AuditGate
API SECURITY PLATFORM

SECURITY ASSESSMENT REPORT

Payments API

API Security Assessment Report

Prepared for	Sample Fintech Ltd
Prepared by	AuditGate (Zynterra Innovations Limited)
Target	`https://api.samplefintech.ng/v1` (Production)
Report date	2 October 2026
Reference	AG-20261002-001, version 1
Classification	**Confidential**

This document contains security-sensitive information about Sample Fintech Ltd. Do not distribute beyond the people listed in the distribution list.

Document control

Document details

Title	API Security Assessment Report: Payments API
Reference	AG-20261002-001
Version	1
Date issued	2 October 2026, 16:30 WAT
Classification	Confidential
Prepared by	AuditGate, automated assessment platform of Zynterra Innovations Limited
Prepared for	Sample Fintech Ltd
Valid until	1 November 2026 (shared link expiry)

Distribution

Recipient	Organisation	Purpose
Workspace owner and security contacts	Sample Fintech Ltd	Remediation and record keeping

Contents

1. Executive summary

2. Scope and approach

3. Risk rating

4. Summary of findings

5. Detailed findings

6. Remediation plan

Appendices

1. Executive summary

Overall risk	**Critical** (set by the most severe open finding)
Findings	6 findings, 5 open
Health score	58 / 100 (up 9 from 49)

1.1 Summary

The assessment identified six findings in Payments API, one of them critical. The onboarding endpoint returns full Bank Verification Numbers to the client, and a transaction lookup endpoint responds without authentication. These two issues expose regulated customer data and should be fixed before the next release.

The remaining findings concern configuration: missing browser security headers, a CORS policy that reflects the request origin, and a header that reveals the server framework. A database password committed to the repository has already been removed.

1.2 Findings by severity

Severity	Found	Open	Resolved
Critical	1	1	0
High	2	2	0
Medium	2	1	1
Low	1	1	0
Info	0	0	0
Total	**6**	**5**	**1**

1.3 Key recommendations

1. Address the data exposure issues (F-01), highest severity Critical, within 24 hours.
2. Address the broken authentication issues (F-02), highest severity High, within 7 days.
3. Address the security misconfiguration issues (F-03, F-04), highest severity High, within 7 days.
4. Address the information disclosure issues (F-06), highest severity Low, within 90 days.

2. Scope and approach

2.1 Scope

Application	Payments API
Target	`https://api.samplefintech.ng/v1`
Environment	Production
Testing performed	Passive monitoring + active scan
Period covered	20 September 2026 to 2 October 2026

2.2 Approach

AuditGate tested the target using the methods below. Findings from all methods are merged, so the same issue seen several times appears once with an occurrence count.

- **Passive traffic analysis.** Requests and responses sent through the AuditGate proxy are checked for data exposure, missing authentication, weak headers and abnormal behaviour. No traffic is altered or blocked.
- **Active scanning.** Controlled requests are sent to the target to confirm authorisation, input handling, transport security and configuration issues. Only safe, non-destructive test cases are used.
- **Source and configuration review.** When a repository is connected, code and infrastructure files are reviewed for hard-coded secrets, injection risks and insecure settings, following call paths across files.

Test results are mapped to the OWASP API Security Top 10 (2023) and to CWE identifiers. Sensitive values in evidence, such as tokens, BVNs and personal data, are masked before storage and in this report.

2.3 Limitations

- This is an automated assessment. It does not replace a manual penetration test, especially for business logic flaws.
- Authenticated testing depends on the test accounts provided. Areas those accounts cannot reach were not tested.
- Results reflect the state of the target during the period above. Changes made since then are not covered.
- Findings marked *Needs verification* were detected by pattern and should be confirmed by your team.

3. Risk rating

Each finding is rated by its likely impact and how easily it could be exploited. The remediation target is counted from the date the finding was first detected.

