AXUM SEC × Meridian BANK ETHIOPIA

CONFIDENTIAL

SECURITY ASSESSMENT REPORT - TECHNICAL

Meridian Bank Ethiopia — Digital Banking Platform: External Penetration Test

AXUM SEC performed an external, authenticated and unauthenticated penetration test of Meridian Bank Ethiopia's digital banking platform (customer web application, mobile API and public gateway) between 26 October and 13 November 2026.

Prepared for **Meridian Bank Ethiopia**

ASSESSMENT AT A GLANCE

11	1	3	4	2	1
TOTAL FINDINGS	CRITICAL	HIGH	MEDIUM	LOW	INFO

Significant exposure requires immediate action
1 critical finding requires remediation before the next release.

ISSUED	ENGAGEMENT	VERSION	CLASSIFICATION
25 November 2026	Digital Banking Platform — web application, mobile API, gateway	1.0	Confidential
TESTING WINDOW	LEAD CONSULTANT	APPROACH	APPROVED
26 October 2026 – 13 November 2026	Hana Tesfaye	Grey-box	25 November 2026

Contents

1 Document control
2 Executive summary
3 Scope and methodology
4 Findings overview
5 Detailed findings
6 Remediation plan
7 Standards alignment
8 Document sign-off
9 Appendix A — Rating definitions
10 Appendix B — Glossary

1 Document control

Document title	Meridian Bank Ethiopia — Digital Banking Platform: External Penetration Test
Document ID	AXR-2026-0147
Classification	Confidential — client distribution
Issued by	AXUM SEC
Prepared for	Meridian Bank Ethiopia
Engagement	Digital Banking Platform — web application, mobile API, gateway
Report type	Security Assessment Report - Technical
Version	1.0
Issued	25 November 2026
Data current as of	25 November 2026, 08:00 UTC
Distribution	The named recipient and their organisation. Not for onward distribution without written consent from AXUM SEC.

DOCUMENT AUTHENTICATION

Issued and sealed by AXUM SEC. Quote the document ID above in any correspondence about this report, including any question about its currency or permitted distribution.

2 Executive summary

11	1	3	4	2	1
TOTAL FINDINGS	CRITICAL	HIGH	MEDIUM	LOW	INFO

AXUM SEC performed an external, authenticated and unauthenticated penetration test of Meridian Bank Ethiopia's digital banking platform (customer web application, mobile API and public gateway) between 26 October and 13 November 2026.

The platform has a sound foundation, but **one critical and three high-severity weaknesses were found that allow unauthenticated access to customer records, cross-customer data access, SQL injection and account takeover.** Three of the four were fixed and verified by retest before this report was issued; the remaining high finding is in remediation.

KEY OBSERVATIONS

- Authorization is enforced inconsistently: some routes check ownership, others check only that a token exists.
- Several defects stem from one missing control (deny-by-default routing) rather than isolated mistakes.
- Three of the four most serious findings were fixed within three weeks and verified.

WHAT IS WORKING WELL

- Passwords are stored with a modern adaptive hash and sign-in is protected by a second factor.
- Cross-site request forgery protections are in place on all state-changing web requests.
- File upload handling validates type and size and stores files outside the web root.
- The engineering team engaged immediately and fixed critical issues during the test window.

Risk and impact assessment

The most serious exposure is the unauthenticated internal API (AXR-0147-001): the customer KYC database could be read by anyone on the internet. Combined with the account-takeover path through the refresh endpoint (AXR-0147-004) and the cross-customer statement access (AXR-0147-002), an attacker could both learn who the bank's customers are and act as them.

The remaining findings are mostly hardening items. They matter mainly because they make the serious findings easier to exploit or harder to detect: the missing Content-Security-Policy is what lets the reflected XSS run, and verbose errors speed up reconnaissance.

Mitigation strategy

Fixes should be sequenced by blast radius. First remove public exposure of anything under `/internal` and fix token verification. Then close the authorization and injection classes of defect at the framework level rather than endpoint by endpoint: server-side ownership checks, parameterised queries and an allow-list of filterable fields. Finally, apply the configuration hardening (TLS, headers, error handling) at the edge so it covers every route.

