Sorami

WEB APPLICATION & API

Penetration test report

Client: [REDACTED]

Project: [REDACTED] supplier portal

DOCUMENT	REVIEW EDITION
SOR-SAMPLE-WEB-2026-01	1.0 | Review edition
16 September 2026	Owner approval pending

SAMPLE / NOT A CUSTOMER REPORT

This is a synthetic sample in a redacted-report format. No testing was performed. All findings, HTTP exchanges, roles and engagement dates are illustrative. No real customer identity or evidence has been redacted.

Prepared by Sorami Consulting Pty Ltd

Document control & contents

This is a synthetic sample in a redacted-report format. No testing was performed. No customer, system, evidence collection, engagement approval or retest is represented as real. Client: [REDACTED] is a presentation convention, not the redaction of an actual client.

Document control	Review edition
Reference / version	SOR-SAMPLE-WEB-2026-01 / 1.0
Issued	16 September 2026
Prepared by	Sorami Consulting Pty Ltd | Security assessment practice
Review state	Owner technical and publication approval pending
Classification	SAMPLE | Review copy. Not a customer-confidential record.
Distribution	Sorami review audience only until publication is approved
Change record	1.0: complete research-led replacement sample, for review only

Handling: retain this disclosure when sharing excerpts. This PDF is not encrypted because it contains only synthetic material; it is not evidence that real reports are distributed without agreed protections. A live engagement would define access, encrypted delivery, retention and secure deletion in its rules of engagement.

Contents

01 / Executive assessment

Tenant and role boundaries are the principal concern in this fictional supplier-workflow platform. Release should be gated on correcting the two high-severity authorisation paths and independently verifying the fixes.

Critical	High	Medium	Low	Total
0	2	2	0	4

Business objective and scenario

The illustrative engagement asks whether an ordinary supplier user can access another tenant's purchase orders or invoke administrator-only actions. The model is a pre-production web portal and REST API supporting purchase-order review and internal case notes. It contains no payment execution or banking integration.

What the evidence illustrates

SOR-01 shows a member in Tenant A reading a known purchase order in Tenant B and changing its approval state. This undermines procurement approval integrity, but does not demonstrate payment fraud. SOR-02 shows a member promoting its own account to a tenant administrator through a profile update and then accessing an administrator-only export. These paths are independent; neither requires the other finding.

SOR-03 illustrates script execution when another user opens a stored case note. The marker demonstrates browser-origin execution, not account takeover or data theft. SOR-04 illustrates a preview worker retrieving one restricted diagnostic marker through an arbitrary URL. It does not demonstrate cloud-credential access or lateral movement.

Prioritisation and management decision

Address SOR-02 first because it expands a member's privileges within its tenant, then SOR-01 because it crosses tenant data boundaries. Both are release blockers in this sample risk treatment. Contain the affected write paths while fixes are developed. Address the two medium findings in the next controlled release rather than treating their lower scores as permission to defer indefinitely.

Systemic interpretation, not a proven root cause

The two authorisation examples suggest policy enforcement at individual route handlers rather than a shared, deny-by-default boundary. Confirm that hypothesis through code review. A common object-and-action policy, server-owned role fields and negative authorisation tests would prevent related defects across routes. A patch to the UI alone would not address these API paths.

These are scenario conclusions, not a security opinion about any real organisation. The report makes no whole-estate risk score, compliance attestation or claim that unlisted controls passed. Counts represent four authored finding scenarios, not four discoveries from a performed assessment.

02 / Scope & rules of engagement

Client: [REDACTED]. Project: [REDACTED] supplier portal. The following engagement envelope is entirely illustrative and does not authorise activity against any host. All .test names are reserved under RFC 2606; all IPv4 examples are documentation addresses under RFC 5737.

Boundary	Illustrative definition
Application	https://portal.client.test | browser UI; build sample-2026.09.1
API	https://api.client.test | REST /v1; same application security authority
Worker fixture	preview-worker; HTTP callback collector at https://collector.test; isolated diagnostic fixture at http://192.0.2.40:8080/diagnostics
Environment	Dedicated fictional staging environment with two seeded tenants. No production parity is asserted.
Test window	7 to 11 September 2026, 09:00 to 17:00 AEST (UTC+10), illustrative only
Approach	Authenticated grey-box web/API assessment model; endpoint inventory and role matrix supplied; no source review
Source address	198.51.100.25, documentation-only assessor address

Allowed functionality and roles

Scope is limited to login/session establishment, purchase-order read and approval-state update, user-profile update, tenant export, case-note submission/display and URL preview. MEMBER_A and ADMIN_A belong to TENANT_A; MEMBER_B and ADMIN_B belong to TENANT_B. Role names are fixtures, not personal identifiers. Anonymous requests are used only as negative controls.

