MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

PREMIUM PROFESSIONAL REFERENCE · 2026

Burp Suite Pro Shortcuts & Extensions Guide

Tools · Workflows · Top 25 BApps

Detailed tool-by-tool workflows, shortcuts, testing methodology, and a curated top-25 BApp extension reference.

21	25	Pro
Tools explained	Extensions	Workflow

https://mnatech.in/ @mna_tech_academy +91 9216110094

How to use this guide

This reference is designed for legal labs, approved assessments, troubleshooting, and professional learning. Replace placeholders with systems you own or are explicitly authorized to test.

> **Authorization first:** Scanning, exploitation, interception, and administrative commands can disrupt services or expose data. Confirm written scope, use conservative rates, preserve evidence, and stop if impact appears.

Contents

01 · Setup & Safe Workflow
Browser, CA certificate, scope, project files, and testing sequence

02 · Every Major Tab & Tool
What it does and how it fits into a professional workflow

03 · Repeater, Intruder & Scanner Deep Dive
Manual validation before automation

04 · Shortcut Reference
High-value navigation and message-editor actions

05 · Top 25 BApp Extensions
Purpose, selection guidance, and operational caution

06 · Official References
Primary documentation and BApp catalog

01

Setup & Safe Workflow

Browser, CA certificate, scope, project files, and testing sequence

1 · Create project

Choose temporary or disk-backed project, then load a reviewed project configuration.

2 · Use embedded browser

It is preconfigured for Burp. For an external browser, configure the proxy and install Burp CA only in a dedicated test profile.

3 · Define scope

Add exact protocols, hosts, ports, and paths; exclude logout, destructive actions, third-party analytics, and production-sensitive routes.

4 · Map manually

Browse each role and workflow, then review Site map and HTTP history before automation.

5 · Test selectively

Use Repeater for hypotheses, Intruder for controlled variation, and Scanner only with approved configurations.

6 · Document

Save evidence, notes, affected requests, observed impact, remediation, and retest results.

02

Every Major Tab & Tool

What it does and how it fits into a professional workflow

Dashboard
Manage crawl/audit tasks, event logs, issue activity, and scan health. Start with strict scope and a saved configuration.

Target / Site map
Build the application map, review discovered endpoints, annotate items, and filter by scope or technology.

Scope
Define included hosts, paths, and protocols plus explicit exclusions so tools do not touch third parties.

Proxy / Intercept
Pause, inspect, edit, forward, or drop browser requests and responses. Keep intercept off during normal browsing.

Proxy / HTTP history
Search and filter all proxied HTTP traffic; send interesting messages to Repeater, Intruder, Comparer, or Organizer.

Proxy / WebSockets history
Inspect bidirectional WebSocket messages and replay selected traffic during authorized testing.

Repeater
Modify and resend one request repeatedly; compare status, length, timing, headers, and body behavior.

Intruder
Automate controlled request variation with positions, payload sets, processing rules, throttling, and result analysis.

Scanner / Audit
Run Burp Professional checks against selected in-scope requests; tune insertion points and scan configuration.

Collaborator
Generate unique interaction domains and detect blind server-side DNS, HTTP, or SMTP callbacks.

Sequencer
Collect token samples and assess randomness characteristics of session or anti-CSRF tokens.

Decoder
Transform URL, HTML, Base64, hex, gzip, and hash representations during analysis.

Comparer
Diff two requests, responses, or token sets by words or bytes.

Logger
Record Burp-generated and extension traffic for troubleshooting complex workflows.

Organizer
Save important requests with notes and status without cluttering Repeater tabs.

Inspector
View and edit decoded parameters, cookies, headers, and HTTP/2 pseudo-headers from the side panel.

Engagement tools
Use discovery, content analysis, scheduling, and report utilities from the context menu.

Extensions / BApp Store
Install reviewed extensions, inspect permissions and resource impact, update regularly, and remove unused tools.

Bambdas
Write small Java-based filters and custom actions to automate Burp data processing.

BChecks
Create custom declarative scan checks for organization-specific vulnerability patterns.

Settings
Separate user defaults from project settings; configure connections, TLS, sessions, logging, and UI behavior.

03

Repeater, Intruder & Scanner Deep Dive

Manual validation before automation

Repeater workflow

```
Proxy history → select request → Ctrl+R → edit one variable → Send → compare response
```

Change one factor at a time. Duplicate tabs for baselines, label tabs, use Inspector for encoded values, and compare status, length, timing, headers, and semantic content.

Note: Use only within approved scope and validate the result before drawing conclusions.

Intruder workflow

```
Send to Intruder → Positions → Payloads → Resource pool → Start attack
```

Choose Sniper for one position at a time, Pitchfork for paired lists, Cluster bomb for combinations, and Battering ram for one payload reused in all positions. Set safe concurrency and delays.