Conclusion and next steps

Meridian Bank responded quickly: three of the four most severe findings were remediated within three weeks and verified by retest. We recommend completing the refresh-token fix and key rotation first, scheduling the medium findings within 90 days, and adding the authorization and injection regression tests to the delivery pipeline so these classes of defect cannot return. A full retest of the open items is available once fixes are deployed.

3 Scope and methodology

Engagement	Digital Banking Platform — web application, mobile API, gateway
Assessment type	Technical
Report template	Security Assessment Report - Technical
Data current as of	25 November 2026, 08:00 UTC

This report states the findings recorded against the engagements and assets in scope at the time of issue. It is generated from the platform's finding records; any finding that was dismissed, duplicated or closed before issue is excluded from the counts unless the selected scope included it.

In scope

ASSET	TYPE	ENVIRONMENT	NOTES
app.meridianbank.example	Web application	Production	Customer portal, authenticated and unauthenticated

ASSET	TYPE	ENVIRONMENT	NOTES
api.meridianbank.example	REST API (v2)	Production	Mobile and web back end, about 140 endpoints
gateway.meridianbank.example	API gateway	Production	Routing, authentication and rate limiting
MeridianBank mobile (Android, iOS)	Mobile API traffic	Production	Back-end only; no binary reverse engineering

Explicitly out of scope

- Denial-of-service and load testing
- Social engineering and physical testing
- Third-party payment processor and SMS provider
- Core banking system and internal networks

Rules of engagement

Testing window	26 October 2026 — 13 November 2026
Approach	Grey-box: unauthenticated testing plus two customer test accounts and one back-office test account supplied by the bank. No production customer data was modified.
Authorisation	Signed rules-of-engagement and testing authorisation, ref. MBE-SEC-2026-044, dated 20 October 2026.
Test accounts	2 customer accounts, 1 back-office account (revoked after testing)
Source IP addresses	196.188.10.24, 196.188.10.25
Test team	Hana Tesfaye (Lead consultant); Samuel Bekele (Application security engineer); Ruth Alemu (Cryptography and infrastructure)

Methodology

1. **Reconnaissance**
   Passive and active discovery of hosts, endpoints, technologies and exposed routes.
2. **Threat modelling**
   Identify high-value assets (customer data, funds movement) and the trust boundaries around them.
3. **Automated scanning**
   Authenticated and unauthenticated scanning to establish a baseline and find known weaknesses.
4. **Manual testing**
   Authorization, business logic, authentication and injection testing guided by the OWASP WSTG and API Security checklists.
5. **Exploitation and impact**
   Safe, read-only proof of exploitability to establish real impact without harming production.
6. **Reporting and retest**
   Findings scored with CVSS v3.1, delivered with evidence and remediation, and retested after the client reports a fix.

Aligned to: OWASP WSTG · OWASP API Security Top 10 · OWASP Top 10 (2021) · PTES · NIST SP 800-115

Tools and techniques

TOOL	USED FOR
Burp Suite Professional	Intercepting proxy, manual request manipulation, authorization testing
sqlmap	Confirming SQL injection (read-only techniques)

TOOL	USED FOR
testssl.sh	TLS protocol and cipher assessment
Nuclei and ffuf	Template-based checks, route and parameter discovery
Custom scripts	Authorization matrices across roles, token handling tests

Limitations and assumptions

- Testing was limited to the in-scope assets and the testing window; later changes are not covered.
- Rate-limit findings were demonstrated at a controlled volume to avoid affecting production availability.
- Mobile application binaries were not decompiled; only their back-end traffic was tested.
- The absence of a finding is not proof that a weakness does not exist.

