APPLICATION SECURITY · FIELD NOTES

OWASP Top 10 for Kenyan Web Applications

> *“Most Kenyan businesses discover a security problem the same way: a customer reports something strange, a payment fails oddly, or a partner's compliance team asks a question nobody can answer.”*

This dossier is a practical field-notes walkthrough of the OWASP Top 10, grounded in the vulnerability classes most often seen assessing web and API applications built and deployed in Kenya's SME, startup, and NGO sector — not a generic restatement of the OWASP wiki.

Scope	Web Applications & APIs
Method	OWASP Top 10 (2021) baseline, human-verified findings
Focus Market	Kenyan SMEs, Startups & NGOs
Analyst	Nazline Mwita, Cybersecurity Assurance Lead, HarLyn Digital Partners

1. Severity Snapshot

Across authorized assessments of web and API applications serving the Kenyan market, six OWASP categories account for the overwhelming majority of exploitable findings.

2. Broken Access Control

The single most common finding: an authenticated user can act on another tenant's data by changing an ID in the URL or request body (Broken Object-Level Authorization / IDOR). Multi-tenant SaaS products built quickly under deadline pressure are especially exposed — authentication is implemented, but per-object authorization checks are not.

> **Security Principle**
>
> **Being logged in is not the same as being authorized for this specific record.**

3. Injection

SQL, NoSQL, and command injection remain common where raw user input reaches a query or shell call without parameterization — frequently in admin/internal tooling that was never expected to face untrusted input, then later exposed via an API gateway.

4. Security Misconfiguration

Verbose stack traces in production, default credentials left on staging environments that are reachable from the public internet, and open admin paths (`/admin`, `/.env`) discoverable by any scanner.

5. Authentication Failures

Weak password-reset flows (predictable tokens, no rate limiting) and session tokens that don't expire or rotate on privilege change.

6. Logging & Monitoring Failures

The quiet one: many organizations only discover they were compromised weeks later, via a third party, because no tamper-evident audit trail existed to answer “what happened, and when?”

7. What This Means Under KDPA

Several of these categories create direct statutory exposure under the Kenya Data Protection Act when personal data is involved — broken access control and injection both create a plausible path to a reportable data breach, not just a technical finding.

OWASP Category	KDPA Relevance
Broken Access Control	Direct risk of unauthorized personal data access
Injection	Risk of bulk data exposure/exfiltration
Security Misconfiguration	Increases attack surface for the above
Auth Failures	Account takeover -> unauthorized data access
Logging Failures	Breach cannot be scoped or reported accurately

---

Related Service

This dossier supports the Authorized Web & API Security Assessment and Security Audits services — permission-based, human-verified findings with KDPA exposure mapping.

Nazline Mwita, CompTIA Security+ certified Cybersecurity Assurance Lead and Co-Founder at HarLyn Digital Partners. Specializing in authorized web & API security assessments, KDPA compliance reviews, and defensive cloud architecture in Nairobi, Kenya.