PENETRATION TEST REPORT

Web Application Penetration Test

Annual external security assessment of the customer-facing digital banking portal, aligned with SAMA Cyber Security Framework expectations.

Client	Riyadh National Bank (fictional)
Engagement	2026 Annual Web Application Assessment
Date	2026-09-17
Report ID	FS-2026-014

Mohammed Al-Faleh (FalehSec)

PENETRATION TEST REPORT

Web Application Penetration Test

FS-2026-014 · v1.0
2026-09-17 · Confidential

CLIENT	ENGAGEMENT	CONSULTANT	VERSION
Riyadh National Bank (fictional)	**2026 Annual Web Application Assessment**	**Mohammed Al-Faleh (FalehSec)**	**1.0**

Handling note. This report contains security findings and is intended solely for Riyadh National Bank (fictional). Do not distribute outside the engagement without written authorization. Findings should be remediated and revalidated before the environment is considered secure.

Contents

Table of Contents

01 Executive Summary

FalehSec performed an external application security assessment of the digital banking portal between **2026-09-01** and **2026-09-12**. A total of **6 findings** were identified: **1 Critical, 2 High, 1 Medium, 1 Low, and 1 Informational**.

No indicators of prior compromise were observed. The most significant risk is an IDOR in the account-statement download endpoint (`F-01`), which could expose customer financial data to authenticated users. Immediate remediation of the Critical and High findings is recommended before the next promotion window.

Assessment Overview

Between **2026-09-01** and **2026-09-12**, an authenticated and unauthenticated security assessment was performed against 3 target(s) at Riyadh National Bank (fictional). Testing aligned with **OWASP Top 10:2025**, **NIST SP 800-115**, and mapped to the **SAMA Cyber Security Framework** and **NCA Essential Cybersecurity Controls (ECC)**.

Severity Summary

1	2	1	1	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

Full technical detail, reproduction steps, and remediation guidance for every finding are provided in Section 4. A retest is available within 3 months at 30% of the original engagement fee.

02 Scope & Methodology

In-Scope Targets

TARGET	TYPE	STATUS	NOTES
`https://portal.rbn.example`	Web Application	In scope	Production, authenticated + unauthenticated
`https://api.rbn.example/v1`	REST API	In scope	Authenticated (test accounts only)
`https://www.rbn.example`	Public Website	Limited	Passive recon only

Methodology

Testing followed the phases below, based on **NIST SP 800-115** technical guidelines and OWASP testing guides, and consistent with SAMA CSF 3.3.17 (Vulnerability Management):

1. **Phase 1 — Reconnaissance:** subdomain enumeration, technology fingerprinting, and API surface mapping (passive + active, agreed scope).
2. **Phase 2 — Configuration & Discovery:** review of headers, TLS posture, CORS policy, error handling, and misconfiguration checks.
3. **Phase 3 — Vulnerability Analysis:** manual testing against OWASP Top 10:2025 categories — broken access control, injection, auth & session flaws, SSRF/CWE-918 handling, supply-chain review of dependencies.
4. **Phase 4 — Exploitation & Validation:** safe exploitation with proof-of-concept that avoids destructive actions, per rules of engagement.
5. **Phase 5 — Reporting & Retest:** findings documented, prioritized, and revalidated within 3 months at 30% of the original fee.

Tools & Techniques

- Burp Suite Professional (manual testing)
- OWASP ZAP (supplemental)
- custom reconnaissance scripts
- nuclei (template-based scanning)
- ffuf (content dictional discovery)

03 Findings Summary

A total of **6** finding(s) were identified. Each finding includes affected location, technical reproduction, business impact, and remediation guidance.

ID	FINDING	SEVERITY	LOCATION	EVIDENCE
F-01	Insecure Direct Object Reference in Statement Download	CRITICAL	GET /api/v1/accounts/{account_id}/statements?month=2026-08	
F-02	Username Enumeration via Login Response Timing	HIGH	POST /api/v1/auth/login	—
F-03	Missing Rate Limiting on One-Time Password Challenge	HIGH	POST /api/v1/auth/otp/verify	
F-04	Session Cookie Missing `Secure` Flag in Staging Mirror	MEDIUM	Set-Cookie on staging.rbn.example	—
F-05	Informative Server Banner Leakage	LOW	HTTP response header "Server: nginx/1.22.1"	—
F-06	Deprecated TLS Cipher Availability	INFO	TLS configuration — portal.rbn.example	—

04 Detailed Findings

Each finding is rated by its technical severity and business impact. Confirmations are provided per finding.