Explicit exclusions

No corporate network, cloud control plane, infrastructure penetration test, production traffic, third-party identity provider, email delivery, payment processor, mobile client, social engineering, denial of service, load testing, persistence or bulk record extraction. Worker testing is limited to the collector and one diagnostic fixture. No metadata endpoint, internal subnet enumeration or secret retrieval is modelled.

Safety and escalation model

For a real engagement, the client sponsor would approve scope and stop conditions; the client technical contact would own test accounts and restoration; a Sorami test lead would control execution; a separate Sorami reviewer would challenge evidence and severity. These are illustrative role assignments, not named personnel or sign-offs.

The sample rules permit one-record, reversible state changes and harmless execution markers only. An unexpected real record, instability, out-of-scope redirect or actual secret would require immediate stop and escalation to the agreed contact channel. No contact channel, authorisation signature or escalation event is fabricated here.

03 / Methodology & limitations

Evidence is the basis for each conclusion. Guidance informs the structure; it does not turn this sample into a performed test or a certification.

Stage	Illustrative workflow
Plan	Confirm target inventory, role matrix, test data, stop conditions and evidence handling before access.
Map	Enumerate only the supplied routes and browser workflows; identify state transitions and trust boundaries.
Hypothesise	Compare expected permissions against object, field and action-level enforcement; examine untrusted content and server-side fetches.
Validate	Replay a legitimate baseline, change one security-relevant input, compare response and authoritative state, then restore the fixture.
Report	Separate evidence from inference; map identifiers and severity; give engineering fixes and explicit closure criteria.
Retest	Repeat original and bypass cases on an identified build, with positive controls and retained evidence. Not performed in this sample.

Technique and tooling assumptions

The model uses a browser with developer tools, an intercepting HTTP proxy and a command-line HTTP client. Community tooling is sufficient for these examples; no paid scanner, subscription or proprietary service is assumed. No tool was run against an application, so tool versions, scanner logs and activity timestamps are not invented.

Reference framework

PTES Reporting informs the executive/technical split and strategic remediation. OWASP WSTG v4.2 informs web-test references and reproducibility. NIST SP 800-115 (September 2008), sections 7.4 and 8, informs data handling, reporting and corrective actions. CREST's December 2022 guide informs practical reporting and follow-up. These are guidance sources, not assertions of mandatory regulatory conformity.

Limits on interpretation

The engagement is fictional. The HTTP exchanges are authored fixtures, not packet captures or lab execution results. Reproduction steps describe how an equivalent deliberately vulnerable fixture would behave; no runnable vulnerable application is included. The selected routes do not represent full WSTG coverage. The absence of a finding never means that a control was tested successfully.

No source code, infrastructure configuration, real logs or real threat model supports these scenarios. Causal statements about implementation are hypotheses unless implied directly by an input/output example. Retest results remain Not performed. Production applicability, attack frequency, monetary loss and regulatory consequences cannot be established from this sample.

In a commissioned assessment, results would be a time-bounded view of the agreed environment and access, with actual constraints and coverage recorded. This review edition is neither a warranty nor a substitute for that assessment.

04 / Coverage & authorisation model

Coverage below describes what is illustrated in the report, not work completed. No row constitutes a pass. WSTG identifiers use version 4.2. The endpoint inventory is deliberately precise so another assessor can identify both covered paths and gaps.

Family / reference	Modelled route and check	Evidence / coverage limit
Object authorisation WSTG-ATHZ-04	GET /v1/purchase-orders/{id} PATCH /v1/purchase-orders/{id} Tenant A actor, Tenant B object	SOR-01. One known foreign order; no enumeration claim.
Privilege escalation WSTG-ATHZ-03	PATCH /v1/users/me POST /v1/admin/exports Member versus administrator	SOR-02. Own-tenant role transition; no global administrator access.
Stored script injection WSTG-INPV-02	POST /v1/cases/{id}/notes GET /cases/{id} Member input, administrator viewer	SOR-03. One HTML body sink; no other rendering contexts covered.
Server-side request forgery WSTG-INPV-19	POST /v1/previews GET /v1/previews/{id} Fetch target restriction	SOR-04. One diagnostic destination; no network scan.
Authentication / session	Login creates fixture sessions; missing-session controls on order/export routes	Context only. Password reset, MFA, revocation, fixation and brute-force resistance not assessed.
Other input / configuration	SQL injection, file upload, TLS, CORS, cache isolation, CSRF and dependency review	Not assessed. No blanket OWASP Top 10 or WSTG coverage claim.

Expected access policy

Actor	Intended permission
Anonymous	No access to orders, notes, preview jobs or exports.
Member, own tenant	Read own-tenant orders; edit own display name; add case notes; request bounded previews. Cannot approve orders or assign roles.
Administrator, own tenant	Approve own-tenant orders and create own-tenant exports; view case notes. Cannot access another tenant.
Any authenticated actor	Server derives tenant and role from trusted identity state. URL identifiers and JSON fields do not confer authority.

