SpotDefence

OFFENSIVE SECURITY. CLEAR ANSWERS.

Application Penetration Test Report

A clear path from exposure to verified remediation.

PUBLIC SAMPLE EDITION

Example Workspace

Web application + REST API | Fictional SaaS environment

REPORT ID

SD-SAMPLE-001

EDITION

September 2026 / Version 1.0

All organisations, accounts, systems, findings and evidence in this report are fictional. This is a deliverable example, not a client assessment or security certification.

DOCUMENT GUIDE

Built for decisions. Ready for engineering.

A public illustration of the depth and structure of a SpotDefence deliverable.

DOCUMENT CONTROL	VALUE
Report / version	SD-SAMPLE-001 / 1.0
Classification	Public sample - fictional content throughout
Prepared by	SpotDefence
System	Example Workspace, a fictional procurement SaaS application
Assessment context	Illustrative authenticated web and API assessment; no real testing dates or customer approvals asserted.
Evidence provenance	Newly authored HTTP transcripts, browser illustrations and fixtures. No client captures, screenshots or attachments reused.

Choose your reading path

AUDIENCE	START HERE
Executives / risk owners	Executive summary (03), findings register (06), remediation plan (15)
Engineers / security teams	Scope and coverage (04-05), detailed findings (07-14), retest criteria (16)
Procurement / assurance	Document control (02), limitations and delivery model (17), references (18)

HOW TO READ THE EXAMPLES

The five findings and their statuses describe an invented scenario. Evidence demonstrates the reporting format only. Values such as SAMPLE_MEMBER_A are deliberately non-functional substitutes, not masked live credentials.

01 / EXECUTIVE SUMMARY

Fix the trust boundaries first.

Illustrative result: one High, two Medium, one Low and one Informational finding.

0	1	2	1	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

Example Workspace lets separate organisations manage invoices and collaborative work items. In this fictional assessment, the highest-impact weakness lets a standard member promote their own workspace privileges. A separate authorisation defect exposes invoices across workspace boundaries. Stored script execution introduces a browser-side risk when another member opens a crafted work item.

RECOMMENDED DECISION

Prioritise F-02 role escalation and F-01 cross-workspace access before expanding access to the application. Assign accountable owners, agree risk-based target dates and independently verify the fixes. Address F-03 in the same remediation cycle.

Business exposure and confidence

- **Workspace control:** F-02 permits access to financial records and modification of billing settings within the attacker's workspace. It does not demonstrate platform-wide administration.
- **Data separation:** F-01 exposes full invoice content in the fixture set. It does not demonstrate writes, code execution or database compromise.
- **Browser trust:** F-03 executes a harmless marker in another member's browser. Credential theft, persistence and external data transfer were not exercised.

The remaining observations concern local browser retention and diagnostic detail. These are reported separately from the three scored vulnerabilities. No overall security grade, compliance pass or guarantee of complete coverage is implied.

02 / ENGAGEMENT SCOPE

Know what was assessed.

A concrete scope and role model make an authorisation finding reproducible.

SURFACE	ILLUSTRATIVE SCOPE
Application	https://workspace.example.com - fictional staging environment
API	/api/v1/invoices, /api/v1/profile, /api/v1/work-items and workspace billing settings
Data	Synthetic invoices, work items and workspace records only
Access	Member A and administrator A in workspace A; member B and administrator B in workspace B
Environment definition	Invented browser UI, REST API, application service and relational data store; no real vendor versions or infrastructure identifiers

Authorisation baseline

ACTOR	ALLOWED	MUST BE DENIED
Member A	Own workspace work items; permitted invoice subset; own display name	Other workspace invoices; changing own role; billing administration
Administrator A	Workspace A billing and membership administration	Workspace B data or platform administration
Member B	Equivalent member access in workspace B	Workspace A resources
Unauthenticated	Public login and help routes	All scoped authenticated API resources

Explicit exclusions: production systems, third-party services, payment execution, social engineering, denial of service, source-code review, cloud control-plane review and AI features. This sample demonstrates an application assessment; it does not imply those excluded services were tested.

