

WEB APPLICATION · BUSINESS PLATFORM

An unauthenticated page that exposed every user's tokens

Web application penetration test · OWASP WSTG

11

FINDINGS

1

HIGH-SEVERITY

4

MEDIUM-SEVERITY

THE CHALLENGE

A business web application with user, admin, and super-user roles needed a manual test against the OWASP Web Security Testing Guide, beyond what automated scanning reaches: authentication, access control, TLS, and the API behind it.

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 the OWASP testing guide: authentication, sessions, authorization, business logic and the API behind it.

03

Escalate

Anything high-risk 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

HIGH

Inconsistent access control: an unauthenticated visitor could reach a resource that listed registered users along with their access tokens, refresh tokens, and personal details.

MEDIUM

Deprecated TLS 1.0 and 1.1 and SHA-1 cipher suites were still enabled, and the Swagger / OpenAPI documentation was public, mapping every API endpoint for an attacker.

MEDIUM

The login form enforced no account lockout, so passwords could be guessed without limit; a weak password policy and session IDs held in local storage compounded it.

THE OUTCOME

Delivered a report mapped to the OWASP WSTG with reproduction steps for each of the 11 findings, sequenced high-severity first. A retest was run once the team had shipped fixes, and the results were reissued as a final report.

A SIMILAR ENGAGEMENT TODAY

Web application penetration test, Medium

An established product with several user roles, an admin panel and an API. 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