Fixture identifiers remain readable for reproduction: TENANT_A / TENANT_B, PO-B-204, CASE-A-12 and U-A-17. These synthetic identifiers replace the need for personal data. [REDACTED] is used for client identity; fixture identifiers are intentionally not concealed.

05 / Findings register & severity

ID / finding	Severity / score	Priority / status
SOR-01 Cross-tenant purchase-order access and approval	High CVSS 3.1: 7.1	P1 | Before release Open (synthetic) Retest: Not performed
SOR-02 Self-assigned administrator role through profile update	High CVSS 3.1: 8.1	P1 | Address first Open (synthetic) Retest: Not performed
SOR-03 Stored script execution in case-note rendering	Medium CVSS 3.1: 5.4	P2 | Next controlled release Open (synthetic) Retest: Not performed
SOR-04 Unrestricted preview fetch exposes a diagnostic response	Medium CVSS 3.1: 4.3	P2 | Next controlled release Open (synthetic) Retest: Not performed

SOR-01: detailed evidence and remediation, page 8

SOR-02: detailed evidence and remediation, page 10

SOR-03: detailed evidence and remediation, page 12

SOR-04: detailed evidence and remediation, page 14

Severity is not the same as delivery priority

CVSS v3.1 Base scores describe technical severity under the stated scenario assumptions. No Temporal or Environmental score is assigned. Version 3.1 is used consistently for this sample and is not described as the latest version of CVSS. Business priority reflects the modelled approval workflow and privilege boundaries, not a numerical organisational risk calculation.

Band	Base score	Interpretation in this report
Critical	9.0 to 10.0	Highest technical severity; no finding in this sample.
High	7.0 to 8.9	Prioritised before release in this fictional risk treatment.
Medium	4.0 to 6.9	Controlled remediation in the next planned release.
Low	0.1 to 3.9	No finding in this sample.
None	0.0	No scored security impact; not used as a pass label.

Scoring discipline

Each vector is checked with the Python cvss implementation and independently with the FIRST v3.1 Base equations in the test suite. Scope is Unchanged for both authorisation findings: crossing tenants or gaining a role within one application does not automatically mean a CVSS security-authority change. SOR-03 uses Changed because the server-side defect affects the victim browser's execution context.

All findings are Open in the fictional scenario only. No remediation or retest has occurred. Each finding separates evidence from impact, then gives concrete remediation and acceptance criteria.

SOR-01 / Cross-tenant purchase-order access and approval

HIGH / CVSS 3.1 7.1 | P1 | Before release

api.client.test | GET and PATCH /v1/purchase-orders/{id}

Prerequisites

A valid MEMBER_A session in TENANT_A and the known fixture identifier PO-B-204 in TENANT_B. The identifier is supplied by the test fixture; guessing or enumerating unknown identifiers is not demonstrated.

Expected / observed

MEMBER_A cannot read or modify a TENANT_B order. The API should return a non-disclosing 404 for a foreign object, and the order state must remain unchanged. Only ADMIN_B may approve this order.

The synthetic sequence returns the foreign order to MEMBER_A and accepts an approval-state update. A separate ADMIN_B read-back returns approved. The failure is object and action authorisation, not simply a predictable identifier.

Reproduction in the fictional fixture

01. Seed PO-B-204 in TENANT_B with status pending. Obtain independent MEMBER_A and ADMIN_B sessions; verify each tenant using the fixture account mapping.

02. Using ADMIN_B, confirm the order is pending. With no session, confirm the order route returns 401 in the fixture baseline.

03. Using MEMBER_A, issue E01-A for the known foreign order. Compare the tenant_id in the response with TENANT_A.

04. Issue E01-B using MEMBER_A, then read the same order as ADMIN_B. The changed status is the persistence check. Reset to pending after the scenario.

E01-A | Foreign-object read | Synthetic evidence

```
GET /v1/purchase-orders/PO-B-204 HTTP/1.1
Host: api.client.test
Cookie: sid=SAMPLE_MEMBER_A

HTTP/1.1 200 OK
Content-Type: application/json

{"id":"PO-B-204","tenant_id":"TENANT_B",
 "status":"pending","total_aud":1250.00}
```

E01-B | State change and independent read-back | Synthetic evidence

```
PATCH /v1/purchase-orders/PO-B-204 HTTP/1.1
Host: api.client.test
Cookie: sid=SAMPLE_MEMBER_A
Content-Type: application/json

{"status":"approved"}

HTTP/1.1 200 OK
{"id":"PO-B-204","status":"approved"}

GET /v1/purchase-orders/PO-B-204 HTTP/1.1
Host: api.client.test
Cookie: sid=SAMPLE_ADMIN_B

HTTP/1.1 200 OK
{"id":"PO-B-204","status":"approved"}
```

SOR-01 / Remediation & verification

HIGH / CVSS 3.1 7.1 | P1 | Before release

Scenario state: Open (synthetic) | **Retest:** Not performed

Impact and evidence bounds

The illustrated read exposes one foreign order's value and state. The write bypasses a procurement approval boundary and can cause an order to be treated as approved without its tenant administrator's decision. Integrity is High because unauthorised approval is a direct, serious consequence for the core workflow even though the evidence involves one record.

