Web Application Assessment

OWASP Top 10:2025

Lysandre Services

01 September 2026 - 05 September 2026

Vulnotes Security Consulting

Version 1.0.0

CONFIDENTIAL

Document reference: WebAPP_Example

Version: 1.0.0

REPORT		
VERSION	DATE	COMMENT
1.0.0	16 September 2026	Original version

REPORT VALIDATORS			
DATE	AUTHOR	DESCRIPTION	FUNCTION
16 September 2026	Julien Perrin	Author	Cybersecurity auditor
16 September 2026	Sophie Roux	Reviewer	Cybersecurity auditor

REPORT DIFFUSION	
NAME	EMAIL
Maya Laurent - application engineering team	maya.laurent@lysandre.example

Table of Contents

Executive assessment

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.

Assessment analysis

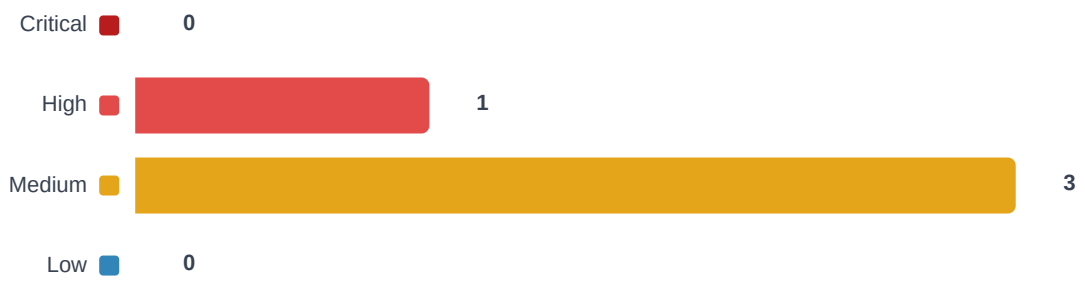
The assessment of Client Portal 3.2.1 identified 4 findings: 0 Critical, 1 High, 3 Medium, 0 Low. The review covered document retrieval, search, comments and document exports across two tenant contexts. Configuration and source records were compared with the agreed service requirements.

The principal improvement concerns document reads lack an explicit tenant authorization constraint. A caller with a valid application session could obtain document data outside the intended tenant boundary if the affected service exposes the reviewed path without another effective check. That would affect document confidentiality. The sample does not establish modification or deletion capability, and business priority depends on the importance of tenant separation. Correction ownership rests with Maya Laurent, application lead. The priority is to reduce this exposure without interrupting the service's required business functions.

The remaining observations concern search queries combine user data with sql structure and stored rich text lacks a documented sanitization boundary and export-job errors leave inconsistent completion state. They require separate acceptance criteria because changing one policy does not establish that the other controls operate effectively. Review effective runtime behavior as well as the saved configuration.

The application has distinct application and repository layers, with named service owners and traceable release records. These controls provide a basis for remediation, but their presence does not compensate for the documented exceptions. The action plan separates implementation evidence from successful retest results.

Risk distribution



Scope and methodology

Application and evidence

Lysandre Services. Client Portal 3.2.1, staging portal.lysandre.example. Documentary sample: document reads, search, comments and document exports. Two tenant contexts and reader/editor roles. E-00 records the supplied scope, configuration, login flow and event schema.

Approach

Review of source excerpts, configuration records and unit-test inventories. Each finding distinguishes a missing control from demonstrated runtime impact. No live target testing, executable payloads or production changes. OWASP Top 10:2025 organizes the risk discussion. Detailed verification requirements require a separately agreed standard and test plan.

Limitations

Production, third-party systems, CI/CD access, full dependency provenance, key management, account recovery and operational alert exercises are excluded. Partial coverage means the supplied records cover only part of a category. No complete security or compliance assurance follows from this sample.

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.

Coverage interpretation

Gap observed: linked evidence supports a finding. Partial: some evidence exists but category-wide conclusions are unavailable. Not assessed: no suitable evidence supplied. A category with no recorded finding is not automatically secure. Classification is by root cause, and a finding may require more than one documented mapping in a real engagement.

