Penetration Test Report

Web Application & External Infrastructure · Sample (redacted) · Prepared by Vanorika Technologies

Client	[REDACTED] · Harare, Zimbabwe
Engagement	External web application penetration test
Scope	1 primary web app, 2 subdomains, public infrastructure
Method	OWASP-aligned, manual + automated, authenticated & unauthenticated
Tester	Donovan Mudarikwa · CompTIA PenTest+

Executive summary

Vanorika Technologies assessed the in-scope web application and public infrastructure for security weaknesses. The testing identified **one Critical** and several lower-severity issues that, combined, would let an attacker access data they should not. All Critical and High findings were reported to the client during testing and remediated before this report was finalised. Risk ratings reflect business impact and ease of exploitation, not just technical severity.

Findings at a glance

#	Severity	Finding
1	CRITICAL	Authentication bypass on an unprotected API endpoint
2	HIGH	Broken access control — horizontal privilege escalation
3	MEDIUM	Outdated CMS component with a known CVE
4	MEDIUM	Missing security headers (CSP, HSTS)
5	LOW	Verbose error messages leak internal paths

Detailed findings

CRITICAL — Authentication bypass on an unprotected API endpoint

Reference: VAN-2026-01

Description

An internal API endpoint returning customer records was reachable without any authentication token. Requesting the endpoint directly returned full records belonging to other users.

Business impact

An attacker could enumerate and exfiltrate the entire customer database — names, contact details and order history — leading to a reportable data breach under the Data Protection Act (2021).

Evidence (redacted)

```
GET /api/v1/customers/ → 200 OK (no Authorization header) [response body redacted]
```

Remediation

Enforce authentication and object-level authorisation on every API route; deny by default. Add server-side checks that the requesting user owns the records being returned.

HIGH — Broken access control — horizontal privilege escalation

Reference: VAN-2026-02

Description

By changing a numeric identifier in a request, a logged-in user could view and modify another user's account.

Business impact

Any customer could tamper with other customers' data, undermining trust and integrity of the platform.

Evidence (redacted)

```
POST /account/update {"user_id": } → 200 OK
```

Remediation

Validate ownership of every referenced object server-side; use non-guessable identifiers; log access anomalies.