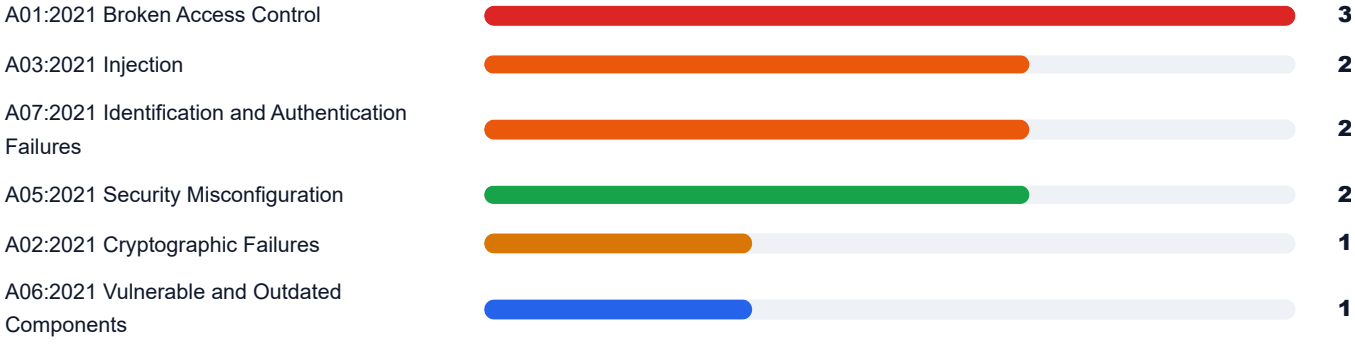
4 Findings overview



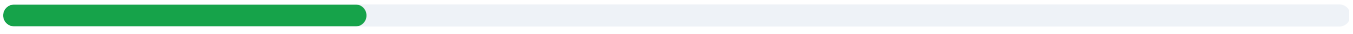
SEVERITY	COUNT	SHARE	DISTRIBUTION
Critical	1	9%	
High	3	27%	
Medium	4	36%	
Low	2	18%	
Info	1	9%	

Average severity score 2.09 on a 1–4 scale (low 1, medium 2, high 3, critical 4), calculated across 11 finding(s).

Findings by weakness category (OWASP Top 10, 2021)



Remediation progress



3 of 11 findings were fixed and verified by retest before this report was issued (27%).

5 Detailed findings

11 findings, ordered as reported. Each finding is cited as its section number.

5.1 Unauthenticated internal API exposes customer KYC records

CVSS 9.1 | CWE-306 | Fixed | CRITICAL

Finding ID	AXR-0147-001
OWASP category	A01:2021 Broken Access Control
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Affected asset	https://api.meridianbank.example/internal/api/v1/kyc/customers
Status	resolved
Reported by	AXUM SEC Red Team
Reported on	29 October 2026
Retest	Fixed and verified 18 November 2026 Route group no longer reachable from the internet; authenticated requests require the back-office role.

DESCRIPTION

The `/internal/api/v1/*` route group is meant for back-office tooling but is published on the same public load balancer as the customer API and performs **no authentication**. Any internet user can list, search and export KYC customer records, including national ID numbers and phone numbers.

The route group was added during a migration and was never placed behind the gateway's authentication plugin; a network ACL that was supposed to restrict it to the office VPN is not applied to the public listener.

IMPACT

Full disclosure of the customer KYC database (about 184,000 records) to any unauthenticated party, which is reportable under the National Bank of Ethiopia data-protection directives and exposes customers to identity fraud and targeted phishing.

EVIDENCE AND REPRODUCTION

1. From an unauthenticated session, send `GET /internal/api/v1/kyc/customers?limit=3`.
2. The API answers `200 OK` with customer records and a `total` of 184,203.
3. Increase `limit` and page through `page=2…n` to enumerate the full dataset. No data was extracted beyond three redacted examples.

RECOMMENDED REMEDIATION

- Remove the `/internal` route group from the public listener immediately, or block it at the load balancer.
- Require the gateway authentication plugin and an explicit back-office role on every `/internal` route.
- Add a deny-by-default test that fails the build if a route is registered without an authentication policy.
- Treat the exposure window as a data-protection incident and assess notification duties.