Review focus by category

Category	Review focus
A01:2025	Object ownership, tenant boundaries and server-side request restrictions
A02:2025	Runtime settings, exposed services and effective deployment configuration
A03:2025	Dependency provenance, build systems and distribution controls
A04:2025	Transport protection, sensitive storage and key lifecycle
A05:2025	Query construction, interpreters and browser rendering contexts
A06:2025	Business invariants, threat assumptions and abuse-resistant workflows
A07:2025	Login, account recovery and session lifecycle
A08:2025	Trust in code and data artifacts at processing boundaries
A09:2025	Security events, alert delivery and response ownership
A10:2025	Error paths, safe failure and recovery consistency

The Top 10 is an awareness taxonomy. Agree detailed verification requirements separately, including the chosen ASVS version and requirement IDs when applicable.

Vulnerabilities

OWASP	Title	CVSS Score
A01:2025	F-1 / Document reads lack an explicit tenant authorization constraint	6.5
A05:2025	F-2 / Search queries combine user data with SQL structure	8.1
A05:2025	F-3 / Stored rich text lacks a documented sanitization boundary	5.4
A10:2025	F-4 / Export-job errors leave inconsistent completion state	5.4

A01:2025 - Broken Access Control

OWASP description - official excerpt

Access control enforces policy such that users cannot act outside of their intended permissions.

Description summary

Authorization must limit each identity to the resources and operations it is entitled to use. Weak object ownership checks, excessive privileges and incomplete server-side enforcement can expose information or permit unauthorized changes. Review authorization at every relevant trust boundary, rather than relying on interface restrictions.

Assessment coverage

Gap observed

F-1 / E-01: document read scope. Other object types and SSRF remain outside this sample.

Findings in this category: 1. Detailed records follow on separate pages.

1.1. Document reads lack an explicit tenant authorization constraint

F-1 / A01:2025

BASE SCORE							6.5
Attack vector	Complexity	Privileges	User interaction	Scope	Confidentiality	Integrity	Availability
Network	Low	Low	None	Unchanged	High	None	None

1.1.1. Description

The source-review bundle identifies a document retrieval service that resolves a record identifier without applying the caller's tenant scope. The accompanying authorization unit-test record omits the cross-tenant denial case. The intended boundary requires every document read to enforce both tenant membership and the permitted operation.

Technical analysis

Authentication identifies the caller but does not establish authorization for the selected object. The service must carry trusted identity context into the data-access decision. Unpredictable record identifiers and a filtered user interface cannot replace a server-side authorization predicate.

Scope and limits

Evidence concerns one read service in staging release 3.2.1. It supports a missing-control finding from documentary analysis. No live cross-account retrieval, write access, administrator compromise or access to actual customer documents was performed.

1.1.2. Impact

A caller with a valid application session could obtain document data outside the intended tenant boundary if the affected service exposes the reviewed path without another effective check. That would affect document confidentiality. The sample does not establish modification or deletion capability, and business priority depends on the importance of tenant separation.

1.1.3. Remediation

1. Apply a centralized authorization decision using the authenticated identity, tenant and requested operation before returning a document.
2. Carry the authorized scope into the repository query and related download or preview services. Treat client-provided tenant identifiers as untrusted input.
3. Add isolated authorization tests covering permitted reads and denied tenant or role combinations. Log denials without recording document contents.

Owner: Maya Laurent, application lead. Planned correction: 30 September 2026.

F-1 / Supporting evidence

evidence

E-01: document-service review and authorization test inventory, 3 September 2026. Tenant predicate absent from the reviewed data-access path. No live response capture.

Acceptance criterion

The corrected service applies the approved tenant and operation constraints. Isolated unit tests cover both allowed and denied cases, with no customer data or external requests.

Retest pending. The statements above describe required closure evidence and do not assert a successful retest.

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.

CVSS v3.1: 6.5 (Medium)
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

The vector rates the affected component and prerequisites described in this finding. Business priority additionally considers exposure, data sensitivity and delivery dependencies.

Repository correction

```
return documents.findOne({
  id: documentId,
  tenantId: principal.tenantId
});
```

1.1.4. References

A01:2025 - Broken Access Control. Mapping rationale: the reviewed root cause matches this category. Other risks require separate evidence.