Severity	Meaning	Fix within
Critical	Can be exploited easily and remotely, leading to data breach, account takeover or financial loss.	24 hours
High	Serious weakness that an attacker can exploit with little effort or that exposes sensitive data.	7 days
Medium	Weakness that needs specific conditions to exploit, or that makes other attacks easier.	30 days
Low	Minor weakness or missing hardening with limited direct impact.	90 days
Info	Observation or best-practice gap with no direct security impact.	180 days

Confidence

Level	Meaning
Confirmed	Reproduced with a test request or observed directly in traffic.
Probable	Strong evidence in code or traffic, not yet reproduced.
Needs verification	Matches a known pattern. Review before acting.

4. Summary of findings

Most severe first. Findings your team marked as false positives are excluded.

ID	Finding	Severity	Status	Target date
F-01	Bank Verification Number (BVN) exposed on POST /onboarding/complete `POST /onboarding/complete`	Critical	Open	**Overdue** (29 Sept 2026)
F-02	GET /transactions/public/:id responds 200 without authentication `GET /transactions/public/:id`	High	Open	7 Oct 2026
F-03	5 security header issues detected (first observed on GET /) `GET /`	High	Acknowledged	**Overdue** (2 Oct 2026)
F-04	CORS policy may reflect the request Origin on GET /onboarding `GET /onboarding`	Medium	Open	29 Oct 2026
F-05	Plaintext secret in docker-compose.yml `IAC docker-compose.yml`	Medium	Resolved	Resolved
F-06	Server technology header leaking version information on OPTIONS / `OPTIONS /`	Low	Open	25 Dec 2026

5. Detailed findings

F-01. Bank Verification Number (BVN) exposed on POST /onboarding/complete

Severity	■ **Critical**
Status	Open
Confidence	Confirmed
Category	Data exposure
Affected	`POST /onboarding/complete` Also: `GET /customers/me`
Code location	`src/onboarding/onboarding.controller.ts (complete)`
OWASP API Top 10	API3:2023 Broken Object Property Level Authorization
CWE	CWE-359, CWE-213
First detected	28 Sept 2026, seen 37 times
Target date	**Overdue** (29 Sept 2026)

Description

A full Bank Verification Number was returned in the response body to a client that only needed a confirmation. BVNs are regulated identifiers under the NDPA and can be used for identity fraud.

Impact

Anyone who can observe or replay this response can harvest BVNs for account takeover and loan fraud.

Evidence

Sensitive values are masked.

Found in	Response body
Field	bvn
Masked BVN	22*******45
Matches	1
Records affected	1
Response status	201

Recommendation

The onboarding response serialises the whole customer record, including the BVN.

1. Return a response DTO that whitelists only id, status and nextStep.
2. Mask BVNs at the serializer layer so no endpoint can return them in full.
3. Add a contract test that fails if a response body contains an 11-digit BVN.

Example

```
@Exclude()
bvn: string;

return plainToInstance(OnboardingResult, customer, {
  excludeExtraneousValues: true,
});
```

To prevent this in future

- Serialise responses through explicit DTOs, never whole database records.

References

- https://cwe.mitre.org/data/definitions/359.html
- https://owasp.org/API-Security/editions/2023/en/0xa3-broken-object-property-level-authorization/

F-02. GET /transactions/public/:id responds 200 without authentication

Severity	■ **High**
Status	Open
Confidence	Needs verification
Category	Broken authentication
Affected	`GET /transactions/public/:id`
OWASP API Top 10	API2:2023 Broken Authentication
CWE	CWE-306
First detected	30 Sept 2026, seen 12 times
Target date	7 Oct 2026

Description

The endpoint returned transaction details to a request that carried no session, token or API key.

Evidence

Sensitive values are masked.

Response status	200
Authentication checked for	authorization header, session cookie, x-api-key header

Steps to reproduce

1. Send the request with no Authorization header, cookie or API key.

   ```
   curl -i https://api.samplefintech.ng/v1/transactions/public/ZRV-2TYD9M
   ```

2. The API answers 200 with the transaction amount, sender and recipient.

> **Verification note.** A guard applied globally or at module level can leave a genuinely protected route looking unguarded in source.

F-03. 5 security header issues detected (first observed on GET /)

Severity	■ **High**
Status	Acknowledged
Category	Security misconfiguration
Affected	`GET /`
OWASP API Top 10	API8:2023 Security Misconfiguration
First detected	25 Sept 2026, seen 1,204 times
Target date	**Overdue** (2 Oct 2026)

Description

Responses are missing browser security headers that defend against clickjacking, MIME sniffing and protocol downgrade.

