# The State of Zimbabwe Web Security 2026

What we found assessing 17 Harare businesses across 5 sectors — and what every Zimbabwean business owner should take from it.

| 17 | 5 | 16/17 | 57 |
|---|---|---|---|
| Businesses assessed | Sectors covered | Had a fixable vuln | Findings logged |

We ran passive, no-touch assessments — no logins, no port scanning, nothing intrusive. Everything below comes from publicly available information any attacker could see.

## What we found

**15 of 17** (88%) Missing critical security headers

**12 of 17** (71%) No privacy policy (DPA 2021 gap)

**11 of 17** (65%) Outdated software / CMS / plugins

**8 of 17** (47%) No HTTPS redirect / weak TLS

**7 of 17** (41%) No SPF/DMARC — email spoofable

**4 of 17** (24%) Exposed admin panel / endpoint

## Sectors assessed

Hospitality · Healthcare · Law firms · Schools · NGOs

## What to do about it

- Add the core security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options).
- Update your CMS, plugins and server software — and keep them updated.
- Publish a privacy policy and force HTTP to redirect to HTTPS.
- Set SPF and DMARC so no one can spoof email from your domain.
- Get a free passive assessment so you know exactly where you stand.