

/ OFFENSIVE

Web Application Penetration Test

€2,000

ONE-OFF

Goal-based web app pentest with a prioritised findings report.

// DELIVERABLES

- Scope & rules-of-engagement document agreed at kickoff.
- Manual, goal-led testing of authenticated and unauthenticated surfaces, aligned to the OWASP Web Security Testing Guide and OWASP Top 10.
- Findings report: executive summary plus technical detail, each issue rated by severity (CVSS) with reproduction steps and proof-of-concept.
- Prioritised, actionable remediation guidance per finding.
- One round of retesting on Critical and High findings after fixes.

// EXPECTED OUTCOMES

- A clear, evidence-backed view of what is genuinely exploitable in the application.
- A ranked fix list the engineering team can act on immediately.
- Reportable assurance for customers, partners and auditors.

// METHOD OF ENGAGEMENT

Time-boxed, goal-based engagement run remotely. Scoping call, hands-on testing combining manual techniques and tooling, then a written report and findings walkthrough.

// TIMELINE

Indicative: ~5–10 business days end to end — 1 day scoping, 3–5 days testing, ~2 days reporting. Retest scheduled once fixes are confirmed.

- Project management is included in all prices.