Impact

Pages can be framed and downgraded to HTTP.

Evidence

Sensitive values are masked.

Headers

Header	Note	Severity
Content-Security-Policy	missing entirely	High
Strict-Transport-Security	missing in production	High
X-Content-Type-Options	missing	Medium
X-Frame-Options	missing	Medium
Referrer-Policy	missing	Low

> **Verification note.** A CDN or reverse proxy that injects these headers after the origin responds makes the origin look bare here while browsers still receive them.

Recommendation

Add Helmet to the HTTP pipeline.

1. Install helmet.
2. Register app.use(helmet()) before routes.
3. Set HSTS with a one-year max-age in production.

F-04. CORS policy may reflect the request Origin on GET /onboarding

Severity	■ **Medium**
Status	Open
Category	Security misconfiguration
Affected	`GET /onboarding`
OWASP API Top 10	API8:2023 Security Misconfiguration
First detected	29 Sept 2026, seen 3 times
Target date	29 Oct 2026

Description

The API echoed the caller's Origin header back in Access-Control-Allow-Origin with credentials allowed.

Evidence

Sensitive values are masked.

Origin sent	https://app-staging.example.ng
Access-Control-Allow-Origin	https://app-staging.example.ng
Access-Control-Allow-Credentials	true
Vary	Origin, Accept-Encoding
Reflection confirmed	No

F-05. Plaintext secret in docker-compose.yml

Severity	■ **Medium**
Status	Resolved
Category	Secrets
Affected	`IAC docker-compose.yml`
OWASP API Top 10	API8:2023 Security Misconfiguration
First detected	20 Sept 2026
Target date	Resolved

Description

A database password is committed in plain text in the compose file.

Evidence

Sensitive values are masked.

File	docker-compose.yml
Line	10
Variable	POSTGRES_PASSWORD

F-06. Server technology header leaking version information on OPTIONS /

Severity	■ **Low**
Status	Open
Category	Information disclosure
Affected	`OPTIONS /`
First detected	26 Sept 2026, seen 410 times
Target date	25 Dec 2026

Description

The X-Powered-By header advertises the server framework.

Evidence

Sensitive values are masked.

Headers revealing the stack	`x-powered-by`: Express

6. Remediation plan

Open findings in recommended order. The owner column is left blank for your team to assign. Re-scan after each fix to confirm it.

ID	Finding	Severity	Target date	Owner
F-01	Bank Verification Number (BVN) exposed on POST /onboarding/complete	Critical	Overdue (29 Sept 2026)	
F-02	GET /transactions/public/:id responds 200 without authentication	High	7 Oct 2026	
F-03	5 security header issues detected (first observed on GET /)	High	Overdue (2 Oct 2026)	
F-04	CORS policy may reflect the request Origin on GET /onboarding	Medium	29 Oct 2026	
F-06	Server technology header leaking version information on OPTIONS /	Low	25 Dec 2026	

Appendices

A. Health score

The health score is a quick indicator for tracking progress between reports. Every project starts at 100, and open findings and poor traffic health deduct points.

Reason	Count	Points each	Deducted
Critical findings	1	20	20
High findings	2	10	20
Medium findings	1	2	2
Score (100 minus 42)			**58**

B. Endpoint performance

Traffic observed through the AuditGate proxy over the last 30 days. Frequent server errors or slow responses can point to weak error handling.

Endpoint	Requests	5xx errors	p99 latency	Last status
`POST /onboarding/complete`	18,432	0	640 ms	201
`GET /transactions/public/:id`	7,291	12	2,410 ms	500
`GET /onboarding`	30,122	0	180 ms	200

C. Disclaimer

This report was produced by AuditGate, an automated security testing service operated by Zynterra Innovations Limited. It reflects automated testing during the period stated and is not an exhaustive assessment or a certification of compliance with any standard. The findings are provided to help Sample Fintech Ltd reduce risk. Zynterra Innovations Limited accepts no liability for actions taken or not taken on the basis of this report.