OWASP Top 10:2025

Engagement baseline WEB-DEMO-2026-09, evidence E-01.

FIRST CVSS v3.1 scoring specification

A02:2025 - Security Misconfiguration

OWASP description - official excerpt

Security misconfiguration is when a system, application, or cloud service is set up incorrectly from a security perspective, creating vulnerabilities.

Description summary

This category concerns insecure operational settings across the application and its hosting stack. Examples include unnecessary services, unchanged defaults, overly permissive cloud settings and excessive diagnostic output. Repeatable hardening and configuration verification help keep environments aligned with their security requirements.

Assessment coverage

Partial
E-00: header and runtime-setting records only. Full deployment review remains open.
Findings in this category: 0. Detailed records follow on separate pages.
No recorded findings in this category. This does not establish that the category is secure.

A03:2025 - Software Supply Chain Failures

OWASP description - official excerpt

Software supply chain failures are breakdowns or other compromises in the process of building, distributing, or updating software.

Description summary

The scope extends beyond outdated libraries to the tools, repositories, dependencies and delivery processes used to produce software. Component inventories, trusted provenance, controlled changes and protected build infrastructure reduce the likelihood that vulnerable or unauthorized components reach production.

Assessment coverage

Not assessed

No dependency inventory, build provenance or pipeline access supplied.

Findings in this category: 0. Detailed records follow on separate pages.

No recorded findings in this category. This does not establish that the category is secure.

A04:2025 - Cryptographic Failures

OWASP description - official excerpt

Generally speaking, all data in transit should be encrypted at the transport layer (OSI layer 4).

Description summary

Sensitive information also needs protection appropriate to its storage and application-level use. Weak algorithms, exposed keys, unreliable randomness, poor certificate validation and inappropriate password handling can undermine confidentiality or authenticity even where encryption is nominally enabled.
Official OWASP Top 10:2025 category description - OWASP, CC BY 3.0. Short excerpt; summary adapted for this report.

Assessment coverage

Partial
E-00: transport configuration only. Storage encryption and key lifecycle remain unassessed.
Findings in this category: 0. Detailed records follow on separate pages.
No recorded findings in this category. This does not establish that the category is secure.

A05:2025 - Injection

OWASP description - official excerpt

An injection vulnerability is an application flaw that allows untrusted user input to be sent to an interpreter ...

Description summary

When an interpreter treats external data as instructions, the intended separation between data and executable structure fails. This applies to database queries, browser markup and other interpreted contexts. Review how each context binds, validates or sanitizes data and whether those controls match the interpreter involved.
Official OWASP Top 10:2025 category description - OWASP, CC BY 3.0. Short excerpt; summary adapted for this report.

Assessment coverage

Gap observed
F-2 / E-02 and F-3 / E-03: query construction and rich-text rendering.
Findings in this category: 2. Detailed records follow on separate pages.

5.1. Search queries combine user data with SQL structure

F-2 / A05:2025

BASE SCORE							8.1
Attack vector	Complexity	Privileges	User interaction	Scope	Confidentiality	Integrity	Availability
Network	Low	Low	None	Unchanged	High	High	None

5.1.1. Description

The data-access review shows one search repository combining a user-controlled filter with SQL statement text. The supplied code-review checklist does not evidence parameter binding for that value. The search function operates on the staging tenant's business-document index.

Technical analysis

When query structure and data share the same construction channel, database interpretation can diverge from the developer's intended query. Binding values separates these roles. Validation alone is insufficient for free-text search, while non-bindable identifiers such as sort columns require an explicit server-side allowlist.

Scope and limits

This finding derives from a source-review record, not an executed injection or database extraction. The database account's full effective privileges and additional runtime controls were not supplied. Authentication bypass, operating-system execution and full database compromise are not claimed.

5.1.2. Impact

The unsafe construction may allow the search operation to address unintended data or change query semantics within the database account's permissions. The exposure concerns confidentiality and potentially integrity, depending on effective privileges. The sample does not establish data loss or availability impact. The High contextual rating reflects a material break between user input and database instructions.