No invoice payment, bank change, production customer disclosure, bulk export or unknown-identifier discovery is shown. Confidentiality is Low because only the bounded order response is demonstrated. Cross-tenant access alone does not justify Scope Changed. Broader route exposure requires investigation, not an assertion that every object is vulnerable.

CVSS v3.1 Base rationale

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N

AV:N: remotely reachable API. AC:L: a known identifier and ordinary request replay suffice. PR:L: member session required. UI:N: no other actor participates in the exploit. S:U: both tenants are enforced by the same application authority. C:L: limited order data. I:H: direct serious approval-integrity failure. A:N: no service interruption illustrated.

Remediation

01. Resolve the object through a trusted tenant-scoped repository, using the authenticated tenant identity. Do not load globally and rely on a UI tenant filter or a caller-provided tenant_id.

02. Evaluate subject, action and object together. Require an administrator role for approval transitions, even for an order in the caller's own tenant. Apply checks before serialisation or mutation.

03. Make approval-state transitions transactional and auditable. Reject unexpected state or fields; include a version precondition to prevent lost updates. Audit actor, tenant, order and transition without copying session tokens.

04. Inventory every order read, update, export and nested resource route for the same policy gap. Opaque identifiers are defence in depth only, not an authorisation fix.

Regression and retest acceptance

01. MEMBER_A GET and PATCH against PO-B-204 return the documented 404 policy and do not disclose tenant or order fields; ADMIN_B read-back remains pending.

02. An own-tenant member can read a permitted order but cannot approve it. An own-tenant administrator can approve an eligible pending order.

03. Repeat with both tenant directions, fresh sessions, unknown IDs, changed tenant_id fields and every supported update method. Denials produce no database side effects.

04. Run the same policy checks on exports and nested resources. Retain the build identifier, actor matrix, responses and authorised read-back as closure evidence.

CWE-639

WSTG-v42-ATHZ-04 | Insecure Direct Object References

SOR-02 / Self-assigned administrator role through profile update

HIGH / CVSS 3.1 8.1 | P1 | Address first

api.client.test | PATCH /v1/users/me and POST /v1/admin/exports

Prerequisites

A valid MEMBER_A session for U-A-17 in TENANT_A. The fixture API obtains current role from server-side account state on each request. The allowed profile contract contains display_name only; role is administrator-managed.

Expected / observed

The self-service profile route must reject protected attributes. MEMBER_A should remain a member and receive 403 from the tenant export action. An authorised ADMIN_A session can create the own-tenant export.

Adding role=admin to a profile update changes server-owned identity state. Reusing the member session then permits an export that was previously denied. The export body contains both seeded confidential procurement records in TENANT_A.

Reproduction in the fictional fixture

01. Reset U-A-17 to member. Seed exactly two TENANT_A procurement records. Confirm ADMIN_A can export these fixtures.

02. Send POST /v1/admin/exports with MEMBER_A; the fixture baseline returns 403 role_required. This distinguishes pre-existing access from a privilege gain.

03. Send E02-A with the protected role attribute and inspect the returned account role.

04. Repeat the previously denied export and retrieve it in E02-B. Confirm it contains both seeded records; restore the role and revoke the session.

E02-A | Protected-field mutation | Synthetic evidence

```
PATCH /v1/users/me HTTP/1.1
Host: api.client.test
Cookie: sid=SAMPLE_MEMBER_A
Content-Type: application/json

{"display_name":"Fixture member","role":"admin"}

HTTP/1.1 200 OK
{"id":"U-A-17","tenant_id":"TENANT_A","role":"admin"}
```

E02-B | Newly available privileged operation | Synthetic evidence

```
POST /v1/admin/exports HTTP/1.1
Host: api.client.test
Cookie: sid=SAMPLE_MEMBER_A
Content-Type: application/json

{"dataset":"procurement"}

HTTP/1.1 201 Created
{"id":"EXP-A-01","download":"/v1/admin/exports/EXP-A-01"}

GET /v1/admin/exports/EXP-A-01 HTTP/1.1
Host: api.client.test
Cookie: sid=SAMPLE_MEMBER_A

HTTP/1.1 200 OK
{"tenant_id":"TENANT_A","records":[
 {"id":"R-A-01","internal_limit_aud":5000},
 {"id":"R-A-02","internal_limit_aud":8000}]}
```

SOR-02 / Remediation & verification

HIGH / CVSS 3.1 8.1 | P1 | Address first

Scenario state: Open (synthetic) | **Retest:** Not performed

Impact and evidence bounds

The privilege gain defeats the application's administrator boundary within TENANT_A. The newly accessible export exposes the complete confidential procurement dataset of the defined two-record fixture, supporting C:H in this deliberately bounded component model. Persistently assigning administrator authority is a direct, serious integrity loss, supporting I:H.