EVIDENCE

Burp Suite - Repeater - /internal/api/v1/kyc/customers

```
REQUEST
GET /internal/api/v1/kyc/customers?limit=3 HTTP/1.1
Host: api.meridianbank.example
Accept: application/json
User-Agent: Mozilla/5.0
# no Authorization header, no session cookie

RESPONSE
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
X-Powered-By: Express

{"data":[
  {"customerId":"C-100231","fullName":"[REDACTED]","nationalId":"[REDACTED]","phone":"+2519*******","kycStatus":"verified"},
  {"customerId":"C-100232","fullName":"[REDACTED]","nationalId":"[REDACTED]","phone":"+2519*******","kycStatus":"verified"},
  {"customerId":"C-100233","fullName":"[REDACTED]","nationalId":"[REDACTED]","phone":"+2519*******","kycStatus":"pending"}
],"total":184203,"page":1}
```

admin-api-unauthenticated.png — Unauthenticated request returning KYC records (data redacted)

REFERENCES

- https://owasp.org/Top10/A01_2021-Broken_Access_Control/
- https://cwe.mitre.org/data/definitions/306.html

5.2 Broken object-level authorization on account statements (IDOR)

CVSS 8.1 | CWE-639 | Fixed | HIGH

Finding ID	AXR-0147-002
OWASP category	A01:2021 Broken Access Control
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
Affected asset	GET /api/v2/accounts/{accountId}/statements
Status	resolved
Reported by	AXUM SEC Red Team
Reported on	30 October 2026
Retest	Fixed and verified 18 November 2026 Ownership check enforced; cross-customer request returns 404.

DESCRIPTION

The statements endpoint checks that the caller holds a valid token but never checks that the requested `accountId` belongs to that caller. Changing the identifier in the path returns another customer's statement.

IMPACT

Any registered customer can read the transaction history and balances of any other customer, and by chaining with the statement-export function can download PDF statements in bulk.

EVIDENCE AND REPRODUCTION

1. Authenticate as customer A and capture the bearer token.
2. Request `/api/v2/accounts/ACC-70415522/statements?month=2026-09`, an account owned by customer B.
3. The response is `200 OK` with customer B's statement. A `403` was expected.

RECOMMENDED REMEDIATION

- Resolve the account from the token subject and verify ownership on the server for every request; never trust the identifier in the path alone.
- Return `404` for accounts the caller does not own to avoid confirming that they exist.
- Replace sequential account numbers in URLs with unguessable identifiers as defence in depth.
- Add cross-customer access tests to the API regression suite.

EVIDENCE



idor-account-statements.png — Customer A reading customer B's statement (data redacted)

REFERENCES

- https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/

5.3 SQL injection in transaction search filter

CVSS 8.8 | CWE-89 | Fixed | HIGH

Finding ID	AXR-0147-003
OWASP category	A03:2021 Injection
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Affected asset	POST /api/v2/transactions/search (filter[reference])
Status	resolved
Reported by	AXUM SEC Red Team
Reported on	02 November 2026
Retest	Fixed and verified 19 November 2026 Queries parameterised; injection payloads no longer change responses.

DESCRIPTION

The `filter[reference]` field is concatenated into a PostgreSQL query. A boolean-based blind injection confirms the field is injectable by any authenticated customer.

IMPACT

An authenticated attacker can read any table the application account can read, including credentials and card tokens, and may be able to modify data. Exploitation was demonstrated read-only; no data was extracted.

EVIDENCE AND REPRODUCTION

1. Authenticate as any customer.
2. Send the search request with `TX-1' AND 4821=4821 AND 'a'='a` and then … `4821=4822` ….
3. The two responses differ, confirming boolean-based blind injection (sqlmap output attached).

RECOMMENDED REMEDIATION

- Use parameterised queries or the ORM's bound parameters for every filter; never build SQL from request fields.
- Allow-list filterable columns and operators server-side.
- Reduce the database account to the minimum privileges the service needs.
- Add SAST and a dynamic injection scan to the pipeline.

