

HR & PAYROLL SAAS

28 findings in a payroll platform, one of them critical

Web application penetration test · fixed price · free retest

28

FINDINGS

1

CRITICAL

5

HIGH

THE CHALLENGE

A payroll and HR SaaS platform handling sensitive employee and financial data needed a deep, manual test of its web application, beyond what automated scanning could reach.

01

Scope

Roles, environments, test accounts and rules of engagement agreed in writing, with a fixed price before any work began.

02

Manual testing

Senior in-house testers worked the application by hand to PTES and OWASP standards: authentication, sessions, authorization, business logic and the framework underneath.

03

Escalate

Anything critical is escalated to the client's team as soon as it is confirmed, not held back for the final report.

04

Report and retest

An executive summary, full technical findings with reproduction steps, and a free retest of every fix.

WHAT WE FOUND

CRITICAL

A file-inclusion flaw that let an attacker read sensitive files from the server through the application itself.

HIGH

Stored cross-site scripting capable of session theft, insecure direct object references, and a vertical authorization bypass that let an administrator create or delete organization owners.

HIGH

Session-handling weaknesses in the application's token model rounded out the high-severity findings.

THE OUTCOME

Delivered a remediation plan sequenced by real business impact, critical and high findings first, with a complimentary retest to verify every fix.

A SIMILAR ENGAGEMENT TODAY

Web application penetration test, Medium

An established product with several user roles, an admin panel and third-party integrations. Fixed in writing before work begins, free retest included.

FROM

\$7,800

PUBLISHED PRICE · USD

Get a fixed-price quote

Scope in one short form. Proposal within one business day.

invadel.com/scope

info@invadel.com · +1 (929) 591-9013