Pre-engagement requirements: written authorisation, confirmed asset ownership, test identities, permitted techniques, stop conditions, an escalation contact and agreed evidence handling.

03 / METHODOLOGY AND COVERAGE

Evidence at every phase.

Five phases, with timing and depth agreed during scoping.

PHASE	PURPOSE / OUTPUT
01 Reconnaissance	Map entry points, trust boundaries and roles. Output: asset and access inventory.
02 Assessment	Form and test hypotheses across authentication, authorisation, input handling and configuration. Output: test log.
03 Controlled exploitation	Use the smallest proof needed; record expected versus actual behaviour and negative controls. Output: reproducible evidence.
04 Reporting	Validate evidence, calculate severity, bound impact and propose practical fixes. Output: prioritised report.
05 Retest	Replay each proof against the changed build and test neighbouring cases. Output: per-finding closure decision.

Illustrative coverage ledger

AREA	EVIDENCE / COVERAGE BOUNDARY
Authentication and sessions	Unauthenticated rejection and post-logout API denial; browser caching assessed separately.
Authorisation and business logic	Two-workspace, two-role matrix; invoice reads, profile mutation and billing operations. F-01, F-02.
Input and output handling	Stored work-item title, rendering in a second account and harmless script marker. F-03.
Client-side storage / error handling	Offline revisit of a sensitive page and malformed invoice filter. F-04, F-05.
Other attack classes	SQL injection, SSRF, file uploads and dependency vulnerabilities are not demonstrated by this sample. No clean bill of health is inferred.

Reference framework: selected OWASP WSTG v4.2 scenarios [1]. Proxy-assisted request replay, browser developer tools and role comparison are suitable techniques for this scope. A tooling list alone does not establish coverage.

04 / RISK AND FINDINGS REGISTER

Five findings. One action queue.

Counts, identifiers and ratings remain consistent throughout this sample.

ID / PAGE	FINDING	RATING
F-01 / 07	Cross-workspace invoice disclosure	Medium / 6.5
F-02 / 09	Self-assigned workspace administrator role	High / 8.1
F-03 / 11	Stored script execution in work-item titles	Medium / 5.4
F-04 / 13	Sensitive invoice retained in browser cache	Low / contextual
F-05 / 14	Diagnostic implementation detail in API errors	Informational / contextual

Scoring policy

F-01 to F-03 use CVSS v3.1 Base scores [2], with complete vectors and assumptions recorded in each finding. This edition uses one scoring version consistently. Threat and environmental scores are not calculated; real engagements should consider the customer's deployment, exposure and business context separately.

CVSS bands: Critical 9.0-10.0; High 7.0-8.9; Medium 4.0-6.9; Low 0.1-3.9; None 0.0. The contextual Low and Informational labels on F-04 and F-05 are analyst judgements, not CVSS scores. Informational is not a CVSS severity band.

> **PRIORITY IS MORE THAN A NUMBER**
>
> F-02 has the highest base score. F-01 also deserves early treatment because tenant separation is a core trust boundary. Owner, exposure, exploit prerequisites and compensating controls should inform the final remediation schedule.

Evidence standard

Each finding identifies an actor, affected operation, expected result, actual result, bounded impact and closure test. "Demonstrated" refers only to the fictional scenario. In an actual report, a finding should be supported by retained test evidence and analyst review; uncertainty and untested consequences must remain explicit.

05 / DETAILED FINDINGS / F-01

Cross-workspace invoice disclosure

An object identifier must never substitute for an authorisation decision.

