**Global Hotkeys**

- Ctrl-I - Send to Intruder
- Ctrl-R - Send to Repeater
- Ctrl-S - Search (places cursor in search field)
- Ctrl-. - Go to next selection
- Ctrl-m - Go to previous selection
- Ctrl-A - Select all
- Ctrl-Z - Undo
- Ctrl-Y - Redo

**Navigational Hotkeys**

- Ctrl-Shift-T - Target Tab
- Ctrl-Shift-P - Proxy Tab
- Ctrl-Shift-R - Repeater Tab
- Ctrl-Shift-I - Intruder Tab
- Ctrl-Shift-O - Project Options Tab
- Ctrl-Shift-D - Dashboard Tab
- Ctrl-Equal - next tab
- Ctrl-Minus - previous tab

**Editor Encoding / Decoding Hotkeys**

- Ctrl-B - Base64 selection
- Ctrl-Shift-B - Base64 decode selection
- Ctrl-H - Replace with HTML Entities (key characters only)
- Ctrl-Shift-H - Replace HTML entities with characters
- Ctrl-U - URL encode selection (key characters only)
- Ctrl-Shift-U - URL decode selection

**Tool Specific Hotkeys**

- Ctrl-F - Forward Request (Proxy)
- Ctrl-T - Toggle Proxy Intercept On and Off
- Ctrl-Space - Send Request (Repeater)
- Double-click <TAB> - Rename a tab

**Editors Hotkeys**

- Ctrl-Delete - Delete Word
- Ctrl-D - Delete Line
- Ctrl-Backspace - Delete Word Backwards
- Ctrl-Home - Go to beginning of document
- Ctrl-Shift-Home - Go to beginning of document and select data on its way
- Ctrl-End - Go to end of document
- Ctrl-Shift-End - Go to end of document and select data on its way
- Ctrl-Left - Go to Previous Word
- Ctrl-Shift-Left - Go to Previous Word and select data on its way
- Ctrl-Right - Go to Next Word
- Ctrl-Shift-Right - Go to Next Word and select data on its way

**Burp Collaborator**

The collaborator enables the penetration tester to listen for call-backs from vulnerable scripts and services via auto-generation of unique DNS names and works on the following protocols:
- DNS
- HTTP & HTTPS
- SMTP & SMTPS

Use the Burp extension Taborator to make Burp Collaborator easier to use on-the-fly.

**Purpose**

This cheat sheet enables users of Burp Suite with quicker operations and more ease of use. Burp Suite is the de-facto penetration testing tool for assessing web applications. It enables penetration testers to rapidly test applications via signature features like repeater, intruder, sequencer, and extender.

It is split into two pages, one page containing common shortcuts to use within the application, the second page containing useful extensions and tips-and-tricks. It is recommended to manually check and test the different extensions available in the product; many which may be very useful to your testing, but outside of what this cheat sheet can cover.

Burp Suite comes in a free community edition and a commercial professional edition. It has a built in Chromium browser for easy set-up of HTTP and SSL/TLS interception.
Users can contribute with extensions to aid in the discovery of vulnerabilities. Be aware of false-positives and use your pentesting capabilities to ensure you fully explore the findings.

**Param Miner**
Allows high-performance identifying of unlinked parameters. Check for unlinked GET and Headers, and unlinked POST when applicable.

**Backslash Powered Scanner**
Will give alerts on interesting transformations of data or other interesting things. Often, it will be false-positives, but it allows the penetration tester to focus on potential vulnerabilities.

**Software Vulnerability scanner**
Checks software version numbers against vulnhub.com for vulnerabilities.

**HTTP Request Smuggler**
This is an extension for Burp Suite designed to help you launch HTTP Request Smuggling attacks.

**Active scan++**
Allows us to find more vulnerabilities in terms of suspicious input transformation, XML input handling, host header attacks and more.

**Retire.js**
Finds outdated JavaScript and links to the relevant CVE's for your investigations.

**Utilities**
These extensions are helpful utilities to a variety of different situations and help bring the penetration tester to their full potential.

**Logger++**
Use this plugin to log and monitor your attacks from e.g., scanner and more. Sort by status-code and do an extra inspection on server 500 errors. When you have done inspections, clear the logs.

**Turbo Intruder**
Python scriptable interface where one can achieve custom functionality and very high speeds of HTTP requests through http pipelining.

**Taborator**
Quickly add and monitor Burp collaborator interactions.

**Authorization and Authentication**

**SAML-Raider**
Useful to inspect SAML messages, edit and resign them.

**JSON Web Tokens**
Lets you decode and manipulate JSON web tokens on the fly, check their validity and automate common attacks.

**Authorize**
Detect if scripts are accessible via different roles or unauthenticated in the web-application.

**Rest API**
The REST API can be enabled in user options. It will by default be enabled on http://127.0.0.1:1337/. It supports interaction via web-application too, not just CLI. Below is a list of endpoints via their URL and the respective cURL command to use them.

The API can be especially useful when you need to send a consolidated list of URLs from a different tool to the scan engine, or perhaps use Burp Suite in headless mode.

To open Burp Suite in headless mode run it with the following arguments:
java -jar -Xmx4g -Djava.awt.headless=true /path/to/burp.jar

Get a list of defined issues:
http://localhost:1337/knowledge_base/issue_definitions
curl -vgw "\n" -X GET 'http://127.0.0.1:1337/v0.1/knowledge_base/issue_definitions'

Scan a URL with the Active Scanner (vulnerability scanner):
http://localhost:1337/scan
curl -vgw "\n" -X POST 'http://127.0.0.1:1337/v0.1/scan' -d '{"urls": ["http://targettgt/scanTarget1", "http://target tgt/scanTarget2"]}'

Check the status and progress of a given scan:
http://localhost:1337/scan/task_id
curl -vgw "\n" -X GET 'http://127.0.0.1:1337/v0.1/scan/mytask_identifier'