This does not establish global administration, cross-tenant access, identity-provider compromise or operating-system privileges. The complete-dataset confidentiality assumption is explicit and must be revisited for a real application with narrower exports. No availability action is attempted or inferred. SOR-01 is a separate tenant-isolation defect, not a prerequisite.

CVSS v3.1 Base rationale

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

AV:N / AC:L: a remote authenticated request with one additional field. PR:L: a member account suffices. UI:N: no approval or victim interaction. S:U: the same application governs profile and tenant permissions. C:H: all confidential records in the scoped tenant fixture are exported. I:H: server-owned administrator authority is changed. A:N: no interruption shown.

Remediation

01. Use a purpose-specific profile input object that explicitly permits display_name only. Reject protected or unknown keys rather than binding arbitrary JSON onto the persisted identity object.

02. Move role changes to a dedicated administrative action with explicit actor/target authorisation, tenant matching and audit logging. Determine tenant and existing role from trusted server state.

03. Review equivalent update, invite, import and bulk routes for protected attributes such as role, tenant_id, permissions and account_state. Protect nested objects and alternate field representations as well.

04. Review existing role transitions for unexpected changes and invalidate affected sessions after correction. Ensure permission caches and token refresh paths cannot preserve an unauthorised role.

Regression and retest acceptance

01. A member update containing role, tenant_id or permissions is rejected under the defined API contract, and an authoritative account read confirms no protected change.

02. A valid display_name-only update still succeeds. The original member session remains denied on export creation and download, including after token refresh or reauthentication.

03. Test nested attribute forms, alternate casing supported by the API, bulk/import routes and both tenants. No caller-controlled path may change protected identity attributes.

04. An authorised own-tenant administrator can make permitted role changes through the dedicated route; foreign-tenant and self-escalation cases fail. Record account state, audit entry and export denial.

CWE-915

WSTG-v42-ATHZ-03 | Privilege Escalation

SOR-03 / Stored script execution in case-note rendering

MEDIUM / CVSS 3.1 5.4 | P2 | Next controlled release

portal.client.test | case-note HTML body sink; API POST /v1/cases/{id}/notes

Prerequisites

MEMBER_A can add notes to CASE-A-12, later viewed by ADMIN_A. The fixture inserts note text into HTML without encoding; no browser policy blocks inline handlers. Only a harmless DOM marker is used.

Expected / observed

The member's note should render as inert text (or sanitised allowed rich text). Its content must not execute JavaScript in another user's portal session. The HTML renderer is the boundary; accepting text in JSON is not by itself the vulnerability.

The response inserts active HTML. An invalid data-image triggers onerror in the administrator's browser and sets a document marker, demonstrating execution but not cookie theft.

Reproduction in the fictional fixture

01. Reset CASE-A-12 and confirm MEMBER_A may add a note. Record a plain-text baseline displayed to ADMIN_A.

02. Submit E03-A as MEMBER_A, preserving the complete note text. The invalid data-image requires no callback host or network exfiltration.

03. Open /cases/CASE-A-12 using a separate ADMIN_A browser session. E03-B shows the relevant HTML response fragment.

04. Inspect document.title in the administrator's developer console. The fixture observation is SOR-03. Remove NOTE-A-09 and reload.

E03-A | Stored input | Synthetic evidence

```
POST /v1/cases/CASE-A-12/notes HTTP/1.1
Host: api.client.test
Cookie: sid=SAMPLE_MEMBER_A
Content-Type: application/json

{"text":"<img src='data:,' onerror=\"document.title='SOR-03'\">"}

HTTP/1.1 201 Created
{"id":"NOTE-A-09","case_id":"CASE-A-12"}
```

E03-B | Rendered sink and execution marker | Synthetic evidence

```
GET /cases/CASE-A-12 HTTP/1.1
Host: portal.client.test
Cookie: sid=SAMPLE_ADMIN_A

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8

<div class="case-note"><img src='data:,'
 onerror="document.title='SOR-03'">
</div>

Developer console observation (synthetic):
document.title
=> "SOR-03"
```

SOR-03 / Remediation & verification

MEDIUM / CVSS 3.1 5.4 | P2 | Next controlled release

Scenario state: Open (synthetic) | **Retest:** Not performed

Impact and evidence bounds

Untrusted member content executes within another user's portal origin. This permits limited reading and alteration of the case page available to that viewer, reflected by C:L and I:L. The marker demonstrates control over the document, while the ability to read same-origin page content follows from that execution context.