5.1.3. Remediation

1. Use the database driver's parameter-binding facility for every search value and keep SQL structure under application control.
2. Map supported sort or field identifiers to a small server-side allowlist. Review adjacent repository methods for the same construction pattern.
3. Add isolated repository tests that verify binding and normal search behavior. Review the service account's database privileges and retain the approved scope.

Owner: Maya Laurent, application lead. Planned correction: 30 September 2026.

F-2 / Supporting evidence

evidence

E-02: search repository review, 3 September 2026. One construction path lacks demonstrated parameter binding. No payload, query execution or database output included.

Acceptance criterion

The reviewed repository binds all user data through the driver and restricts structural identifiers. Regression evidence confirms normal search behavior in an isolated test database.

Retest pending. The statements above describe required closure evidence and do not assert a successful retest.

E-02 / WEB APP

Reviewed item	Scope	Recorded state
Search repository	User filter	Concatenated into query text
Data-access checklist	Parameter binding	Not demonstrated

Evidence register / Review window: 01-05 September 2026

E-02 - Reviewed record extract, September 2026.

CVSS v3.1: 8.1 (High)
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

The vector rates the affected component and prerequisites described in this finding. Business priority additionally considers exposure, data sensitivity and delivery dependencies.

Parameterized query

```
const sql = "SELECT id, title FROM documents WHERE tenant_id = $1 AND title
ILIKE $2";
return db.query(sql, [principal.tenantId, searchPattern]);
```

5.1.4. References

A05:2025 - Injection. Mapping rationale: the reviewed root cause matches this category. Other risks require separate evidence.

OWASP Top 10:2025

Engagement baseline WEB-DEMO-2026-09, evidence E-02.

FIRST CVSS v3.1 scoring specification

5.2. Stored rich text lacks a documented sanitization boundary

F-3 / A05:2025

BASE SCORE							5.4
Attack vector	Complexity	Privileges	User interaction	Scope	Confidentiality	Integrity	Availability
Network	Low	Low	Required	Changed	Low	Low	None

5.2.1. Description

The rendering review identifies a stored-comment view that accepts rich HTML and renders it through a raw HTML insertion mechanism. The provided component contract does not identify a sanitization step or an allowed-element policy before rendering.

Technical analysis

Rich text deliberately preserves some markup, so ordinary text escaping and HTML sanitization address different requirements. A maintained HTML parser with a constrained policy can retain approved formatting while excluding active content. The same policy must cover editing, previews and later display of previously stored material.

Scope and limits

The source record shows a missing documented control in one comment component. No executable browser payload, session theft or interaction with a real user was performed. Existing browser policy and upstream controls were not fully evidenced and may affect practical exposure.

5.2.2. Impact

If untrusted markup reaches the browser without effective sanitization, a stored comment may alter trusted page content or permit script behavior in the application origin. The possible reach depends on the viewer's permissions and browser controls. HttpOnly cookies reduce direct cookie access but do not establish that all same-origin actions are safe. The Medium rating remains contextual to the reviewed component.

5.2.3. Remediation

1. Define the formatting requirement and use text rendering where HTML is unnecessary. For necessary rich text, apply a maintained sanitizer with an explicit element and attribute policy.
2. Use the same sanitization boundary for previews and persisted content. Assess legacy stored comments before deploying the corrected renderer.
3. Retain restrictive browser policies as defense in depth and add isolated component tests for allowed formatting and rejected unsupported markup.

Owner: Noah Vidal, frontend lead. Planned correction: 16 October 2026.

F-3 / Supporting evidence

evidence

E-03: comment-view component and rendering contract, 4 September 2026. No sanitization boundary documented for stored rich HTML. No executable evidence included.

Acceptance criterion

Component tests confirm the approved formatting policy across edit, preview and display paths. The release review covers existing stored comments and the effective browser policy.

Retest pending. The statements above describe required closure evidence and do not assert a successful retest.

E-03 / WEB APP

Reviewed item	Scope	Recorded state
Comment renderer	Stored HTML	No sanitizer contract
Policy review	Allowed elements	Not defined

Evidence register / Review window: 01-05 September 2026

E-03 - Reviewed record extract, September 2026.

