Payload List: File containing path-based SSRF payloads

Collaborator Domain: Burp Collaborator domain for out-of-band testing

Bruteforce Attack: Option to enable/disable bruteforce attack mode

Proxy: Configure HTTP proxy (e.g., Burp Suite)

Threads: Number of concurrent threads for scanning (default: 20)

Output Format: JSON, CSV, or XML

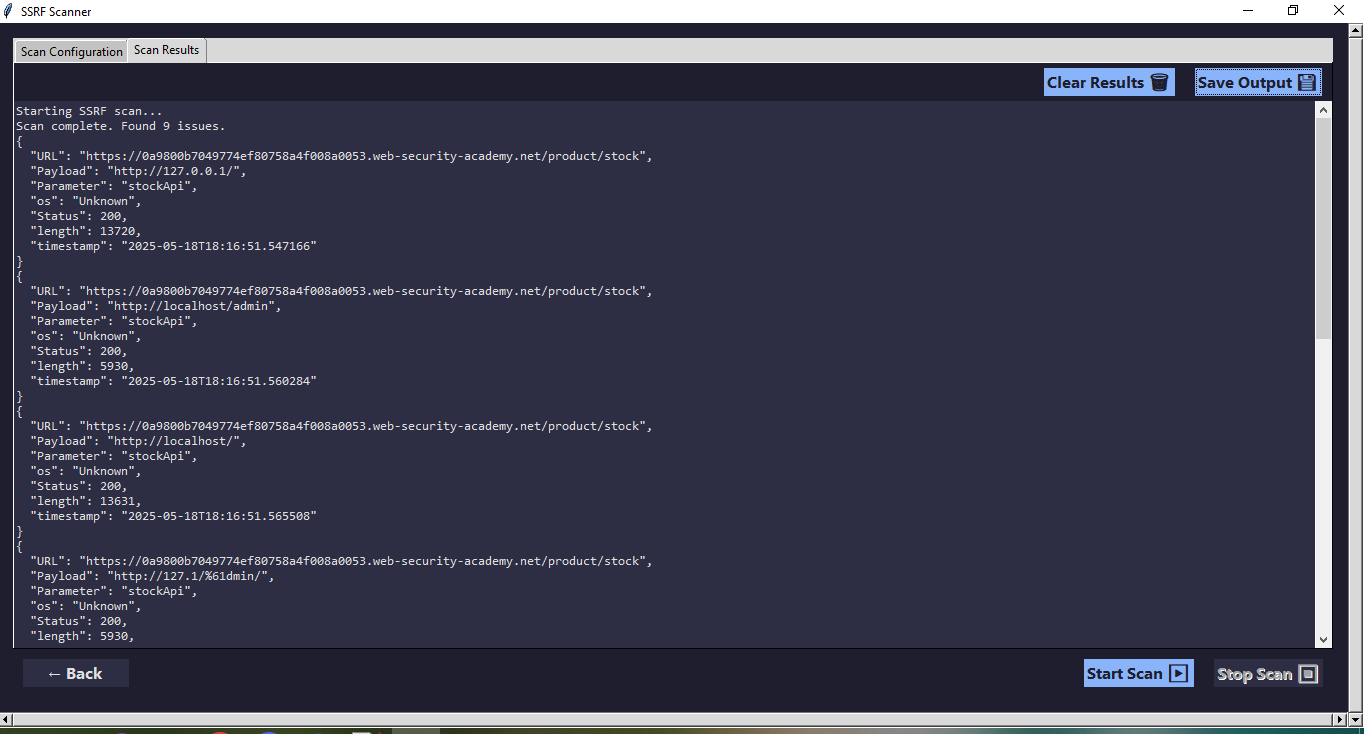
Options

Bruteforce Attack : Choose between "Yes" or "No" to enable/disable additional bruteforce techniques

Output Format : Select the format for displaying results (JSON, CSV, XML)

Proxy : Optional proxy server setting for routing requests through a proxy

Results Display



The scan results are shown in a scrollable text area that supports:

JSON-formatted output

CSV-formatted output

XML-formatted output

Controls

Start Scan : Initiates the scan with the configured parameters

Stop Scan : Stops an ongoing scan

Save Output : Saves the scan results to a file

Clear Results : Clears the results display area

Back : Returns to the parent window/application