No privileged API request, external transfer, session-token extraction, account takeover or persistent access is shown. HttpOnly cookies would not prevent script execution or page manipulation, but their theft is not claimed. The score is not inflated to High based solely on an administrator being the viewer. Other HTML, attribute, URL and script contexts remain unassessed.

CVSS v3.1 Base rationale

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

AV:N / AC:L: authenticated note submission with a stable rendering path. PR:L: note-author permission required. UI:R: another user must open the case. S:C: vulnerable server rendering affects the victim browser security context. C:L / I:L: limited in-origin page access and modification; marker-only demonstration. A:N: no availability effect.

Remediation

01. Render plain-text notes through the framework's escaped text binding or textContent. Remove innerHTML or equivalent unsafe HTML insertion for this field.

02. If rich text is required, sanitise using a maintained allowlist-based HTML sanitiser with explicit permitted elements and attributes. Remove event handlers and unsafe URL schemes; do not attempt a hand-written blacklist.

03. Apply the same policy to existing stored notes, previews and exports that render HTML. Fix the output context as well as validation at input; stored data may pre-date new validation.

04. Deploy a restrictive Content Security Policy without unsafe-inline where practicable, with nonce/hash-based scripts and Trusted Types where supported. Treat this as an additional control, not a substitute for safe rendering.

Regression and retest acceptance

01. Replay the exact stored payload: it appears as text or safe sanitised markup, no event handler remains and the SOR-03 title marker is absent.

02. Test pre-existing stored notes and alternate case views, previews and HTML exports. They must use the same safe rendering policy.

03. Exercise allowed formatting plus encoded tags, event-handler variants and dangerous URLs. The DOM must remain inert without breaking permitted notes.

04. Repeat with member and administrator viewers. Retain the raw response, final DOM and browser-policy observation; a filter error or blank case page alone is not closure.

CWE-79

WSTG-v42-INPV-02 | Stored Cross Site Scripting

SOR-04 / Unrestricted preview fetch exposes a diagnostic response

MEDIUM / CVSS 3.1 4.3 | P2 | Next controlled release

api.client.test | POST /v1/previews; preview-worker outbound HTTP client

Prerequisites

MEMBER_A can create/read its own previews. An isolated fictional network routes documentation address 192.0.2.40 to an application diagnostic fixture reachable only by the worker. This address is not an actual target.

Expected / observed

Only approved sources may be fetched. The diagnostic fixture is not approved: reject its URL or refuse the worker connection without returning the body.

The collector correlates the first worker job. A second job returns the restricted diagnostic marker to the member. Both services exist solely for this application and share its CVSS security scope.

Reproduction in the fictional fixture

01. Configure the diagnostic fixture as worker-only, serving a non-secret marker. Confirm direct assessor access is denied.

02. Create the collector preview as MEMBER_A. Correlate E04-A's path and job header.

03. Submit E04-B with the diagnostic URL. Retrieve PRE-A-02 using the same member session after the job completes.

04. Compare the returned marker. Stop at this single destination; remove the jobs and collector records after an executable test.

E04-A | Worker correlation at approved collector | Synthetic evidence

```
POST /v1/previews HTTP/1.1
Host: api.client.test
Cookie: sid=SAMPLE_MEMBER_A
Content-Type: application/json

{"url":"https://collector.test/SOR-04"}

HTTP/1.1 202 Accepted
{"id":"PRE-A-01"}

GET /SOR-04 HTTP/1.1
Host: collector.test
X-Preview-Job: PRE-A-01
```

E04-B | Restricted body returned to member | Synthetic evidence

```
POST /v1/previews HTTP/1.1
Host: api.client.test
Cookie: sid=SAMPLE_MEMBER_A
Content-Type: application/json

{"url":"http://192.0.2.40:8080/diagnostics"}

HTTP/1.1 202 Accepted
{"id":"PRE-A-02"}
GET /v1/previews/PRE-A-02 HTTP/1.1
Host: api.client.test
Cookie: sid=SAMPLE_MEMBER_A

HTTP/1.1 200 OK
{"id":"PRE-A-02","status":"complete",
 "text":"SAMPLE_DIAGNOSTIC_MARKER build=sample-2026.09.1"}
```

SOR-04 / Remediation & verification

MEDIUM / CVSS 3.1 4.3 | P2 | Next controlled release

Scenario state: Open (synthetic) | **Retest:** Not performed

Impact and evidence bounds

A low-privilege member can cause the worker to cross its intended destination boundary and disclose a restricted diagnostic response. The demonstrated disclosure is a non-secret operational marker and build label, so confidentiality is Low. A callback alone would prove outbound fetching, not this body disclosure; E04-B provides the additional evidence.

