+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 05/19/2026

Sign up

Burp Suite Certified Practitioner Training

4 days (28 hours)

Overview

The Burp Suite Certified Practitioner training course prepares you to use Burp Suite methodically to audit web applications and APIs. You will gain efficiency in practical use cases: interception, request manipulation, automation, vulnerability validation, and evidence documentation.

The goal is to make you operational so you can conduct a comprehensive application penetration test with Burp Suite: mapping, identifying entry points, controlled exploitation, and risk prioritization. The focus is on common vulnerabilities (authentication, sessions, injections, business logic) and on the reproducibility of results.

The approach is hands-on: guided workshops, step-by-step demos, timed exercises, and corrections. You'll leave with audit checklists, an optimized Burp configuration, Repeater/Intruder scripts and playbooks, and a report template including evidence, impact, and recommendations.

Objectives

- Configure Burp Suite (proxy, CA, scope) and secure the testing environment.
- Map an application and identify web/API attack surfaces.
- Use Repeater, Intruder, and Sequencer to validate hypotheses.
- Detect and demonstrate vulnerabilities (authentication, session, injections, access).
- Produce reproducible evidence and formulate actionable recommendations.

Target Audience

- Penetration testers and application security consultants
- Developers/DevSecOps looking to strengthen security testing
- SOC/AppSec analysts responsible for patch validation

Prerequisites

- Solid foundation in HTTP/HTTPS, cookies, headers, and status codes
- Basic understanding of web security (OWASP Top 10) and authentication
- Ability to read and edit JSON and understanding of REST APIs
- Knowledge of Linux/Windows and terminal usage

Technical prerequisites

- PC with at least 8 GB of RAM (16 GB recommended) and 10 GB of free disk space
- Windows, macOS, or Linux (Chromium/Firefox browser)
- Burp Suite (Community or Professional depending on context) and Java if required
- Additional tools: curl, a code editor, Docker or VM for labs

Burp Suite Certified Practitioner Training Program

[Day 1 - Morning]

Getting started with Burp Suite and setting up the proxy

- Understanding Burp's role in a web penetration test (proxy, interception, modification)
- Configuring the browser and CA certificate to intercept HTTPS traffic
- Mastering the essential views: Proxy, HTTP History, Target, Logger
- Defining the scope and effectively filtering relevant traffic
- Hands-on workshop: Configuring Burp + browser and intercepting a login session.

[Day 1 - Afternoon]

Mapping the application: Target, crawling, and request analysis

- Building a map: directory structure, endpoints, parameters, HTTP methods
- Identifying sensitive areas: authentication, administration, APIs, uploads, search
- Analyzing sessions (cookies, tokens) and security headers
- Reproducing and comparing requests (Repeater) to validate hypotheses
- Hands-on workshop: Mapping a target application and isolating 10 priority endpoints.

[Day 2 - Morning]

Test authentication and session management with Burp

- Verify the robustness of login mechanisms (error messages, lockouts, MFA)
- Verify cookie security (Secure, HttpOnly, SameSite) and session rotation

- Detect common weaknesses: pinning, reuse, expiration, incomplete logout
- Manipulate tokens (JWT, opaque tokens) and validate server-side impacts
- Hands-on workshop: Re-enact an authentication flow and demonstrate a session issue.

[Day 2 - Afternoon]

Automate attacks: Intruder, payloads, and detection rules

- Configuring Intruder: positions, attack types, encoding handling
- Building effective payloads (lists, rules, transformations, grep/extract)
- Quickly detect anomalies: codes, sizes, response times, redirects
- Optimizing tests (throttling, exclusions, error handling, noise reduction)
- Hands-on workshop: Perform parameter-targeted fuzzing and identify abnormal behavior.

[Day 3 - Morning]

Exploiting web vulnerabilities with Repeater and Burp tools

- Test injections (SQLi, NoSQLi, command injection) using controlled variations
- Validate XSS vulnerabilities (reflected/stored) and context/encoding constraints
- Analyzing access controls (IDOR, BOLA) via changes to credentials and roles
- Identify logic flaws (workflow, bypasses, client-side validations)
- Hands-on workshop: Exploit an IDOR and demonstrate unauthorized access to a resource.

[Day 3 - Afternoon]

Burp scanning and manual validation: prioritize, confirm, and reduce false positives

- Run targeted scans based on the scope and interpret the results (severity, confidence)
- Manually confirm an alert: proof, impact, reproducibility conditions
- Exploit common vulnerabilities: SSRF, path traversal, open redirect, CORS, headers
- Document proof requests/responses and prepare corrective recommendations
- Hands-on workshop: Scan a defined area and produce 3 validated proofs of concept (PoCs) with Repeater.

[Day 4 - Morning]

Extensions, macros, and advanced workflows to boost efficiency

- Install and use extensions (BApp Store) tailored to your needs (auth, JWT, logging)

- Configure macros and session handling rules to automate authentication
- Chain tests: token extraction, re-injection, session maintenance on Intruder/Repeater
- Enhance analysis: Compare, Decode, Sequencer, search, and annotations
- Hands-on workshop: Set up a login macro and use it in an Intruder test.

[Day 4 - Afternoon]

Certification preparation: methodology, reporting, and mock exam

- Structuring an “exam-ready” approach: reconnaissance, prioritization, exploitation, evidence
- Managing time and scope: checklists, notes, reliable reproduction of vulnerabilities
- Writing actionable findings: description, steps, impact, fixes, technical references
- Consolidating knowledge: common mistakes, pitfalls, Burp best practices
- Hands-on workshop: Guided mock exam + mini-report (evidence, impacts, remedies).

Target Audience

This training is intended for both individuals and companies, large or small, seeking to train their teams in new advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

Assessment upon enrollment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Practical Course: 60% Practical, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and reflection sessions, and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been properly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training program.