FINDING	RATING	STATE
F-01	Medium / 6.5	Open in fictional scenario

Affected surface: GET /api/v1/invoices/{invoice_id}

Classification: CWE-639 [3]; WSTG-v42-ATHZ-04 [1]

CVSS v3.1 base vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

Scenario: Member A can read an invoice belonging to workspace B by substituting a known fixture identifier. The API verifies authentication but does not constrain the lookup to the caller's workspace. Invoice identifiers are obtained from the agreed fixture manifest; enumeration is not assumed.

F01-E01 / REQUEST / SYNTHETIC EVIDENCE

```
GET /api/v1/invoices/INV-B-DEMO-02 HTTP/1.1
Host: workspace.example.com
Authorization: Bearer SAMPLE_MEMBER_A
```

F01-E02 / RESPONSE EXCERPT / SYNTHETIC EVIDENCE

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

{"invoiceId":"INV-B-DEMO-02","workspace":"B",
 "supplier":"Example Supplier","amount":2400,
 "currency":"USD","bankReference":"DEMO-ONLY"}
```

Expected: 403 or a consistently applied non-disclosing 404. **Actual:** the complete workspace B invoice is returned to member A. The response shown is abbreviated; all fixture values are synthetic.

Impact boundary: the scenario assumes full financial invoice disclosure across the protected dataset, supporting C:H. No modification or availability effect is demonstrated; I:N and A:N. A normal account is required (PR:L).

05 / F-01 / ENGINEERING ACTION

Enforce workspace ownership.

F-01 remediation and closure criteria.

Reproduce with two controlled accounts

• 1. Establish the fixture map: INV-A-DEMO-01 belongs to workspace A; INV-B-DEMO-02 belongs to workspace B. Confirm ownership using each workspace's administrator.

• 2. As member A, read the permitted invoice INV-A-DEMO-01 and retain the 200 response as a positive control.

• 3. Replace only the invoice identifier with INV-B-DEMO-02, keeping member A's token. Compare the returned workspace and invoice fields with the B fixture.

• 4. Repeat without credentials (expected 401), then as an authorised B account (expected 200). Stop after the minimum controlled cross-workspace proof.

Remediation guidance

Apply a central server-side policy to every invoice access path. Bind the object lookup to the authenticated workspace and verify the actor's permission for that operation. Reject by default before serialisation; repeat the check for downloads, exports and background jobs. Random identifiers reduce guessing but do not fix missing authorisation.

POLICY SKETCH / NOT PRODUCTION CODE / SYNTHETIC EVIDENCE

```
actor = require_authenticated_actor(request)
invoice = load_invoice(id=request.invoice_id,
                       workspace_id=actor.workspace_id)
require(invoice is not None)
require(policy.allows(actor, "invoice:read", invoice))
return permitted_invoice_fields(invoice)
```

RETEST CASE	ACCEPTANCE CRITERION
Member A -> workspace B invoice	Denied; no invoice content or sensitive metadata returned.
Member A -> allowed workspace A invoice	Permitted fields still returned; legitimate workflow preserved.
Alternate download / export routes	Same object and workspace rules applied; no bypass.
Absent / invalid authentication	401; no invoice content.

Reference: CWE-639 and OWASP WSTG v4.2 authorisation testing. See sources [1, 3] on page 18.

05 / DETAILED FINDINGS / F-02

Self-assigned workspace administrator role

A profile update accepts a privileged attribute controlled by the requester.

FINDING	RATING	STATE
F-02	High / 8.1	Open in fictional scenario

Affected surface: PATCH /api/v1/profile

Classification: CWE-915 [4]; WSTG-v42-ATHZ-03 [1]

CVSS v3.1 base vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Scenario: the member profile endpoint binds the JSON role field to the account record. A member changes their role to workspace_admin without a separate authorisation check. Follow-up requests confirm access to all workspace invoices and billing configuration changes.

F02-E01 / REQUEST / SYNTHETIC EVIDENCE

```
PATCH /api/v1/profile HTTP/1.1
Host: workspace.example.com
Authorization: Bearer SAMPLE_MEMBER_A
Content-Type: application/json

{"displayName":"Sample Member A",
 "role":"workspace_admin"}
```

F02-E02 / RESPONSE EXCERPT / SYNTHETIC EVIDENCE

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

{"account":"MEMBER-A","workspace":"A",
 "role":"workspace_admin"}
```

Expected: a forbidden role mutation is rejected and stored privileges remain unchanged. **Actual:** the new role persists and protected billing operations become available. The finding is supported by behavioural verification, not the echoed role field alone.