No credentials, cloud metadata, arbitrary internal network reachability, write action or service disruption is demonstrated. Redirect following and DNS rebinding are not established by this evidence; they are regression cases for the fix. A future discovery of separate-security-authority or secret-bearing targets would require new evidence and rescoring, not retrospective inflation.

CVSS v3.1 Base rationale

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

AV:N / AC:L: member-accessible API accepts a direct URL with no race. PR:L: authenticated preview permission. UI:N: no victim action. S:U: worker and diagnostic fixture serve the same application authority. C:L: restricted diagnostic marker only. I:N / A:N: no state change or interruption demonstrated.

Remediation

01. Prefer accepting an application-managed content identifier rather than an arbitrary URL. If external previews are essential, define explicit approved HTTPS hosts and ports and reject other schemes, credentials and ambiguous URL forms.

02. Parse and canonicalise once, then validate every resolved address against destination policy. Restrict worker egress to approved destinations at the network layer; deny diagnostic and management services irrespective of URL spelling.

03. Disable redirects or reapply scheme, host, port and resolved-address checks at every hop. Avoid validation/connect resolution gaps by connecting to a validated address while preserving correct TLS hostname verification.

04. Bound response size, connection/read timeouts and concurrency. Do not forward application cookies or authorisation headers, and do not expose raw diagnostic/error bodies to callers. Keep ownership checks on preview job retrieval.

Regression and retest acceptance

01. The original diagnostic URL fails with a generic policy error; no worker connection reaches the fixture and no marker is included in job output.

02. Approved HTTPS previews still complete and retain correct TLS verification. A legitimate job remains readable only by its authorised tenant/owner.

03. Test loopback, private/link-local and documentation fixtures in an isolated lab, IPv6 forms, non-HTTP schemes, embedded credentials, alternate ports and ambiguous encodings against the policy.

04. Test an approved host redirecting to a denied destination and controlled DNS address changes. Verify every hop/connection is denied as appropriate; retain worker egress observations as well as API responses.

CWE-918

WSTG-v42-INPV-19 | Server-Side Request Forgery

06 / Remediation programme

Treat the two authorisation failures as a shared control-design problem, while retaining separate fixes and closure evidence for each route.

The milestones below are proposed relative targets for the fictional engagement, not contractual service levels or promises. A real client would approve the dates, owners, compensating controls and residual risk after considering operational constraints.

Milestone	Accountable role	Action and completion evidence
Contain Before release	Application owner	SOR-02: reject role updates through /users/me. SOR-01: suspend member approval-state writes and enforce tenant scoping. Record configuration change and rollback route; containment alone is not closure.
Correct Within 7 calendar days of acceptance	API engineering lead	Deploy shared subject/object/action checks and explicit profile-field allowlists. Provide build identifier and automated negative/positive tests for SOR-01 and SOR-02.
Harden Within 30 calendar days of acceptance	Web and platform leads	SOR-03: remove unsafe HTML sink and add sanitiser regression cases. SOR-04: constrain fetching and network egress. Provide build/configuration evidence and failure-path tests.
Verify Before closure	Independent security reviewer	Replay original requests and alternative roles/routes; record response and authoritative state. Mark each finding with evidence-linked retest status, not ticket completion alone.
Prevent recurrence Next development cycle	Engineering manager	Adopt an owned role/action matrix, policy library and security regression gate. Inventory equivalent APIs and browser sinks; fund wider assessment where coverage is missing.

Dependencies and sequencing

Define who may approve an order before implementing SOR-01. Define which identity service owns roles before implementing SOR-02. For SOR-03, product must decide whether plain text is sufficient or a constrained rich-text model is required. For SOR-04, agree the business-approved preview destinations before creating a fetch allowlist. A generic filter without these decisions is likely to break functionality or leave bypasses.

Detection and residual-risk handling

Record denied foreign-object attempts and privileged-field submissions without retaining tokens or sensitive response bodies. Alert on unexpected role transitions and blocked worker destinations. Detection is supplementary; logging a successful unauthorised action does not repair authorisation. Any deferral should name an accountable owner, expiry date and compensating control, then be reassessed at expiry.

No implementation effort, financial loss, risk acceptance or client commitment is invented in this plan. In particular, the sample evidence provides no basis for estimating exposure across a real production dataset.

07 / Retest procedure & status

> Retest status: Not performed for SOR-01, SOR-02, SOR-03 and SOR-04. No fix has been verified and no certificate, signature or attestation is issued.

Entry criteria

Obtain a new written authorisation and scope confirmation for the retest; record application build, relevant configuration version and deployment time. Request a change summary, developer regression results, two fresh tenants, member/administrator fixtures and a reset procedure. Verify that mitigations are present in the environment under test rather than only on a developer branch.

01. Recreate each original baseline and confirm the authorised workflow still succeeds. A broken endpoint is not proof of a complete security fix.