F-01

CRITICAL | CVSS 9.1 | CWE-639

Insecure Direct Object Reference in Statement Download

AFFECTED LOCATION

```
GET /api/v1/accounts/{account_id}/statements?month=2026-08
```

DESCRIPTION

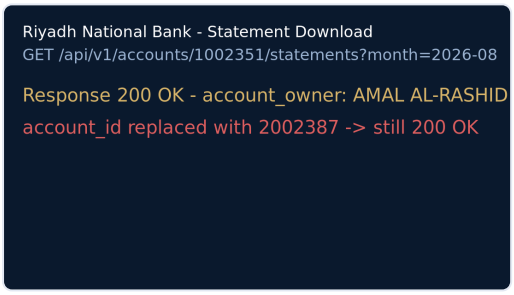
The statement download endpoint trusts the `account_id` path parameter without verifying that the authenticated session owns the requested account. Replacing the identifier with another customer's account number returns their monthly statement PDF.

This maps to **OWASP A01:2025 (Broken Access Control)** and **NCA ECC 4.2 (Privileged Access Management / access verification)**.

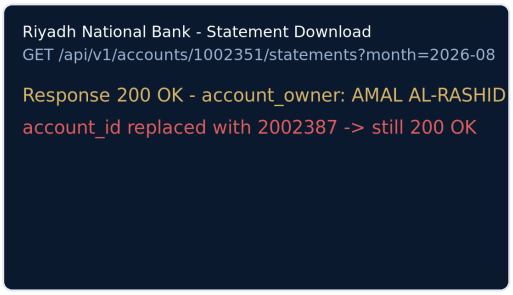
REPRODUCTION STEPS

1. Log in with test account A and request `GET /api/v1/accounts/1002351/statements?month=2026-08`.
2. Replay the same request with `account_id` set to `1002362` (account of a second test account).
3. Observe the server returns the statement resource without a 403 or ownership check.

EVIDENCE



Replacing account_id returns another customer's statement (200 OK)



Identical response served for foreign account_id — no 403 raised

BUSINESS IMPACT

An authenticated user can download the confidential banking statements of **any customer**, causing direct financial data exposure, regulatory non-compliance (SAMA CSF), and reputational damage to the bank.

REMEDIATION

Enforce object-level authorization on the server: resolve the account from the authenticated session (never from the request parameter), and add a 403 on ownership mismatch. Add an authorization unit test for each account-scoped endpoint.

REFERENCES

- https://owasp.org/Top10/A01_2021-Broken_Access_Control/
- https://cwe.mitre.org/data/definitions/639.html

F-02

HIGH CVSS 5.3 CWE-204

Username Enumeration via Login Response Timing

AFFECTED LOCATION

```
POST /api/v1/auth/login
```

DESCRIPTION

Login responses for unknown usernames return in ~35ms while valid usernames (even with a wrong password) take ~620ms due to an additional password-hash comparison. This allows reliable account enumeration, a precursor to targeted credential attacks.

REPRODUCTION STEPS

1. Send `POST /api/v1/auth/login` with a random username; measure response time.
2. Repeat with a known-valid username; observe a statistically significant timing difference.
3. Confirm response body and status code are identical in both cases (only timing differs).

BUSINESS IMPACT

Enables attackers to build a list of valid account identifiers, significantly improving the success rate of credential-stuffing and phishing campaigns.

REMEDIATION

Execute a dummy hash comparison for unknown usernames so response timing is uniform, or rate-limit authentication endpoints and alert on sustained timing-based enumeration.