CVSS v3.1: 5.4 (Medium)
CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

The vector rates the affected component and prerequisites described in this finding. Business priority additionally considers exposure, data sensitivity and delivery dependencies.

Rich-text rendering policy

```
const safeHtml = sanitizer.clean(storedHtml, {
  allowedTags: ["p", "strong", "em", "ul", "li"],
  allowedAttributes: {}
});
```

5.2.4. References

A05:2025 - Injection. Mapping rationale: the reviewed root cause matches this category. Other risks require separate evidence.

OWASP Top 10:2025

Engagement baseline WEB-DEMO-2026-09, evidence E-03.

FIRST CVSS v3.1 scoring specification

A06:2025 - Insecure Design

OWASP description - official excerpt

Insecure design is a broad category representing different weaknesses, expressed as “missing or ineffective control design.”

Description summary

Architectural omissions differ from implementation defects: correct code cannot enforce a safeguard that was never designed. Security requirements, business-risk analysis and threat modeling should establish expected behavior, abuse cases, tenant separation and safe failure paths before implementation.

Official OWASP Top 10:2025 category description - OWASP, CC BY 3.0. Short excerpt; summary adapted for this report.

Assessment coverage

Partial

E-00: workflow specification reviewed. No complete threat model or abuse-case review.

Findings in this category: 0. Detailed records follow on separate pages.

No recorded findings in this category. This does not establish that the category is secure.

A07:2025 - Authentication Failures

OWASP description - official excerpt

When an attacker is able to trick a system into recognizing an invalid or incorrect user as legitimate, this vulnerability is present.

Description summary

Identity assurance depends on the complete authentication lifecycle. Weak password and recovery rules, ineffective multifactor controls, insufficient protection against automated guessing and incorrectly managed sessions can allow an identity to be accepted or retained without adequate proof.

Assessment coverage

Partial

E-00: login and sign-out records only. Recovery and federated identity remain unassessed.

Findings in this category: 0. Detailed records follow on separate pages.

No recorded findings in this category. This does not establish that the category is secure.

A08:2025 - Software or Data Integrity Failures

OWASP description - official excerpt

Software and data integrity failures relate to code and infrastructure that does not protect against invalid or untrusted code or data ...

Description summary

The central problem is accepting an artifact or data object as trustworthy without establishing its integrity. Review verification of updates, plugins and pipeline artifacts, as well as trust boundaries around serialized input. Provenance and integrity checks must remain effective throughout consumption.

Official OWASP Top 10:2025 category description - OWASP, CC BY 3.0. Short excerpt; summary adapted for this report.

Assessment coverage

Not assessed

No signed-update or imported-data integrity evidence supplied.

Findings in this category: 0. Detailed records follow on separate pages.

No recorded findings in this category. This does not establish that the category is secure.

A09:2025 - Security Logging and Alerting Failures

OWASP description - official excerpt

Without logging and monitoring, attacks and breaches cannot be detected, ...

Description summary

Recording events is only part of the requirement. Useful telemetry must be protected, reviewed and connected to timely escalation and response. Missing security events, ineffective alert rules, excessive noise and incomplete response procedures can prevent defenders from recognizing or addressing an incident.

Assessment coverage

Partial
E-00: event schema only. No alert delivery or response exercise demonstrated.
Findings in this category: 0. Detailed records follow on separate pages.
No recorded findings in this category. This does not establish that the category is secure.

A10:2025 - Mishandling of Exceptional Conditions

OWASP description - official excerpt

Mishandling exceptional conditions in software happens when programs fail to prevent, detect, and respond to unusual and unpredictable situations, ...

Description summary

Unexpected input, unavailable dependencies and resource or state errors require explicit handling. Inconsistent recovery, missed exceptions or unsafe failure paths can leave business operations and security controls in an unintended state. Evaluate prevention, detection and recovery together, including the integrity of partially completed operations.

Assessment coverage

Gap observed
F-4 / E-04: export-job cleanup on dependency error. Other failure paths remain open.
Findings in this category: 1. Detailed records follow on separate pages.