02. Replay the original exploit with fresh sessions and objects. Preserve the request, response, actor/tenant mapping and resulting authoritative state.

03. Exercise each finding's acceptance cases, including alternate methods, unknown identifiers, stale sessions, encoded input or alternate destinations as applicable.

04. Check equivalent routes and data paths identified by engineering. Track new defects separately instead of quietly broadening the original result.

05. Remove test notes and preview jobs, restore the seeded role/order state, revoke fixture sessions and confirm cleanup with the technical contact.

06. Issue an evidence-linked addendum showing retest date, build, reviewer role, observed status, remaining gaps and residual risk. Retain the original severity and findings history.

Allowed outcome	Meaning in a future commissioned retest
Resolved	Original path and agreed bypass cases no longer succeed; positive controls work; build and evidence retained.
Partially resolved	Some paths are blocked but a material bypass or acceptance gap remains.
Unresolved	The reported behaviour is still reproducible.
Not retested	Unavailable access, scope or environment prevented verification. This is not a pass.
Risk accepted	A documented client decision, not a technical resolution; requires owner and expiry. Not used in this sample.

For this edition, Not performed is the only applicable retest state. An actual retest would verify the defined fixes, not establish that the entire application or organisation is secure. New features and material architecture changes require additional scoping.

Appendix A / Evidence conventions

Synthetic evidence register

Evidence ID	Authored material and interpretation
E01-A / E01-B	Foreign order read, unauthorised approval-state write and administrator verification. Supports SOR-01 only.
E02-A / E02-B	Member export denial, protected role-field update and export retrieval after promotion. Supports SOR-02 only.
E03-A / E03-B	Stored note input and resulting HTML/DOM marker. Supports origin execution, not session theft.
E04-A / E04-B	Controlled collector request and worker-only diagnostic body returned through a preview job. Supports one bounded SSRF retrieval.

HTTP representation

Exchanges are normalised excerpts, not complete wire captures. Content-Length, Date, transport framing and unrelated headers are intentionally omitted. JSON response bodies may be formatted across lines for readability. Cookie values such as SAMPLE_MEMBER_A are inert fixture labels, not usable session tokens. No token is a concealed real secret.

An exchange arrow in prose means a response paired with the immediately preceding request. HTTP status alone is not used to infer a lasting change: SOR-01 includes an administrator read-back, SOR-02 includes a privileged export and SOR-03 includes the resulting DOM marker. Job IDs link submission and retrieval for SOR-04.

Fixture reset and evidence retention

A future executable lab would reset PO-B-204 to pending, U-A-17 to member, remove NOTE-A-09 and jobs PRE-A-01/PRE-A-02, and revoke its sessions between scenarios. No cleanup is claimed here because no application was run. Only this editable report and generated review PDF exist as report artefacts; there is no raw assessment evidence pack.

Redaction convention

Client: [REDACTED] and Project: [REDACTED] demonstrate how identity can be withheld while preserving technical traceability. Generic domains, accounts and order values are original synthetic content. No real customer evidence was redacted to create this document. Sorami's own corporate identity and branding are not redacted.

Abbreviations

API: application programming interface. CWE: Common Weakness Enumeration. CVSS: Common Vulnerability Scoring System. WSTG: Web Security Testing Guide. SSRF: server-side request forgery. XSS: cross-site scripting. AEST: Australian Eastern Standard Time (UTC+10).

Appendix B / References & basis

Primary guidance consulted on 16 September 2026. These documents guide structure and technical classification; none constitutes accreditation of Sorami or evidence that this fictional engagement met a regulatory scheme. The research/design note accompanying the editable source records professional report comparisons and design decisions.

PTES Reporting, unversioned online guidance

OWASP WSTG v4.2, Reporting (release source)

NIST SP 800-115, September 2008, sections 7.4 and 8

FIRST CVSS v3.1 Specification, sections 2, 5 and 7

CREST A Guide to Penetration Testing, December 2022

CWE-639: Authorisation Bypass Through User-Controlled Key

CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes

CWE-79: Improper Neutralization of Input During Web Page Generation

CWE-918: Server-Side Request Forgery (SSRF)

RFC 2606: Reserved Top Level DNS Names

RFC 5737: IPv4 Address Blocks Reserved for Documentation

Authority and version notes

OWASP explicitly describes its reporting chapter as suggestions, not strict rules. PTES is a community methodology; NIST SP 800-115 is technical guidance. CREST scheme-specific requirements apply only in the relevant scheme context; no CREST membership, qualification, CDPT symbol or compliance is claimed. CVSS is a technical severity specification, not a probability-of-loss model.

Versioned WSTG links in the findings point to the official v4.2 release source because several versioned website routes returned HTTP 404 during preparation. CWE names retain the terminology of their official entries. Reference links are for further reading and do not endorse any particular product or paid tool.