REFERENCES

- https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

F-03

HIGH CVSS 6.5 CWE-307

Missing Rate Limiting on One-Time Password Challenge

AFFECTED LOCATION

`POST /api/v1/auth/otp/verify`

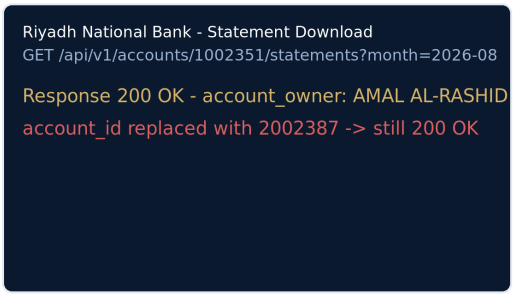
DESCRIPTION

The OTP verification endpoint does not enforce a lockout or request-rate limit. With a 6-digit OTP and no attempt cap, an attacker can brute-force the challenge within a practical window.

REPRODUCTION STEPS

1. Trigger an OTP challenge to a test account.
2. Issue repeated `POST /api/v1/auth/otp/verify` attempts with sequential codes.
3. Observe unlimited attempts without lockout or throttling until the window expires.

EVIDENCE



Repeated OTP guesses return valid codes (no throttling)

BUSINESS IMPACT

Bypass of second-factor authentication via brute-force, exposing accounts to account takeover even when customers have MFA enabled.

REMEDIATION

Enforce a maximum of 5 failed attempts followed by revocation of the challenge and a configurable cool-down. Add per-IP + per-account combined rate limiting.

REFERENCES

- https://cwe.mitre.org/data/definitions/307.html

F-04

MEDIUM CVSS 4.3 CWE-614

Session Cookie Missing `Secure` Flag in Staging Mirror

AFFECTED LOCATION

```
Set-Cookie on staging.rbn.example
```

DESCRIPTION

The staging mirror sets the session cookie over HTTPS but omits the `Secure` attribute. If the cookie is ever transmitted over a downgraded connection, it can be intercepted in transit.

REPRODUCTION STEPS

1. Authenticate against the staging mirror.
2. Inspect the `Set-Cookie` header; note the absence of the `Secure` flag.

BUSINESS IMPACT

Low likelihood in practice, but increases the risk of session-hijacking under network downgrade scenarios and violates security-header hardening expectations (NCA ECC 4.2).

REMEDIATION

Add the `Secure` attribute to all session cookies, and consider `SameSite=Strict` and a short session lifetime for non-banking surfaces.

REFERENCES

- https://owasp.org/www-community/controls/SecureFlag

F-05

LOW CVSS 0.0 CWE-200

Informative Server Banner Leakage

AFFECTED LOCATION

```
HTTP response header "Server: nginx/1.22.1"
```

DESCRIPTION

The web server exposes its exact version in response headers, and the 404 handler reveals the backend framework and patch level.

REPRODUCTION STEPS

1. curl -sI https://portal.rbn.example
2. Observe `Server: nginx/1.22.1` and `X-Powered-By: Express 4.19`.

BUSINESS IMPACT

Minor. Aids attackers in selecting version-specific exploits; low risk given current patching cadence.

REMEDIATION

Obfuscate the `Server` header, disable `X-Powered-By`, and ensure custom 404 templates.

REFERENCES

- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint-Web-Server

F-06

INFO CVSS 0.0 CWE-327

Deprecated TLS Cipher Availability

AFFECTED LOCATION

`TLS configuration — portal.rbn.example`

DESCRIPTION

Server advertises legacy cipher suites (e.g., TLS 1.0-compatible suites) during handshake negotiation, despite TLS 1.2/1.3 being enforced for browsers.

REPRODUCTION STEPS

1. Run `nmap --script ssl-enum-ciphers -p 443 portal.rbn.example`.
2. Observe deprecated suites listed as available.

BUSINESS IMPACT

Primarily a hardening observation; no practical exploit identified given modern client enforcement.

REMEDIATION

Disable pre-TLS-1.2 ciphers and enable BoringSSL-style cipher policy. Re-run cipher enumeration after change to confirm.

REFERENCES

- https://cwe.mitre.org/data/definitions/327.html

05 Recommendations & Remediation Plan

Priority order

1. **F-01 (Critical)** — implement object-level authorization and retest. Block release until resolved.
2. **F-02 / F-03 (High)** — normalize login timing and enforce OTP rate limits. Target: next sprint.
3. **F-04 / F-05 (Medium/Low)** — cookie hardening and banner removal with the next deployment.
4. **F-06 (Info)** — schedule TLS cipher cleanup in the platform hardening backlog.

