Web Application Assessment Slides

OWASP Top 10:2025

Lysandre Services

01 September 2026 - 05 September 2026

Vulnotes Security Consulting

Version 1.0.0

CONFIDENTIAL

Engagement scope

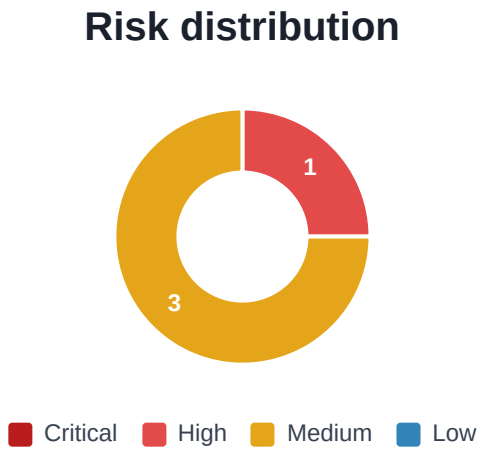
Client Portal 3.2.1 in staging. The review covers document reads, search, comments and export jobs across two tenant contexts. Source and unit-test records provide the evidence. Production and third-party systems remain outside the assessment.

Assessment conclusions

The Client Portal assessment identified four findings: one High and three Medium. The search repository presents the highest technical severity because the reviewed query path mixes input with SQL structure. Tenant authorization, stored content rendering and export-state consistency require separate corrections.

Limits

The review covers the application records and release identified in scope. Supply-chain provenance, recovery flows and operational alert delivery require additional assessment.



Evidence review

E-01 / WEB APP		
Reviewed item	**Scope**	**Recorded state**
Read service	Document repository	Tenant predicate missing
Authorization tests	Cross-tenant reads	Denial case absent
Evidence register / Review window: 01-05 September 2026		

E-01 - Reviewed record extract, September 2026.

OWASP Top 10:2025 / A01-A10

Category	Coverage	Evidence and limits
A01:2025 - Broken Access Control	Gap observed	F-1 / E-01: document read scope. Other object types and SSRF remain outside this sample.
A02:2025 - Security Misconfiguration	Partial	E-00: header and runtime-setting records only. Full deployment review remains open.
A03:2025 - Software Supply Chain Failures	Not assessed	No dependency inventory, build provenance or pipeline access supplied.
A04:2025 - Cryptographic Failures	Partial	E-00: transport configuration only. Storage encryption and key lifecycle remain unassessed.
A05:2025 - Injection	Gap observed	F-2 / E-02 and F-3 / E-03: query construction and rich-text rendering.
A06:2025 - Insecure Design	Partial	E-00: workflow specification reviewed. No complete threat model or abuse-case review.
A07:2025 - Authentication Failures	Partial	E-00: login and sign-out records only. Recovery and federated identity remain unassessed.
A08:2025 - Software or Data Integrity Failures	Not assessed	No signed-update or imported-data integrity evidence supplied.
A09:2025 - Security Logging and Alerting Failures	Partial	E-00: event schema only. No alert delivery or response exercise demonstrated.
A10:2025 - Mishandling of Exceptional Conditions	Gap observed	F-4 / E-04: export-job cleanup on dependency error. Other failure paths remain open.

Source: OWASP Top 10:2025. Coverage records describe this engagement only.

Finding F-1

F-1 / A01:2025	Medium / CVSS 6.5 / 10

Document reads lack an explicit tenant authorization constraint

One document read service omits the tenant constraint. Enforce the server-side boundary and retain authorization regression results.

Required closure evidence: Scoped repository query, policy review and passing isolated allow/deny tests. Retest pending.

Owner and planned target

Maya Laurent, application lead. 30 September 2026 (planned).

Finding F-2

F-2 / A05:2025	High / CVSS 8.1 / 10

Search queries combine user data with SQL structure

One search repository mixes filter data with query text. Parameter binding and controlled identifiers address the construction defect.

Required closure evidence: Reviewed binding implementation and isolated repository regression results. Retest pending.

Owner and planned target

Maya Laurent, application lead. 30 September 2026 (planned).

Finding F-3

F-3 / A05:2025	Medium / CVSS 5.4 / 10

Stored rich text lacks a documented sanitization boundary

The comment renderer accepts stored HTML without a defined sanitizer boundary. Apply the same formatting policy across every rendering path.

Required closure evidence: Sanitizer policy, component regression results and legacy-content review. Retest pending.

Owner and planned target

Noah Vidal, frontend lead. 16 October 2026 (planned).

Finding F-4

F-4 / A10:2025	Medium / CVSS 5.4 / 10

Export-job errors leave inconsistent completion state

Export completion precedes artifact persistence. Define a consistent failure state and verify idempotent recovery with an isolated mocked dependency.

Required closure evidence: State-transition review and isolated failure/retry regression results. Retest pending.

Owner and planned target

Ines Martin, backend lead. 16 October 2026 (planned).

Remediation decisions

Maya Laurent owns the application correction plan. Noah Vidal owns rich-text rendering and Ines Martin owns export recovery. The sponsor must approve the proposed correction dates and provide a staging build for retest. All four findings remain Open.

Retest and closure

Planned window: 19-20 October 2026. Review the corrected release and isolated regression evidence for all four findings. Sophie Roux reviews closure. Record residual exceptions explicitly before changing finding status.

OWASP Top 10:2025. Category names: OWASP, CC BY 3.0.