Note: Use only within approved scope and validate the result before drawing conclusions.

Scanner workflow

```
Target/Repeater → Audit selected items → choose scan configuration → review issue evidence
```

Begin with passive checks, then audit a small representative selection. Validate findings manually and avoid unsafe checks unless explicitly approved.

Note: Use only within approved scope and validate the result before drawing conclusions.

Collaborator workflow

```
Generate payload → place in approved input → poll interactions → correlate unique ID
```

Useful for blind SSRF, XXE, SMTP/header injection, and asynchronous behavior. A callback proves interaction, not complete impact; validate context safely.

Note: Use only within approved scope and validate the result before drawing conclusions.

04

Shortcut Reference

High-value navigation and message-editor actions

Shortcut	Use
`Ctrl+R`	Send selected request to Repeater
`Ctrl+I`	Send selected request to Intruder
`Ctrl+Shift+B`	Base64-encode selected text
`Ctrl+Shift+U`	URL-encode selected text
`Ctrl+Z / Ctrl+Y`	Undo / redo editor changes
`Ctrl+F`	Search inside the current message or table
`Ctrl+Plus / Minus`	Increase or decrease UI font size where supported
`Ctrl+Tab`	Move between tabs
`Shift+Ctrl+Tab`	Move to previous tab
`Context menu`	Right-click for send-to-tool, scope, notes, and extension actions

> Keyboard mappings can differ by operating system and Burp version. Open Settings → Keyboard shortcuts to verify or customize them.

05

Top 25 BApp Extensions

Purpose, selection guidance, and operational caution

01 · Logger++
Advanced request/response logging, filtering, highlighting, and investigation.

02 · Autorize
Repeats requests with alternate authorization context to identify access-control differences.

03 · JWT Editor
Views, edits, signs, verifies, encrypts, and decrypts JWTs during authorized testing.

04 · JSON Web Tokens
Decodes and manipulates JWT structures inside Burp messages.

05 · Turbo Intruder
Runs high-performance, scriptable request engines for carefully rate-limited tests.

06 · Param Miner
Finds hidden headers, cookies, and parameters and supports cache-related research.

07 · Active Scan++
Adds extra scan checks for selected web vulnerability classes.

08 · Backslash Powered Scanner
Uses syntax transformation to identify unusual server-side injection behavior.

09 · Collaborator Everywhere
Adds non-destructive Collaborator payloads to reveal hidden backend interactions.

10 · HTTP Request Smuggler
Supports research and detection workflows for HTTP desynchronization issues.

11 · Upload Scanner
Tests file-upload validation using configurable test cases.

12 · Retire.js
Identifies client-side JavaScript libraries with known vulnerable versions.

13 · Software Vulnerability Scanner
Looks for software versions associated with public vulnerability information.

14 · Java Deserialization Scanner
Helps identify Java serialization inputs and test them in controlled environments.

15 · SAML Raider
Views, edits, signs, and tests SAML messages and certificates.

16 · Hackvertor
Applies nested encodings, transformations, tags, and custom conversions.

17 · Content Type Converter
Converts request bodies between form, JSON, XML, and other structures for parser testing.

18 · Copy As Python-Requests
Exports a Burp request as reproducible Python Requests code.

19 · Flow
Provides an alternative chronological view of HTTP and WebSocket traffic.

20 · Wsdler
Parses WSDL files and generates SOAP requests for testing.

21 · GraphQL Raider
Improves GraphQL request editing and supports schema-aware testing workflows.

22 · InQL
Assists GraphQL introspection, query generation, and endpoint analysis.

23 · JS Miner
Finds endpoints, secrets-like strings, and interesting references in JavaScript and JSON.

24 · Taborator
Manages Collaborator payloads and interactions from a dedicated tab.

25 · 403 Bypasser

Tests benign request variations against access-denied endpoints to find inconsistent enforcement.

Extension hygiene: Extensions are third-party code. Review source, publisher, permissions, update history, resource impact, and data handling. Install only what the project needs.

06

Official References

Primary documentation and BApp catalog

Burp Suite documentation
https://portswigger.net/burp/documentation/contents

Desktop tools
https://portswigger.net/burp/documentation/desktop/tools

BApp Store
https://portswigger.net/bappstore

Keep learning safely

Website
https://mnatech.in/

Instagram
@mna_tech_academy

Call / WhatsApp
+91 9216110094

Practice rule
Only test systems you own or have written authorization to assess.

© 2026 MNA Tech Academy. All rights reserved.
Original educational reference. Product names and trademarks belong to their respective owners. Commands may vary by version and operating system; verify with official documentation before production use.