CyberDudeBivash QuickScan™ Report

Version 1.2.1 · Website Security Auditor

Executive Summary

QuickScan raised **11** indicator(s) for review across 4 categor(y/ies). Confirm each indicator manually before treating it as a finding.

Assessment Scope

QuickScan tests four categories only: reflected-XSS indicators, SQL-error indicators, open-redirect behavior, and exposed sensitive files. It performs unauthenticated, non-destructive GET probes against the single target below. It does not test authenticated flows, DOM/stored/second-order issues, or business logic.

Scan Metadata

Target: http://demo-fixture.local/ (controlled local fixture)
Scan date (UTC): 2026-09-23T16:30:26+00:00
Requests made: 25
QuickScan version: 1.2.1

Findings Summary

Category	Indicators
XSS	3
SQLi	4
Open Redirect	3
Exposed Files	1

XSS — 3 indicator(s)

Severity	Type	URL	Evidence
High	Reflected XSS (indicator)	http://demo-fixture.local/?q=%3Cscript%3Ealert%28%27QuickScanXSS%27%29%3C%2Fscript%3E	Exact payload reflected unencoded in the respo
High	Reflected XSS (indicator)	http://demo-fixture.local/?q=%27%3E%3Cimg%20src%3Dx%20onerror%3Dalert%281%29%3E	Exact payload reflected unencoded in the respo
High	Reflected XSS (indicator)	http://demo-fixture.local/?q=%22%3E%3Csvg%20onload%3Dalert%281%29%3E	Exact payload reflected unencoded in the respo

Remediation: Context-encode all user input on output; set a strict Content-Security-Policy.

SQLi — 4 indicator(s)

Severity	Type	URL	Evidence
Critical	SQL error disclosure (indicator)	http://demo-fixture.local/?id=%27	Database error string surfaced: 'you have an err

Critical	SQL error disclosure (indicator)	http://demo-fixture.local/?id=%27%20OR%20%271%27%3D%271	Database error string surfaced: 'you have an err
Critical	SQL error disclosure (indicator)	http://demo-fixture.local/?id=1%27%20UNION%20SELECT%20NULL--%20	Database error string surfaced: 'you have an err
Critical	SQL error disclosure (indicator)	http://demo-fixture.local/?id=admin%27--%20-	Database error string surfaced: 'you have an err

Remediation: Use parameterized queries / prepared statements; never build SQL by string concatenation; disable verbose DB errors in production.

Open Redirect — 3 indicator(s)

Severity	Type	URL	Evidence
Medium	Open Redirect (indicator)	http://demo-fixture.local/redirect?url=%2F%2Fexample.net	3xx redirect Location points off-site: '//example.c
Medium	Open Redirect (indicator)	http://demo-fixture.local/redirect?url=https%3A%2F%2Fexample.net	3xx redirect Location points off-site: 'https://redir
Medium	Open Redirect (indicator)	http://demo-fixture.local/redirect?url=%2F%5Cexample.net	3xx redirect Location points off-site: '/\\redirect-p

Remediation: Validate redirect targets against an allowlist of known-safe paths/hosts.

Exposed Files — 1 indicator(s)

Severity	Type	URL	Evidence
High	Exposed Sensitive File	http://demo-fixture.local/.env	HTTP 200; Content-Type=text/plain; 37 bytes.

Remediation: Remove backups/dotfiles from the web root; deny access to sensitive paths at the server/CDN.

Methodology

Each category sends a small set of crafted, non-destructive GET requests and inspects the HTTP status, headers, and response body for a specific indicator (unencoded payload reflection, a database error string, an off-site 3xx Location, or a 200 on a known-sensitive path). Redirects are never followed.

Limitations

QuickScan raises *indicators*, not confirmed exploits, and covers only the four categories above. A clean result does not prove the target is secure. It does not perform authenticated testing, DOM/stored/second-order XSS, blind or time-based SQLi, WAF-bypass, or business-logic testing. Confirm every indicator manually and use a full DAST/manual assessment for broader coverage.