FalehSec recommends a **retest within 3 months** (30% of original fee) to confirm remediation, followed by a recurring assessment aligned with SAMA CSF 3.3.17 Vulnerability Management expectations.

Immediate priorities. Address all Critical and High findings before exposing any affected system to untrusted users. FalehSec offers a **re-test within 3 months at 30% of the original engagement fee** to confirm remediations.

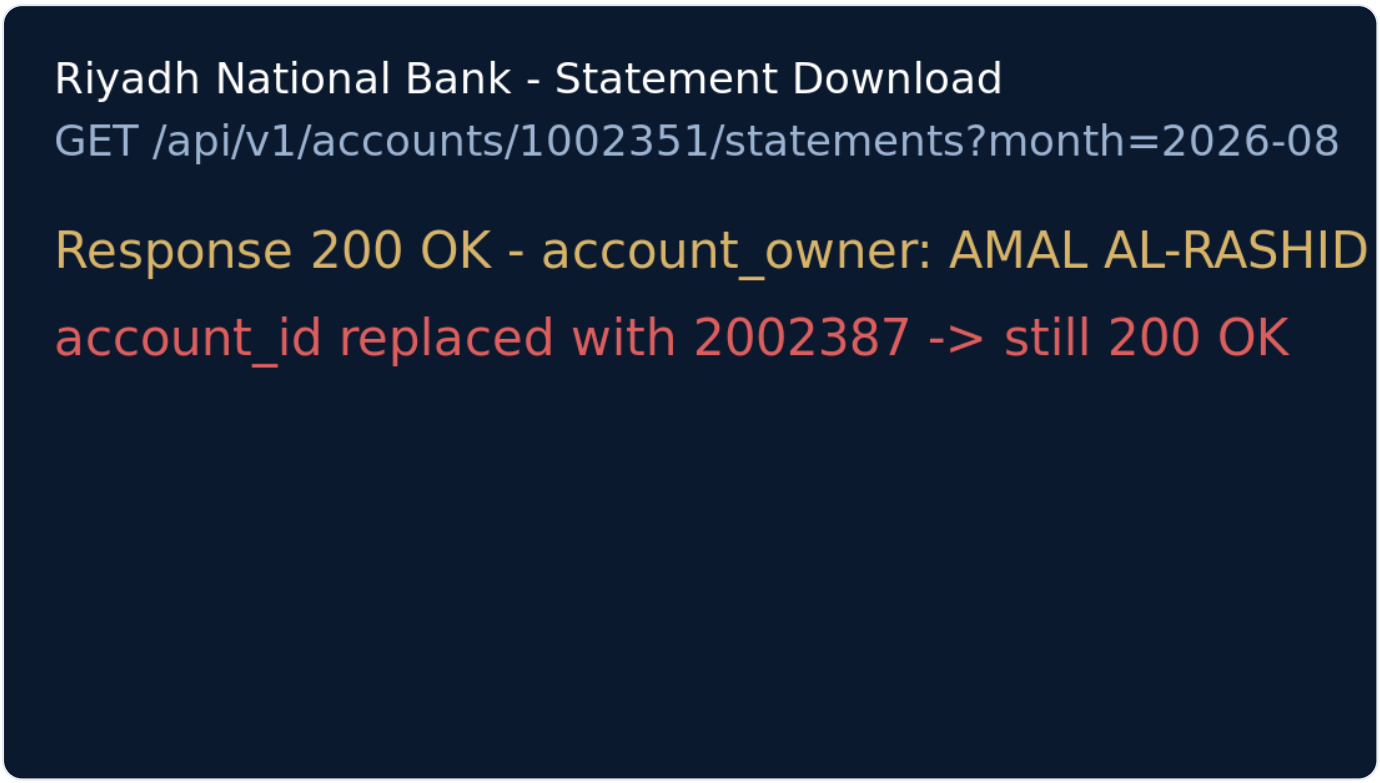
06 Methodology Evidence (Sample Screenshots)

This section is reserved for evidence screenshots captured during testing. Screenshots prove reproducibility and are referenced per finding above.

