Burp Suite Cheatsheet

A comprehensive cheat sheet covering essential Burp Suite tools, features, and workflows for web application security testing.

Burp Suite Basics

Core Tools Overview

Proxy: Intercepts and modifies HTTP/S traffic between your browser and web servers.

Repeater: Manually modify and resend individual HTTP requests.

Intruder: Automates customized attacks, such as fuzzing and brute-forcing.

Scanner: Automatically crawls and audits web applications for vulnerabilities (Burp Suite Professional only).

Sequencer: Analyzes the randomness of session tokens.

Decoder: Encodes and decodes data in various formats.

Comparer: Visually compares differences between two sets of data.

Extender: Allows extending Burp Suite's functionality using custom extensions.

Setting up Burp Proxy

1. **Configure Proxy Listener:** In Burp Suite, go to Proxy > Options and configure a listener on a specific interface and port (e.g., 127.0.0.1:8080).

2. **Browser Configuration:** Configure your browser to use Burp Suite as its proxy server. This usually involves setting the HTTP and HTTPS proxy settings to the same address and port as your Burp Suite listener.

3. **Install Burp's CA Certificate:** To intercept HTTPS traffic, you need to install Burp Suite's CA certificate in your browser. Access `http://burp` in your browser, download the certificate, and import it into your browser's trusted root certificates.

Essential Keyboard Shortcuts

`Ctrl+Shift+P`	Intercept Next Request
`Ctrl+R`	Send to Repeater
`Ctrl+I`	Send to Intruder
`Ctrl+S`	Send to Scanner (Professional Only)
`Ctrl+T`	Send to Sequencer
`Ctrl+D`	Send to Decoder

Repeater and Intruder

Using Repeater

1. **Send Request to Repeater:** Right-click on an intercepted request in the Proxy tab and select "Send to Repeater".

2. **Modify the Request:** In the Repeater tab, modify the request parameters, headers, or body as needed.

3. **Send and Analyze:** Click the "Go" button to send the modified request. Analyze the server's response in the response panel.

4. **Common Use Cases:** Testing for input validation issues, parameter tampering, and replaying requests.

Intruder Attack Types

Sniper: Uses a single payload set, iterating through each payload position.

Battering Ram: Uses a single payload set, inserting the same payload into all defined payload positions in each request.

Pitchfork: Uses multiple payload sets, one for each payload position. Iterates through the payload sets in parallel.

Cluster Bomb: Uses multiple payload sets, one for each payload position. Iterates through every possible combination of payloads.

Intruder Payloads

1. **Simple List:** A list of strings used as payloads (e.g., common usernames, passwords).

2. **Runtime File:** Reads payloads from a file.

3. **Custom Iterator:** Generates payloads based on a custom pattern or algorithm.

4. **Character substitution:** Substitute specified characters for other characters.

5. **Case modification:** Modify the case of an existing payload.

Burp Scanner (Professional)

Scanning Modes

Passive Scanning: Analyzes traffic as it passes through Burp Proxy without actively sending requests. Useful for identifying information disclosure and insecure configurations.

Active Scanning: Sends crafted requests to the application to identify vulnerabilities. More thorough but can be intrusive.

Scan Configuration

1. **Scan Scope:** Define the target URLs for the scan. This helps to avoid accidentally scanning unintended targets.

2. **Scan Configuration:** Configure the types of vulnerabilities to scan for (e.g., SQL injection, XSS). You can choose from predefined configurations or create custom configurations.

3. **Optimization:** Adjust scan settings to balance speed and thoroughness. Consider factors like request throttling and concurrency.

Interpreting Scan Results

1. **Issue Severity:** Burp Scanner assigns a severity level (High, Medium, Low, Information) to each identified issue.

2. **Issue Details:** Each issue includes a detailed description, affected URL, request/response samples, and remediation advice.

3. **Reporting:** Generate reports in various formats (HTML, XML) to document scan findings.

Advanced Techniques

Using Burp Collaborator

1. **Purpose:** Detects vulnerabilities that are typically invisible, like out-of-band interactions (e.g., SSRF, blind SQL injection).
2. **How it Works:** Burp Collaborator provides a unique domain that Burp Suite uses to monitor for interactions initiated by the application being tested.
3. **Configuration:** Configure Burp Collaborator client within Burp Suite.
4. **Usage:** Inject Collaborator payloads into application inputs and monitor for DNS lookups or HTTP requests back to the Collaborator server.

Macros

1. **Purpose:** Automate multi-step sequences of requests, such as logging in and navigating to a specific page.
2. **Configuration:** Define macros in Burp Suite's Project options > Sessions > Macros.
3. **Usage:** Use macros in Intruder or Scanner to handle authentication or other complex workflows.

Extender API

1. **Purpose:** Extend Burp Suite's functionality by writing custom extensions in Java, Python, or other languages.
2. **Key Interfaces:** `IBurpExtender`, `IHttpListener`, `IScannerCheck`, etc.
3. **Example Use Cases:** Custom vulnerability checks, automated data extraction, integration with other tools.