BurpSuite Notes

Tabs :

Intruder : Brute force , can automate any change in the request header.
Sequencer : analyzing the quality of randomness in a sample of data items (tokens are random or not).
Comparer : compares two requests or responses (good for broken access controls).
Repeater : save the request to be able to edit many times.
Spider : open all the referer links and send default requests to map the server files).
Scanner: try some values and some attack to the requests and responses to know if this code has any vuln), not in a separate tab from v2.

Extensions :

Authorize : detect broken access control.
Software vulnerability scanner : detects CVE's good for first time when u use a software for first time.
Upload Scanner : Checks for file upload vulnerabilities.
Logger ++ : logs all requests that burp sends , u can grep on them or filter to search for a request.

Collaborator:

like beeceptor and request bin, creates a server that you can send requests too.
good for cookie stealing tests.

Clickbandit:

used for clickjacking POC , easy to do

Engagement tools :

To use , go to a request and right click
Search : (in a target)
    a) HTTP methods
    b) Negative match for CSRF tokens (csrf ,xsrf ,etc ..)
Find comments : get all comments
Find scripts : get all scripts , can export to file and manipulate (also the comments)
CSRF POC :

Response Modification :

inside proxy --> options
u can see hidden forms
enable disabled form fields
convert http to https
remove secure flag --> send cookie on http

Match and Replace :

inside proxy --> options

Upstream Proxy :

inside user options
send to another proxy (local) or directly to a webserver

Tips

Run in incognito :
Firefox -- > addon --> foxyproxy --> manage --> run in private windows --> Allow
in firefox : ALT + D , Alt + Enter --> Duplicates the tab

Shortcuts :

https://github.com/rinetd/BurpSuite-1/blob/master/CheatSheet.md

Send to Repeater : Ctrl+R
Send to Intruder : Ctrl+I

Forward intercepted Proxy message : Ctrl+F
Toggle Proxy interception : Ctrl+T

Switch to Target : Ctrl+Shift+T
Switch to Proxy : Ctrl+Shift+P
Switch to Scanner : Ctrl+Shift+S
Switch to Intruder : Ctrl+Shift+I
Switch to Repeater : Ctrl+Shift+R
Switch to Suite options: Ctrl+Shift+O
Switch to Alerts tab : Ctrl+Shift+A

Go to previous tab :Ctrl+Minus
Go to next tab : Ctrl+Equals

Search : Ctrl+S
Go to previous search match : Ctrl+Comma
Go to next search match : Ctrl+Period

URL-decode : Ctrl+Shift+U
URL-encode key characters : Ctrl+U
HTML-decode : Ctrl+Shift+H
HTML-encode key characters : Ctrl+H
Base64-decode : Ctrl+Shift+B
Base64-encode : Ctrl+B

Backspace word : Ctrl+Backspace
Delete word : Ctrl+Delete
Delete line : Ctrl+D
Go to previous word : Ctrl+Left
Go to previous word (extend selection) : Ctrl+Shift+Left
Go to next word : Ctrl+Right
Go to next word (extend selection) : Ctrl+Shift+Right
Go to previous paragraph : Ctrl+Up
Go to previous paragraph (extend selection) : Ctrl+Shift+Up
Go to next paragraph : Ctrl+Down
Go to next paragraph (extend selection) : Ctrl+Shift+Down
Go to start of document : Ctrl+Home
Go to start of document (extend selection) : Ctrl+Shift+Home
Go to end of document : Ctrl+End
Go to end of document (extend selection) : Ctrl+Shift+End