EVIDENCE

sqlmap - POST /api/v2/transactions/search

```
$ sqlmap -r search.req -p "filter[reference]" --batch --technique=B --dbms=postgresql
[INFO] testing connection to the target URL
[INFO] testing if the target URL content is stable
[INFO] POST parameter 'filter[reference]' appears to be dynamic
[INFO] heuristic (basic) test shows that POST parameter 'filter[reference]' might be injectable
[INFO] POST parameter 'filter[reference]' is 'PostgreSQL boolean-based blind' injectable
---
Parameter: filter[reference] (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: {"filter":{"reference":"TX-1' AND 4821=4821 AND 'a'='a"}}
---
[INFO] the back-end DBMS is PostgreSQL
[INFO] fetching current database: [REDACTED]  (read-only proof; no data extracted)
```

sqli-transaction-search.png — sqlmap confirming boolean-based blind injection (read-only)

REFERENCES

- https://owasp.org/Top10/A03_2021-Injection/
- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

5.4 Refresh endpoint accepts JWTs with the "none" algorithm

CVSS 7.5 | CWE-347 | Open | HIGH

Finding ID	AXR-0147-004
OWASP category	A07:2021 Identification and Authentication Failures
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Affected asset	POST /api/v2/auth/refresh
Status	in_progress
Reported by	AXUM SEC Red Team
Reported on	03 November 2026
Retest	Open 19 November 2026 Fix in review; the endpoint still accepted an unsigned token on the day of retest.

DESCRIPTION

The token refresh handler selects the verification algorithm from the token's own header. A token whose header declares `"alg":"none"` and carries an empty signature is accepted.

IMPACT

An attacker can mint a valid session for any user identifier without credentials, leading to full account takeover.

EVIDENCE AND REPRODUCTION

1. Take any expired access token and decode it.
2. Replace the header with `{"alg":"none","typ":"JWT"}`, set `sub` to a target user id, and remove the signature.

3. Submit it to `/api/v2/auth/refresh`: a fresh access token for the target user is returned.

RECOMMENDED REMEDIATION

- Pin the expected algorithm (RS256) in the verifier and reject any other value, including `none`.
- Upgrade the JWT library and enable its strict mode.
- Bind refresh tokens to a server-side session record that is checked on every use.
- Rotate the signing keys after the fix, because forged tokens may exist.

REFERENCES

- https://datatracker.ietf.org/doc/html/rfc8725#section-3.1

5.5 Profile API returns more personal data than the client displays

CVSS 6.5 | CWE-213 | MEDIUM

Finding ID	AXR-0147-005
OWASP category	A01:2021 Broken Access Control
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Affected asset	GET /api/v2/profile
Status	triaged
Reported by	AXUM SEC Red Team
Reported on	04 November 2026

DESCRIPTION

The profile response includes the national ID number, date of birth and the full registered address. The mobile and web clients display only the name and a masked phone number; the rest is filtered in the browser.

IMPACT

Anyone who obtains a session (for example through the XSS in AXR-0147-006) receives data the product does not need to expose, widening the impact of any session compromise.

EVIDENCE AND REPRODUCTION

1. Sign in and open the browser developer tools.
2. Inspect the response to `GET /api/v2/profile`: `nationalId`, `dateOfBirth` and `address` are present in clear text.

RECOMMENDED REMEDIATION

- Return only the fields each client needs (an explicit response schema per endpoint).
- Mask national ID and phone number on the server.
- Move rarely needed attributes behind a re-authentication step.

REFERENCES

- https://owasp.org/API-Security/editions/2023/en/0xa3-broken-object-property-level-authorization/

5.6 Reflected cross-site scripting in the transfer receipt page

CVSS 6.1 | CWE-79 | MEDIUM

Finding ID	AXR-0147-006
OWASP category	A03:2021 Injection
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Affected asset	GET /receipt?ref=
Status	triaged
Reported by	AXUM SEC Red Team
Reported on	05 November 2026

DESCRIPTION

The `ref` query parameter is written into the receipt page without output encoding. A crafted link executes script in the victim's browser in the bank's origin.

IMPACT

An attacker who persuades a signed-in customer to open a link can act as that customer in the web application and read data from the profile API.

EVIDENCE AND REPRODUCTION

1. Open `/receipt?ref="><svg onload=alert(document.domain)>` while signed in.
2. The script runs and the alert shows the bank's domain.

RECOMMENDED REMEDIATION

- Encode all output for its context (HTML, attribute, JavaScript) using the framework's templating, not string concatenation.
- Deploy a Content-Security-Policy that blocks inline script (see AXR-0147-010).
- Set session cookies `HttpOnly`, `Secure` and `SameSite=Strict`.

