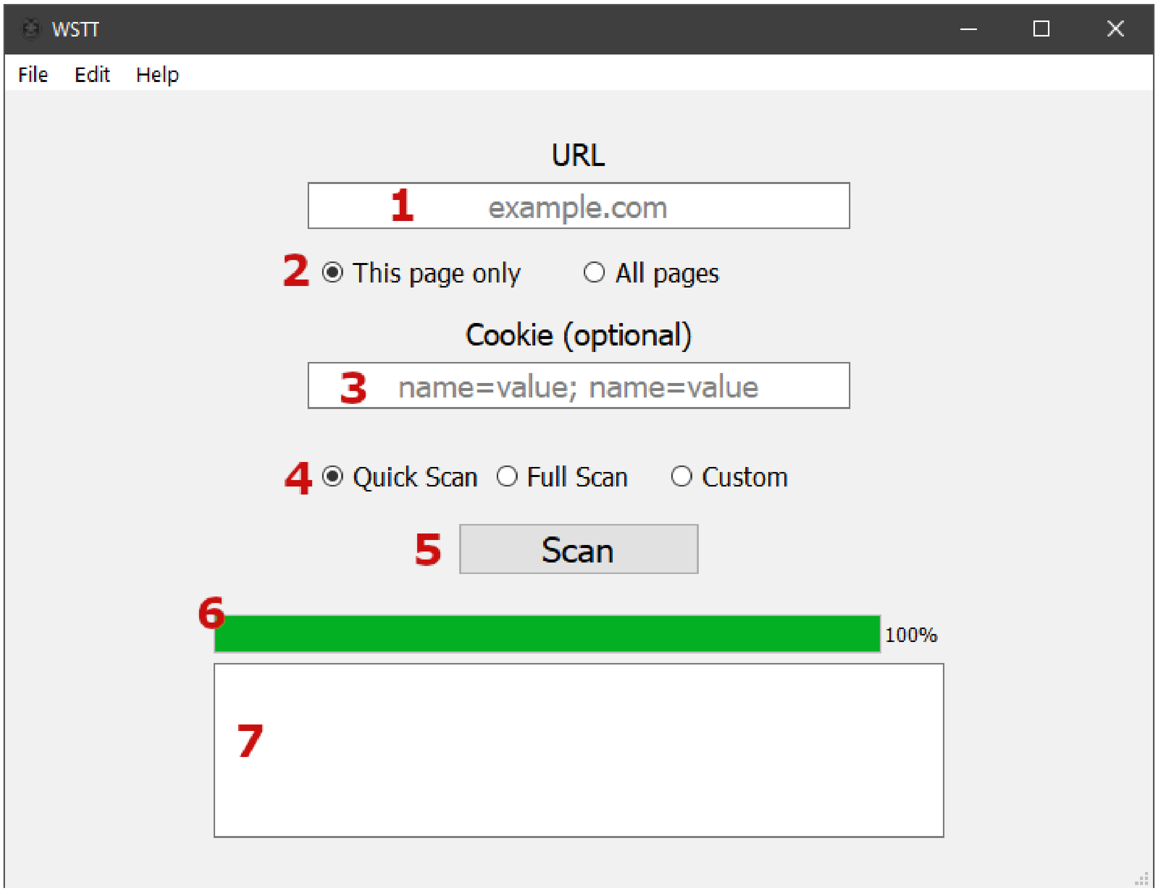
WSTT USER MANUAL

This document will provide a guide for how to use the graphical user interface of WSTT (Web Security Testing Tool).

The following picture is the main window of WSTT. Each item of interest is labeled with a red number for illustration purposes. Each numbered item will then be described in detail below.



URL

example.com

● This page only ○ All pages

Cookie (optional)