10.1. Export-job errors leave inconsistent completion state

F-4 / A10:2025

BASE SCORE							5.4
Attack vector	Complexity	Privileges	User interaction	Scope	Confidentiality	Integrity	Availability
Network	Low	Low	None	Unchanged	None	Low	Low

10.1.1. Description

The exception-path review shows a document-export job recording completion metadata before the dependent artifact store acknowledges persistence. The supplied failure-path unit-test record lacks rollback or terminal-failure assertions when that dependency returns an error.

Technical analysis

A workflow that spans metadata and artifact storage needs a defined failure state. Success must reflect the completed business operation, not an intermediate step. Consistent cleanup and idempotent recovery prevent later readers from treating an incomplete result as a valid export.

Scope and limits

The finding concerns a review of one exceptional path. No storage outage, resource exhaustion or fault injection was performed. The evidence does not establish authorization bypass, real document corruption or a production incident.

10.1.2. Impact

Users may encounter exports marked complete while the associated artifact is unavailable. Operators may have to reconcile metadata and job state manually, delaying delivery and reducing trust in status indicators. Integrity of workflow state and service reliability are the supported concerns. The sample does not show loss of the original document or access to another tenant's data.

10.1.3. Remediation

1. Define pending, completed and failed states with a clear success boundary. Publish completion only after required persistence succeeds.
2. Implement compensating cleanup or another consistency mechanism for partial work. Make retry behavior idempotent and bound attempts to avoid repeated incomplete records.
3. Add isolated failure-path tests using a mocked dependency. Record terminal state and an opaque correlation identifier while keeping operator diagnostics restricted.

Owner: Ines Martin, backend lead. Planned correction: 16 October 2026.

F-4 / Supporting evidence

evidence

E-04: export workflow review, 5 September 2026. Completion precedes artifact acknowledgement and failure assertions are absent from the supplied unit-test record.

Acceptance criterion

Mocked dependency failures produce the approved failed or pending state, with no false completion. A subsequent permitted retry produces one consistent result and preserves tenant ownership.

Retest pending. The statements above describe required closure evidence and do not assert a successful retest.

E-04 / WEB APP

Reviewed item	Scope	Recorded state
Export workflow	Completion event	Before persistence acknowledgement
Failure tests	Dependency error	Rollback assertion absent

Evidence register / Review window: 01-05 September 2026

E-04 - Reviewed record extract, September 2026.

CVSS v3.1: 5.4 (Medium)
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L

The vector rates the affected component and prerequisites described in this finding. Business priority additionally considers exposure, data sensitivity and delivery dependencies.

Export completion boundary

```
await store.persist(exportArtifact);
await jobs.markCompleted(jobId);
// On failure: record Failed, retain correlation ID, schedule bounded
retry.
```

10.1.4. References

A10:2025 - Mishandling of Exceptional Conditions. Mapping rationale: the reviewed root cause matches this category. Other risks require separate evidence.

OWASP Top 10:2025

Engagement baseline WEB-DEMO-2026-09, evidence E-04.

FIRST CVSS v3.1 scoring specification

Remediation and retest

1. F-1: Maya Laurent, application lead. Target 30 September 2026. Open. Closure evidence: Scoped repository query, policy review and passing isolated allow/deny tests.
2. F-2: Maya Laurent, application lead. Target 30 September 2026. Open. Closure evidence: Reviewed binding implementation and isolated repository regression results.
3. F-3: Noah Vidal, frontend lead. Target 16 October 2026. Open. Closure evidence: Sanitizer policy, component regression results and legacy-content review.
4. F-4: Ines Martin, backend lead. Target 16 October 2026. Open. Closure evidence: State-transition review and isolated failure/retry regression results.

Retest status

Proposed retest: 19-20 October 2026 on a corrected staging release. Review the four finding-specific acceptance criteria and document residual exceptions. No correction, risk acceptance or successful retest is asserted at issue.

Rating and limitations

Technical findings use CVSS v3.1 base scores with complete vectors. The score describes the affected component and stated prerequisites, rather than remediation priority. Business urgency also considers tenant separation and data sensitivity. CVSS is owned by FIRST and used by permission.

Conclusions apply to the assessed release and scope. Preserve evidence provenance and reassess risk after material changes. OWASP category names are attributed to the OWASP Top 10 project, CC BY 3.0.
OWASP Top 10:2025