REFERENCES

- https://owasp.org/www-community/attacks/xss/
- https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

5.7 Weak TLS configuration: TLS 1.0/1.1 and CBC / 3DES suites enabled

CVSS 5.9 | CWE-326 | MEDIUM

Finding ID	AXR-0147-007
OWASP category	A02:2021 Cryptographic Failures
CVSS vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
Affected asset	api.meridianbank.example:443
Status	triaged
Reported by	AXUM SEC Red Team
Reported on	28 October 2026

DESCRIPTION

The public API endpoint still negotiates TLS 1.0 and 1.1 and offers cipher suites without forward secrecy (including 3DES, which is exposed to SWEET32).

IMPACT

A network attacker able to observe traffic can, under specific conditions, downgrade or recover session data. This also fails PCI DSS requirements for strong cryptography.

EVIDENCE AND REPRODUCTION

Protocol and cipher enumeration with testssl.sh shows TLS 1 and TLS 1.1 offered and three weak TLS 1.2 suites (attached).

RECOMMENDED REMEDIATION

- Disable TLS 1.0 and 1.1; offer TLS 1.2 and 1.3 only.
- Remove CBC, 3DES and non-forward-secret suites; prefer ECDHE with AES-GCM or ChaCha20.
- Enable HSTS with a long max-age after confirming client compatibility.

EVIDENCE



tls-configuration.png — testssl.sh protocol and cipher results

REFERENCES

- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/01-Testing_for_Weak_Transport_Layer_Security

5.8 No rate limiting on one-time-password verification

CVSS 5.3 | CWE-307 | MEDIUM

Finding ID	AXR-0147-008
OWASP category	A07:2021 Identification and Authentication Failures
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Affected asset	POST /api/v2/auth/otp/verify
Status	triaged
Reported by	AXUM SEC Red Team
Reported on	06 November 2026

DESCRIPTION

The six-digit SMS code can be submitted without a limit on attempts or a lock-out. Roughly 1 in 10^6 guesses succeeds, and the code stays valid for ten minutes.

IMPACT

An attacker who knows a customer's username and password can brute-force the second factor within its validity window.

EVIDENCE AND REPRODUCTION

Sustained 1,200 verification attempts in 60 seconds against a test account without throttling or lock-out.

RECOMMENDED REMEDIATION

- Limit verification attempts per account and per source (for example five tries, then lock for 15 minutes).
- Invalidate the code after repeated failures and notify the customer.
- Shorten code validity and add device binding.

REFERENCES

- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/03-Testing_for_Weak_Lock_Out_Mechanism

5.9 Verbose error responses disclose stack traces and internal hostnames

CVSS 4.3 | CWE-209 | LOW

Finding ID	AXR-0147-009
OWASP category	A05:2021 Security Misconfiguration
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
Affected asset	POST /api/v2/transactions/export
Status	triaged
Reported by	AXUM SEC Red Team
Reported on	07 November 2026

DESCRIPTION

Malformed requests to several endpoints return a full stack trace with source file paths, framework versions and internal service hostnames.

IMPACT

The detail shortens an attacker's reconnaissance and helps tailor exploits to the exact framework and topology.

EVIDENCE AND REPRODUCTION

Send an export request with an invalid date range: the `500` response body contains the trace and `db-primary.internal.meridian`.

RECOMMENDED REMEDIATION

- Return a generic error with a correlation identifier to the client and log the detail server-side.
- Run production with the framework's error detail disabled.

REFERENCES

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

5.10 Missing security headers: CSP, X-Content-Type-Options, Referrer-Policy

CVSS 3.7 | CWE-693 | LOW

Finding ID	AXR-0147-010
OWASP category	A05:2021 Security Misconfiguration
CVSS vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N
Affected asset	https://app.meridianbank.example
Status	triaged
Reported by	AXUM SEC Red Team
Reported on	28 October 2026

DESCRIPTION

Responses from the web application carry no Content-Security-Policy, `X-Content-Type-Options` or `Referrer-Policy`, and `X-Frame-Options` is inconsistent between pages.

IMPACT

Defence in depth only, but the missing CSP is what allows the reflected XSS in AXR-0147-006 to execute inline script.