Placeholder — replace with your evidence images in the final deliverable.

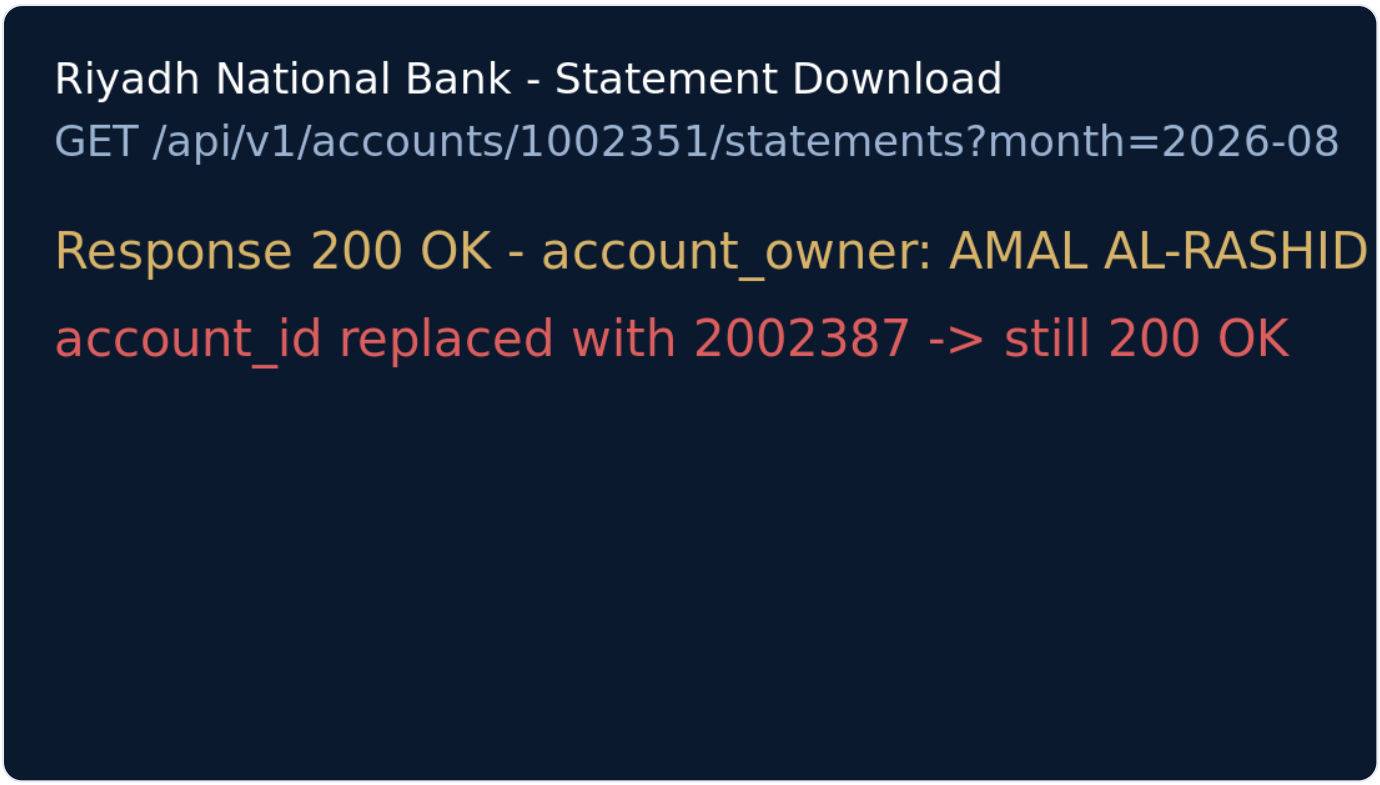
AP Evidence Gallery

Full-size captures referenced from Section 4 findings. Click any thumbnail in the findings to jump back here; captions are repeated for traceability.