Rating rationale: network access, ordinary account, no victim action; full workspace financial confidentiality and integrity impact (C:H/I:H). Platform administrator rights, other workspaces and availability impact are not established.

05 / F-02 / ENGINEERING ACTION

Keep privilege changes explicit.

F-02 reproduction, bounded proof and remediation.

CONTROLLED SEQUENCE	ILLUSTRATIVE RESULT
As member A: GET /api/v1/billing/settings	403 before the profile mutation.
Submit the role field through PATCH /api/v1/profile	200; role persisted as workspace_admin.
Replay GET /api/v1/billing/settings with member A	200; workspace A billing configuration returned.
PATCH /api/v1/billing/settings with a demo billing label	200; synthetic billing label changed. No payments or external actions executed.
Restore fixtures using administrator A	Role reset to member and billing label restored.

Fix the update boundary

• Use a dedicated profile input schema that allows only editable fields such as displayName. Never bind an arbitrary request body directly to the account or authorisation model.

• Move role changes to a separate administrative operation. Verify the initiating actor, permitted role transition and workspace boundary on the server.

• Reject forbidden attributes consistently, including nested objects and alternate content types. Re-evaluate privileges on subsequent requests and invalidate stale authorisation caches where applicable.

• Audit legitimate and denied privilege changes with actor, subject, workspace and correlation identifiers. Avoid placing bearer tokens or sensitive record content in logs.

> **CLOSURE CRITERIA**
>
> A member cannot change role, workspace affiliation or permission flags through any profile route. Direct administrative calls remain denied. Approved administrator role changes still work and generate an audit event. Previously issued sessions must not retain unintended privilege.

Regression set: role, permissions and workspaceId fields; nested payloads; alternate profile methods; direct billing endpoint access; authorised administrator flow. Keep each test scoped to controlled fixtures.

Reference: CWE-915 and OWASP WSTG v4.2 privilege escalation testing. See sources [1, 4] on page 18.

05 / DETAILED FINDINGS / F-03

Stored script execution in work-item titles

Browser execution is demonstrated separately from storage or HTML rendering.

FINDING	RATING	STATE
F-03	Medium / 5.4	Open in fictional scenario

Affected surface: POST /api/v1/work-items -> /work-items/{id}

Classification: CWE-79 [5]; WSTG-v42-INPV-02 [1]

CVSS v3.1 base vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

Scenario: a member submits a work-item title that is stored and later inserted into an HTML sink. Another member opens the item and the supplied handler executes in that browser. The isolated proof changes a visible marker only; it sends no data externally.

F03-E01 / REQUEST BODY EXCERPT / SYNTHETIC EVIDENCE

```
POST /api/v1/work-items HTTP/1.1
Host: workspace.example.com
Authorization: Bearer SAMPLE_MEMBER_A
Content-Type: application/json

{"title":"<img src=x onerror=alert('SAMPLE-XSS')>"}
```

F03-E02 / PERSISTED RESPONSE EXCERPT / SYNTHETIC EVIDENCE

```
HTTP/1.1 201 Created
Content-Type: application/json

{"id":"WORK-DEMO-03",
 "title":"<img src=x onerror=alert('SAMPLE-XSS')>"}
```

Execution proof: in a separate browser session for another member of workspace A, opening WORK-DEMO-03 produces the SAMPLE-XSS alert. The next page illustrates this observation. Storage of the payload alone would not establish XSS.