EVIDENCE AND REPRODUCTION

Header review of the landing, login and dashboard responses.

RECOMMENDED REMEDIATION

- Add a strict CSP (no `unsafe-inline`), `X-Content-Type-Options: nosniff`, `Referrer-Policy: strict-origin-when-cross-origin` and `frame-ancestors 'none'`.
- Apply the headers at the edge so every route inherits them.

REFERENCES

- https://owasp.org/www-project-secure-headers/

5.11 Outdated jQuery 3.3.1 with published advisories (no exploitable path found)

CWE-1104 | INFO

Finding ID	AXR-0147-011
OWASP category	A06:2021 Vulnerable and Outdated Components
Affected asset	https://app.meridianbank.example/static/vendor/jquery-3.3.1.min.js
Status	triaged
Reported by	AXUM SEC Red Team
Reported on	28 October 2026

DESCRIPTION

The web application bundles jQuery 3.3.1, which has published prototype-pollution and XSS advisories. No exploitable path to these issues was found in the way the application uses the library.

IMPACT

No direct impact was demonstrated. The component should be kept current so that a future change does not make an advisory exploitable.

RECOMMENDED REMEDIATION

- Upgrade to a supported jQuery release and add dependency scanning to the build.

REFERENCES

- https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

6 Remediation plan

Findings are grouped by the time within which they should be fixed. The table below restates the recommendation recorded against each finding.

Immediate
within 7 days

1

- Unauthenticated internal API exposes customer KYC records **FIXED**

Short term
within 30 days

3

- Broken object-level authorization on account statements (IDOR) **FIXED**
- SQL injection in transaction search filter **FIXED**
- Refresh endpoint accepts JWTs with the "none" algorithm

Planned
within 90 days

4

- Profile API returns more personal data than the client displays
- Reflected cross-site scripting in the transfer receipt page
- Weak TLS configuration: TLS 1.0/1.1 and CBC / 3DES suites enabled
- No rate limiting on one-time-password verification

Hardening
next maintenance cycle

3

- Verbose error responses disclose stack traces and internal hostnames
- Missing security headers: CSP, X-Content-Type-Options, Referrer-Policy
- Outdated jQuery 3.3.1 with published advisories (no exploitable path found)

#	FINDING	SEVERITY	WEAKNESS	REMEDIATION
1	Unauthenticated internal API exposes customer KYC records	CRITICAL	CWE-306	Remove the /internal route group from the public listener immediately, or block it at the load balancer.
2	Broken object-level authorization on account statements (IDOR)	HIGH	CWE-639	Resolve the account from the token subject and verify ownership on the server for every request; never trust the identifier in the path alone.
3	SQL injection in transaction search filter	HIGH	CWE-89	Use parameterised queries or the ORM's bound parameters for every filter; never build SQL from request fields.
4	Refresh endpoint accepts JWTs with the "none" algorithm	HIGH	CWE-347	Pin the expected algorithm (RS256) in the verifier and reject any other value, including none.
5	Profile API returns more personal data than the client displays	MEDIUM	CWE-213	Return only the fields each client needs (an explicit response schema per endpoint).
6	Reflected cross-site scripting in the transfer receipt page	MEDIUM	CWE-79	Encode all output for its context (HTML, attribute, JavaScript) using the framework's templating, not string concatenation.
7	Weak TLS configuration: TLS 1.0/1.1 and CBC / 3DES suites enabled	MEDIUM	CWE-326	Disable TLS 1.0 and 1.1; offer TLS 1.2 and 1.3 only.

#	FINDING	SEVERITY	WEAKNESS	REMEDIATION
8	No rate limiting on one-time-password verification	MEDIUM	CWE-307	Limit verification attempts per account and per source (for example five tries, then lock for 15 minutes).
9	Verbose error responses disclose stack traces and internal hostnames	LOW	CWE-209	Return a generic error with a correlation identifier to the client and log the detail server-side.
10	Missing security headers: CSP, X-Content-Type-Options, Referrer-Policy	LOW	CWE-693	Add a strict CSP (no unsafe-inline), X-Content-Type-Options: nosniff, Referrer-Policy: strict-origin-when-cross-origin and frame-ancestors 'none'.
11	Outdated jQuery 3.3.1 with published advisories (no exploitable path found)	INFO	CWE-1104	Upgrade to a supported jQuery release and add dependency scanning to the build.