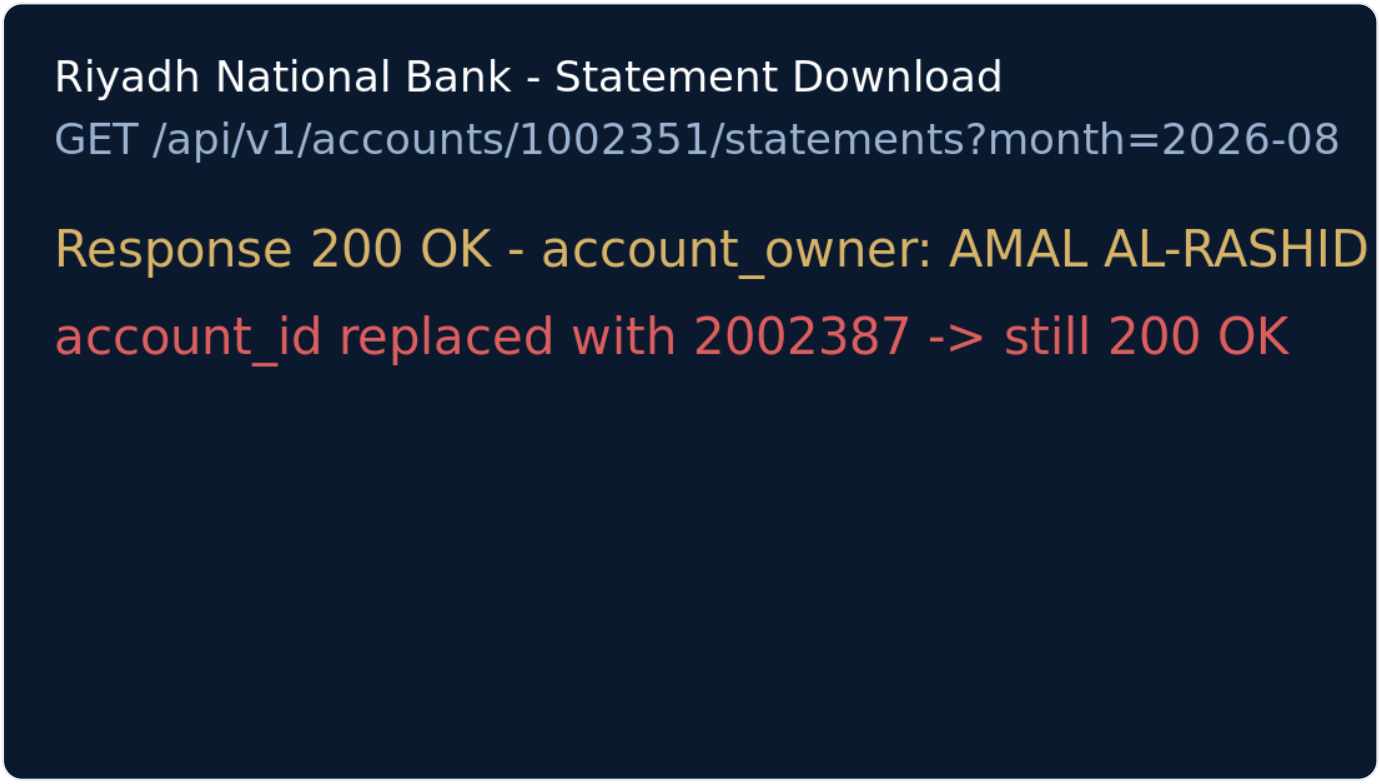
F-01 — Replacing account_id returns another customer's statement (200 OK)

← Back to F-01 in Section 4



F-01 — Identical response served for foreign account_id — no 403 raised

← Back to F-01 in Section 4



F-03 — Repeated OTP guesses return valid codes (no throttling)

← Back to F-03 in Section 4

AP Appendix & References

Engagement artifacts

- Rules of engagement: signed 2026-08-25
- Evidence archive: encrypted, retained 24 months
- Retest window: expires 2026-12-12

References: OWASP Top 10:2025 · NIST SP 800-115 · SAMA Cyber Security Framework (3.3.17) · NCA ECC-1:2018 · ISO/IEC 27001:2022

Markup Reference

Severity ratings follow CVSS 3.1 vectors where provided, mapped to OWASP Top 10:2025 risk categories and referenced to NCA ECC controls as applicable.