09 - Wrap up on XSS

We should be using automated tools to facilitate locating these vulnerable inputs. An automated tool will be able to cover a lot more ground than we can by "hand". We can either make a tool, or use one that already exists. Lets see if we can find a trustworthy one.

We want to learn how to run three of this automated tools. Just so we have a couple of option under our belt.

Automated Scanners for XSS

- 1. [OWASP ZAP (Zed Attack Proxy)]
 - · Description: A powerful open-source web application scanner.
 - Features:
 - Detects XSS vulnerabilities during active scanning.
 - Provides automated payload injection and results analysis.
 - How to Use:
 - Set up ZAP as a proxy.
 - · Crawl your web application.
 - Run an active scan to detect XSS.
 - Learn more
- 2. [Burp Suite Community/Professional]
 - · Description: A popular tool for web application security testing.
 - Features:
 - · Includes an "Intruder" and "Scanner" module for XSS.
 - · Allows manual XSS injection testing.
 - How to Use:
 - · Use the "Intruder" tool to test specific input fields.
 - · Use the Professional version for automated scanning (paid).
 - Learn more

3. Acunetix

- Description: A commercial web application security scanner.
- Features:
 - Automated detection of reflected, stored, and DOM-based XSS.
 - · Integration with CI/CD pipelines for testing.
- · Learn more

4. Nikto

- · Description: A simple open-source web server scanner.
- Features:
 - · Detects basic XSS vulnerabilities.
 - · Provides information on web server misconfigurations.
- Learn more

Manual Testing Tools



1. XSStrike

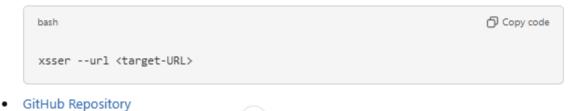
- Description: An advanced XSS detection tool.
- Features:
 - Fuzzes for reflected and DOM-based XSS.
 - · Attempts to identify filter bypass methods.
- Command:



GitHub Repository

XSSER

- Description: A tool specifically for detecting XSS vulnerabilities.
- Features:
 - · Supports reflected, stored, and DOM-based XSS.
 - · Provides customizable payloads.
- Command:



3. XSS Payload List

· Use payloads from public repositories like PayloadsAllTheThings to test manually:

PayloadsAllTheThings GitHub Repository

Browser Extensions for XSS Testing

- 1. XSS Radar
 - · Description: A browser extension for identifying potential XSS.
 - · Supported Browsers: Google Chrome, Mozilla Firefox.

2. HackBar

- · Description: A browser plugin that helps craft and test XSS payloads.
- Supported Browsers: Mozilla Firefox.

Cloud based options:

Cloud-Based Scanners

- 1. Detectify
 - Cloud-based scanner offering automated XSS detection.
 - Website
- 2. Tenable.io
 - Includes web application security testing.
 - Website