7 Standards alignment

Each finding mapped to the control references a reviewer or auditor is likely to ask about. The mapping is advisory: it points to the relevant requirement, it does not assert compliance.

FINDING	OWASP TOP 10	PCI DSS V4.0	ISO/IEC 27001:2022
Unauthenticated internal API exposes customer KYC records	A01:2021	Req. 7.2, 8.2	A.8.3, A.5.15
Broken object-level authorization on account statements (IDOR)	A01:2021	Req. 7.2	A.8.3
SQL injection in transaction search filter	A03:2021	Req. 6.2.4	A.8.28
Refresh endpoint accepts JWTs with the "none" algorithm	A07:2021	Req. 8.3, 8.6	A.8.5
Profile API returns more personal data than the client displays	A01:2021	Req. 3.4	A.8.11
Reflected cross-site scripting in the transfer receipt page	A03:2021	Req. 6.2.4	A.8.28
Weak TLS configuration: TLS 1.0/1.1 and CBC / 3DES suites enabled	A02:2021	Req. 4.2.1	A.8.24
No rate limiting on one-time-password verification	A07:2021	Req. 8.3.4	A.8.5
Verbose error responses disclose stack traces and internal hostnames	A05:2021	Req. 6.2.4	A.8.9
Missing security headers: CSP, X-Content-Type-Options, Referrer-Policy	A05:2021	Req. 6.4.1	A.8.9

FINDING	OWASP TOP 10	PCI DSS V4.0	ISO/IEC 27001:2022
Outdated jQuery 3.3.1 with published advisories (no exploitable path found)	A06:2021	Req. 6.3.2	A.8.8

8 Document sign-off

Hana Tesfaye
Lead consultant, AXUM SEC
PREPARED BY · 24 NOVEMBER 2026

Dawit Girma
Head of Offensive Security, AXUM SEC
TECHNICAL REVIEW · 24 NOVEMBER 2026

Meron Haile
Director, AXUM SEC
APPROVED FOR RELEASE · 25 NOVEMBER 2026

Issued by AXUM SEC. This document is confidential and intended for the named recipient only. Findings reflect the state of the in-scope systems during the testing window; they are not a guarantee of the absence of other vulnerabilities.

9 Appendix A — Rating definitions

SEVERITY	CVSS V3.1	MEANING AND EXPECTED RESPONSE
CRITICAL	9.0 – 10.0	Exploitable without preconditions, with direct impact on confidentiality, integrity or availability of production systems or customer data. Remediate immediately.
HIGH	7.0 – 8.9	Exploitable in realistic conditions with material impact. Remediate in the current release cycle.
MEDIUM	4.0 – 6.9	Requires specific conditions or has limited impact. Schedule within the next planned release.
LOW	0.1 – 3.9	Defence-in-depth or hardening item with limited direct impact. Address as part of routine maintenance.
INFO	0.0	An observation with no direct security impact, recorded for awareness.

Severity is assigned by the triager against this scale. Where a CVSS vector is recorded it is shown with the finding, but the severity rating is the one that governs remediation priority.

10 Appendix B — Glossary

TERM	MEANING
CVSS	Common Vulnerability Scoring System. A 0-10 score of the technical severity of a vulnerability.
CWE	Common Weakness Enumeration. A catalogue of software weakness types.
IDOR / BOLA	Insecure Direct Object Reference / Broken Object Level Authorization: reading or changing another user's record by changing an identifier.
XSS	Cross-site scripting: attacker-controlled script running in another user's browser.

TERM	MEANING
SQL injection	Attacker-controlled input changing the meaning of a database query.
JWT	JSON Web Token, a signed token used to carry a session or identity between systems.
MFA	Multi-factor authentication: a second proof of identity beyond a password.
PoC	Proof of concept: the minimum demonstration that a weakness is exploitable.
Retest	A repeat of the original exploit after the client reports a fix, to confirm the weakness is closed.