Burp Suite Cheat Sheet by Codelivly

---

1. Getting Started

Launch Burp:

- Start Burp and open the browser.
- Go to `Proxy > Intercept` to turn on HTTP interception.

Set Target Scope:

- Define your target's scope in `Target > Site map`.
- Right-click the site map entry > `Add to scope`.
- Exclude out-of-scope traffic by selecting `Yes` when prompted.

---

2. Proxy

Intercept Traffic:

- Enable `Proxy > Intercept` to capture requests.
- Use `Forward` to send the request, or edit it before forwarding.

HTTP History:

- View all traffic in `Proxy > HTTP history`.
- Filter to view only in-scope traffic via `Filter > Show only in-scope items`.

---

3. Burp Repeater (Manual Testing)

Send Request to Repeater:

- Right-click an HTTP request in Proxy or Target > `Send to Repeater`.

Modify and Send Requests:

- Modify the request’s parameters, headers, or body.
- Click `Send` to view server responses in real-time.

Analyze Responses:

- Compare different responses by switching between tabs in Repeater.

---

4. Burp Intruder (Automated Attacks)

Send Request to Intruder:

- Right-click a request and select `Send to Intruder`.

Attack Types:

- **Sniper**: Test one variable at a time.
- **Battering Ram**: Use the same payload across multiple positions.
- **Pitchfork**: Use multiple payloads, each for a specific position.
- **Cluster Bomb**: Combine payloads with multiple variables.

Payloads:

- Choose the payload positions and set payload types: simple lists, brute-force numbers, or custom dictionaries.

Launch Attack:

- Click `Start Attack` to brute force or test multiple payloads simultaneously.

---

5. Burp Scanner (Vulnerability Scanning)

Launching a Scan:

- Go to `Dashboard > New Scan` and enter the target URL.
- Choose between **Lightweight** (fast) and **Thorough** (comprehensive) scans.

Configure Scan:

- Set scan options: cookies, authentication, login sequences, etc.
- You can limit the scan to in-scope traffic by setting the scope properly.

View Scan Results:

- Navigate to `Dashboard > Issues` to see found vulnerabilities.
- Click on each issue to see remediation advice.

---

6. Burp Collaborator (Out-of-Band Testing)

Configure Burp Collaborator:

- Enable Collaborator in `Project options > Misc > Burp Collaborator client`.

Test for OAST:

- Burp Collaborator helps you detect Out-Of-Band vulnerabilities such as DNS lookups or asynchronous HTTP requests by creating external service interactions.

---

7. Burp Sequencer (Session Analysis)

Capture Tokens:

- Go to `Sequencer > Live Capture` and capture session tokens.
- Analyze tokens for randomness to assess security.

Manual Analysis:

- You can import session tokens from HTTP history or a manual list and assess their randomness.

---

8. Extender (Extend BurpSuite with Plugins)

Load Extensions:

- Use the `Extender` tab to load additional functionality via BApp Store.
- You can also write your own extensions using the Burp Extender API.

Popular Extensions:

- **Logger++**: Adds advanced logging.
- **JWT4B**: Manages JWTs for testing authentication.
- **Autorize**: Automates authorization tests.

---

9. Burp Decoder (Encode/Decode Data)

Manual Encoding/Decoding:

- Go to `Decoder` tab, paste data, and select encoding methods (Base64, URL encoding, etc.).

Smart Decode:

- Use `Smart Decode` to let Burp automatically identify and decode the input.

---

10. Burp Comparer (Compare Responses)

Compare Requests/Responses:

- Send items to `Comparer` (right-click > `Send to Comparer`).
- Compare them line by line or as a whole, great for detecting subtle differences in behavior.

---

11. Target (Site Mapping & Analysis)

Site Map:

- Browse through the site structure via `Target > Site map`.
- Highlight specific files or directories for further analysis.

Filter Options:

- Filter traffic in the Site Map to include/exclude specific types of requests (e.g., JavaScript, images).

---

12. Tips for Effective Usage

Collaborate Across Tools:

- Combine multiple Burp tools for effective testing. For example, send a request from Proxy to Intruder or Repeater, analyze responses, then repeat tests.

Automate Common Tasks:

- Use **Burp's Macros** to automate repetitive actions like login sequences.
- **Use Burp Extensions**:

- Explore Burp Suite extensions (like **Retire.js** for detecting outdated JavaScript libraries) to extend functionality.

Save/Export Findings:

- Save your session via `Project > Save As`.
- You can export findings (such as issues or HTTP history) for documentation or further analysis.

Common Shortcuts

- **CTRL+Shift+R**: Send request to Repeater.
- **CTRL+Shift+I**: Send request to Intruder.
- **CTRL+Shift+S**: Start a scan.
- **CTRL+Shift+C**: Send request to Comparer.
- **CTRL+E**: Encode/Decode a request.

This cheat sheet is designed to provide quick access to BurpSuite's most powerful features, ensuring an efficient workflow when performing penetration tests and security audits.