Rating rationale: a member must store the payload (PR:L) and another user must open it (UI:R). The vulnerable application affects the browser security authority (S:C); limited browser-context confidentiality and integrity impact are modelled. Full account takeover is not claimed.

05 / F-03 / ENGINEERING ACTION

Render user content as data.

F-03 synthetic browser illustration and closure tests.

BROWSER ILLUSTRATION / NOT A CLIENT SCREENSHOT

workspace.example.com/work-items/WORK-DEMO-03

This page says

SAMPLE-XSS

Reproduction and evidence limits

Create the work item as a standard member, capture the stored response, then sign in as a different authorised member of the same workspace and open the item. Record the alert and page origin; a plain-text control must not execute. Remove the test item and restore any modified fixtures. No session-token theft or third-party callback is needed to establish execution.

Remediation

- Render titles using a text-only sink or framework escaping. Do not use raw innerHTML for plain-text fields.
- If rich text is a real requirement, use a maintained allowlist sanitiser and validate the supported markup contract. Review existing stored content and all rendering surfaces.
- Add a restrictive Content Security Policy as defence in depth. It does not replace safe rendering; verify compatibility with legitimate application scripts.

RETEST CASE	ACCEPTANCE CRITERION
Stored payload in a second account	No script execution; title rendered as text or safely sanitised.
Detail, list and notification views	Same safe treatment in every sink using the title.
Normal punctuation and supported formatting	Legitimate input remains usable without double encoding.
Existing persisted test item	Unsafe historical content is handled safely after the fix.

Reference: CWE-79 and OWASP WSTG v4.2 stored XSS testing. See sources [1, 5] on page 18.

05 / DETAILED FINDINGS / F-04

Sensitive invoice retained in browser cache

Local residual data exposure after logout; distinct from session invalidation.

FINDING	RATING	STATE
F-04	Low / contextual	Open in fictional scenario

Affected surface: GET /invoices/INV-A-DEMO-01

Classification: CWE-525 [6]; WSTG-v42-ATHN-06 [1]

CVSS: Not assigned; contextual observation, not a scored exploit.

Scenario: a rendered invoice page is cached in the browser. After logout and loss of network connectivity, a normal history revisit displays the cached invoice in the same browser profile. New API calls with the former token return 401; no server-side session bypass is demonstrated.

F04-E01 / SENSITIVE HTML RESPONSE EXCERPT / SYNTHETIC EVIDENCE

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: private, max-age=3600

[HTML containing invoice INV-A-DEMO-01]
```

Reproduction: view the synthetic invoice, log out, disable networking, then revisit through normal browser history in the same profile. Record the browser/version and distinguish disk cache, back-forward cache and application storage. In this fixture, developer tools identifies the response as served from disk cache.

Expected: invoice content is unavailable after logout. **Actual:** the cached response remains readable locally. **Risk:** a subsequent user of an unlocked/shared browser profile may read invoice content. Remote unauthenticated retrieval is not established; the Low rating is contextual.

Fix and verify

Use Cache-Control: no-store on sensitive authenticated responses. Clear application-managed sensitive state and caches on logout; prevent service workers from caching those responses. Test supported browsers, including offline and back/forward navigation. Do not assume that a header retroactively removes existing cache entries.

Closure: sensitive content is unavailable through the tested post-logout revisit paths; former tokens still receive 401; authenticated viewing still works. Document browser-specific behaviour and any residual shared-device risk.

Reference: CWE-525 and OWASP WSTG v4.2 browser cache testing. See sources [1, 6] on page 18.

05 / DETAILED FINDINGS / F-05

Diagnostic detail in API error responses

Report the information actually disclosed, without inferring an unproven exploit.

FINDING	RATING	STATE
F-05	Informational / contextual	Open in fictional scenario

Affected surface: GET /api/v1/invoices?limit=invalid

Classification: CWE-209 [7]; WSTG-v42-ERRH-01 [1]

CVSS: Not assigned; contextual observation, not a scored exploit.

Scenario: an authenticated malformed filter returns an internal handler name and a synthetic source path. No secrets, personal records, stack trace or exact component version are present in this fixture. The disclosure provides implementation hints but does not demonstrate compromise.

F05-E01 / REQUEST AND RESPONSE / SYNTHETIC EVIDENCE

