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

Updated on 06/05/2026

Sign up

GIAC GWEB® Certification Training

3 days (21 hours)

Overview

The GIAC Certified Web Application Defender (GWEB) Practitioner certification prepares you to defend web applications in real-world conditions: risk analysis, hardening, testing, and vulnerability response. It is designed for teams responsible for securing APIs, business portals, and exposed applications.

During this training, you will adopt a practical and operational approach focused on common vulnerabilities (authentication, session management, injections, XSS, configuration) and defensive controls (validation, encoding, headers, logging). Concepts are systematically linked to real-world scenarios: code review, alert triage, remediation, and verification.

The training alternates between demos and guided workshops: replicating attacks, implementing countermeasures, and then validating them through testing. Deliverables: hardening checklists, review grid, prioritized remediation plan, and verification scripts/commands.

Objectives

- Identify web attack vectors and their impacts.
- Analyze an application and prioritize risks.
- Implement defensive controls (validation, encoding, headers).
- Test and verify fixes using appropriate tools.
- Document a remediation plan and security evidence.

Target Audience

- Web and API developers
- Application security engineers / AppSec
- DevOps / SRE professionals involved in hardening
- Defense-oriented testers / pentesters

Prerequisites

- Basics of HTTP, cookies, sessions, REST
- Basic understanding of web security (OWASP Top 10)
- Code reading (at least one web language)
- Comfortable with the command line

Technical prerequisites

- Windows (WSL2), macOS, or Linux
- Modern browser and code editor
- Burp Suite Community, curl, Docker (or provided VM)

Course Outline for our GIAC GWEB® Certification Training

[Day 1 - Morning]

Fundamentals of Web Application Security and Risk Mapping

- Understanding the client/server model: HTTP/HTTPS, cookies, sessions, headers
- Identifying attack surfaces: endpoints, parameters, files, APIs, authentication
- Prioritizing risks using the OWASP Top 10 and realistic exploitation scenarios
- Implementing a defense strategy: prevention, detection, response
- Hands-on workshop: Map a target application (routes, parameters, sensitive data) and create a risk matrix.

[Day 1 - Afternoon]

Authentication, sessions, and access controls

- Hardening authentication: password policies, MFA, lockout, anti-brute-force
- Securing sessions: Secure/HttpOnly/SameSite cookies, rotation, expiration
- Avoiding access control vulnerabilities: IDOR, privilege escalation, role separation
- Best practices for implementation: error handling, messages, redirects
- Hands-on workshop: Testing and fixing IDOR and session fixation scenarios on a demo application.

[Day 2 - Morning]

Input validation and injection prevention

- Implementing robust validation: whitelists, normalization, server-side constraints
- Preventing SQL Injection: parameterized queries, ORM, least privilege database
- Preventing system injections: commands, paths, deserialization, templates
- Handling encoding/output: HTML context, attributes, URLs, JavaScript
- Hands-on workshop: Exploit and then fix an injection (SQL and command) using parameterization and validation.

[Day 2 - Afternoon]

Protection against XSS, CSRF, and browser-side attacks

- Distinguish between reflected, stored, and DOM XSS and apply appropriate countermeasures
- Implement a pragmatic CSP and handle exceptions (nonce, hash)
- Preventing CSRF: tokens, SameSite, origin verification, double-submit
- Hardening headers: HSTS, X-Content-Type-Options, Referrer-Policy, Permissions-Policy
- Hands-on workshop: Add a CSP and CSRF protections, then validate their effectiveness through attack tests.

[Day 3 - Morning]

API security and secret management

- Securing REST APIs: authentication, authorization, scopes, object control
- Limiting exposure: pagination, filtering, rate limiting, anti-enumeration protections
- Validating schemas: contracts, types, sizes, formats, error handling
- Managing secrets: environment variables, rotation, vault, removing secrets from code
- Hands-on workshop: Auditing an API (access controls, rate limiting, validation) and fixing .

[Day 3 - Afternoon]

Hardening, logs, testing, and preparation for the GWEB exam

- Configuring application security: TLS, error handling, server hardening, and dependencies
- Implementing actionable logging: auth events, access, errors, correlation, retention
- Integrating security into the development cycle: reviews, SAST/DAST, dependency scans, quality criteria
- Building a remediation plan: prioritization, proof of correction, non-regression
- Hands-on workshop: Conduct an end-to-end mini-audit (tests + fixes) and produce a GWEB-aligned defense checklist.

Relevant companies

This training program is designed for both individuals and businesses—large and small—that wish to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

Placement 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.