name=value; name=value

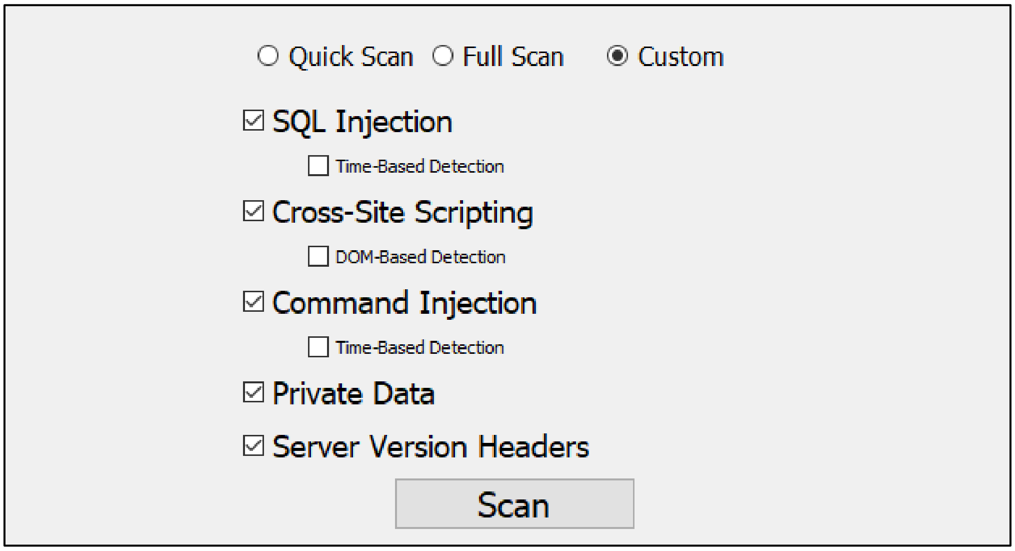
● Quick Scan ○ Full Scan ○ Custom

1: This is the URL text box. The URL of a website that is entered here will be scanned for security vulnerabilities. Typing “http://” is optional and not required because the tool will automatically append it to entered text.

2: The two radio buttons below the URL text box are used to instruct WSTT to either scan for the entered URL only or the whole website. The default option (“This page only”), will only scan one page. While the other option, (“All pages”) will make WSTT try to crawl and find all the webpages on the website. WSTT will ignore any external links it finds that lead to pages outside of the given website.

3: This is the cookie text box. A cookie is not required for scanning webpages, but it can be used if the given URL is behind a login screen. In that case, the user must provide a session cookie by going to that URL using their preferred web browser and login manually. Then, the user will get a session cookie. This cookie can be viewed from the web browser. Here is a guide on how to do it: How to Check Cookies on Your Website Manually. The user should then type the cookie following this syntax: “name=value”. For example, “PHPSESSID=2r5bfcokovgu1hjf1v08”. If the user wants to include more than one cookie, a semicolon should be used between them: “name1=value1; name2=value2”.

4: This row of radio buttons is used to select a scan mode. There are three modes: quick scan, full scan, and custom scan. Quick scan is the default mode. A quick scan will scan for all vulnerabilities, but it will not scan using DOM-based XSS detection method or time-based methods for SQL injection and command injection. It will also scan using less payloads. A full scan will scan for every vulnerability and method, including the DOM-based method and the time-based method. When the custom scan is selected, it will reveal a list of checkboxes for the user as shown in the below picture. The user can then choose which vulnerability to check for.



○ Quick Scan ○ Full Scan ● Custom

☑ SQL Injection
- □ Time-Based Detection

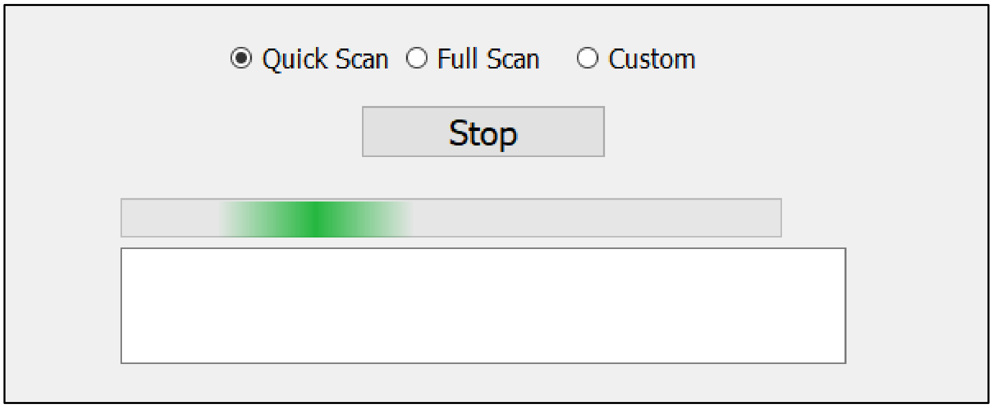
☑ Cross-Site Scripting
- □ DOM-Based Detection

☑ Command Injection
- □ Time-Based Detection

☑ Private Data

☑ Server Version Headers

5: This is the scan button. When this button is pressed, items number 6 and number 7 will be revealed, and the scan will commence. As shown below, the button text will change to “Stop". The scan can then be stopped by pressing the button again.



6: The progress bar. This bar will show the status of the scan and an estimate percentage of the scan progress. The bar will be in a waiting state if the user clicked the stop button or if WSTT is still in pre-scan stage (e.g., crawling the websites to get all URLs)

7: The log text box. This box will contain log messages about the scan. The messages are colored according to their log level. Errors and critical messages are colored Red. While warning messages are colored Orange. Harmless info messages are colored Black or White depending on the background color. More detailed log messages can be found in the generated file “WSTT.log”. This file will be generated at the current working directory of the user.