```
GET /api/v1/invoices?limit=invalid HTTP/1.1
Host: workspace.example.com
Authorization: Bearer SAMPLE_MEMBER_A

HTTP/1.1 400 Bad Request
Content-Type: application/json

{"error":"InvoiceFilterError",
 "detail":"Invalid limit in /srv/demo/invoice-filter",
 "requestId":"REQ-DEMO-05"}
```

Reproduction: compare a valid numeric limit with the malformed value above using the same account. Repeat only on scoped endpoints; retain status, response body and request identifier. **Expected:** a safe validation message with a correlation ID. **Actual:** internal diagnostic detail is exposed.

Fix and verify

Return a stable, useful validation response such as "limit must be an integer". Keep internal exception and source detail in access-controlled server logs, correlated by request ID. Apply the same policy to gateway, application and asynchronous job failures.

Closure: malformed inputs return appropriate 4xx responses without internal paths, exception internals or secrets. Support staff can still locate the corresponding internal log event. Reassess severity if testing reveals sensitive data beyond this limited fixture.

Reference: CWE-209 and OWASP WSTG v4.2 error handling testing. See sources [1, 7] on page 18.

06 / REMEDIATION PLAN

Turn findings into owned work.

Suggested order for this fictional scenario; dates are agreed with the risk owner.

ORDER	OWNER / WORK PACKAGE	EXIT EVIDENCE
1 / F-02	Identity and API engineering: restrict profile updates and privileged role transitions.	Denied member mutation; approved admin flow; role-change audit trail.
2 / F-01	API engineering: centralise tenant and object policy across reads, downloads and jobs.	Cross-workspace test matrix and successful legitimate access controls.
3 / F-03	Frontend and API engineering: safe rendering, rich-text contract and existing-content handling.	Second-user execution test fails safely on all relevant views.
4 / F-04	Web platform engineering: sensitive-response caching and logout state cleanup.	Browser/version-specific offline and history retest records.
5 / F-05	API platform engineering: consistent public errors and internal diagnostics.	Clean 4xx responses with working log correlation.

Create a useful remediation ticket

Include the finding ID, responsible team, affected route, test actor, evidence reference, proposed control change, implementation owner, agreed target date, build identifier and the acceptance tests in this report. Link the ticket to the retained evidence without copying live credentials into the work tracker.

> **RISK ACCEPTANCE IS A DECISION**
>
> If a fix is deferred, record the business reason, remaining exposure, compensating controls, accountable approver and review expiry. "Accepted risk" is not equivalent to "Fixed" and must remain visible in the retest register.

Avoid cosmetic closure

Hiding a UI field does not close F-02. Switching to random invoice IDs does not close F-01. Blocking one payload at a perimeter filter does not close F-03. Verify the underlying control and neighbouring routes, then retain evidence of both denial and legitimate functionality.

07 / RETEST AND CLOSURE

A fix is a verified outcome.

The public sample makes no claim that remediation or a real retest has occurred.

ID	CURRENT SAMPLE STATE	RETEST REQUIRED
F-01	Open / not retested	Cross-workspace denial plus allowed-access controls.
F-02	Open / not retested	Role mutation denied; direct billing access denied.
F-03	Open / not retested	No execution in second-user rendering paths.
F-04	Open / not retested	No sensitive post-logout content in supported browser paths.
F-05	Open / not retested	Safe public errors with internal diagnostic correlation.

Closure states

STATE	MEANING
Fixed	Original proof fails safely; agreed regression tests pass on the identified build.
Partially fixed	Some paths are remediated but a relevant bypass or exposure remains.
Not fixed	The original condition is still reproducible.
Unable to verify	Access, environment or evidence is insufficient; state the blocker.
Accepted risk	Documented risk-owner decision; the technical exposure is not represented as remediated.

Retest evidence record

For each result, capture the assessor, timestamp, target environment, deployed build, original evidence ID, updated request/response, positive and negative controls, remaining limitations and owner acknowledgement. Preserve the original severity and document any residual-risk reassessment separately.

> **REGRESSION BOUNDARY**
>
> Retesting verifies the agreed fixes and related cases. It is not automatically a new full-scope penetration test. Significant architecture, authentication or feature changes may require additional assessment.

08 / ASSURANCE AND LIMITATIONS

Clear conclusions. Explicit boundaries.

A useful report distinguishes observed controls, assumptions and remaining uncertainty.

Positive controls illustrated in this scenario

CONTROL	BOUNDED OBSERVATION
Authentication enforcement	Protected fixture endpoints return 401 without valid credentials. This does not prove object-level authorisation.
Logout invalidation	Old API tokens fail after logout. F-04 separately concerns locally cached content.
Workspace separation on one admin route	Administrator A cannot access workspace B billing settings. Other object routes still require their own checks.

Assessment limitations

• Results are point-in-time and dependent on the assessed build, environment, identities and available access. An unreported weakness may still exist.

• Coverage follows the agreed scope and test budget. This sample contains selected examples, not exhaustive testing of every OWASP category.

• Impact is limited to the evidence and explicitly stated scenario assumptions. Production exploitation, real data theft, availability disruption and persistence are not demonstrated.

• Framework mappings organise tests and findings. They do not constitute OWASP endorsement, regulatory certification or proof that a system is secure.

What an actual delivery should include

An engagement-specific report should identify the authorised target and testing dates, access and exclusions, evidence provenance, actual affected builds, severity rationale, accountable reviewers and agreed retest scope. Delivery and retention arrangements should be confirmed with the client through the agreed secure channel.

SAMPLE HANDLING

This PDF is intentionally public. All application names, records, credentials, requests and browser illustrations were created for this sample. No real customer data or original assessment evidence is included.

09 / REFERENCES AND NEXT STEPS

Standards behind the structure.

Versioned references support reproducibility and make the reporting basis explicit.

[1] OWASP Web Security Testing Guide v4.2

Selected mappings: ATHZ-04, ATHZ-03, INPV-02, ATHN-06 and ERRH-01. This is not a claim of complete WSTG coverage.

https://owasp.org/www-project-web-security-testing-guide/v42/

[2] FIRST CVSS v3.1 specification

Base vectors and qualitative bands for F-01 to F-03. This sample deliberately uses one explicit scoring version.

https://www.first.org/cvss/v3.1/specification-document

[3] MITRE CWE-639

Authorisation bypass through a user-controlled key.

https://cwe.mitre.org/data/definitions/639.html

[4] MITRE CWE-915

Improperly controlled modification of object attributes.

https://cwe.mitre.org/data/definitions/915.html

[5] MITRE CWE-79

Cross-site scripting.

https://cwe.mitre.org/data/definitions/79.html

[6] MITRE CWE-525

Sensitive information retained in a web browser cache.

https://cwe.mitre.org/data/definitions/525.html

[7] MITRE CWE-209

Sensitive implementation information in error messages.

https://cwe.mitre.org/data/definitions/209.html

Discuss your assessment

Start with the application, trust boundaries, business-critical workflows and desired delivery window. SpotDefence can help define the testing scope, evidence requirements and remediation priorities.

Schedule an assessment with SpotDefence

security@spotdefence.io

PUBLIC SAMPLE / ALL SCENARIOS AND EVIDENCE ARE FICTIONAL