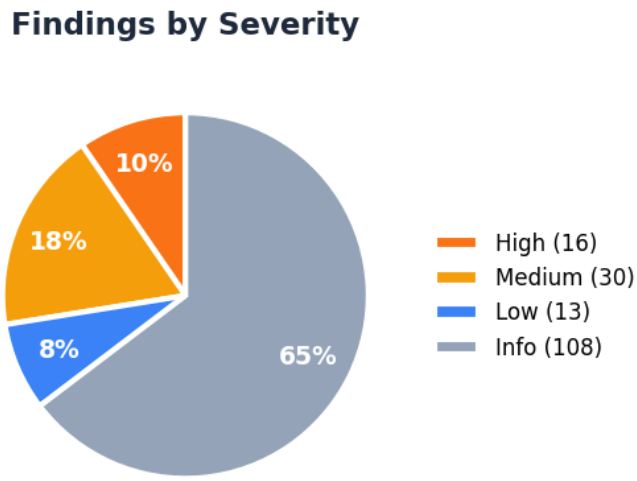
Glablla Coast

Executive Security Summary

Scope: Glablla Coast • Generated: February 16, 2026 at 14:13 UTC • 5 suppressed findings excluded



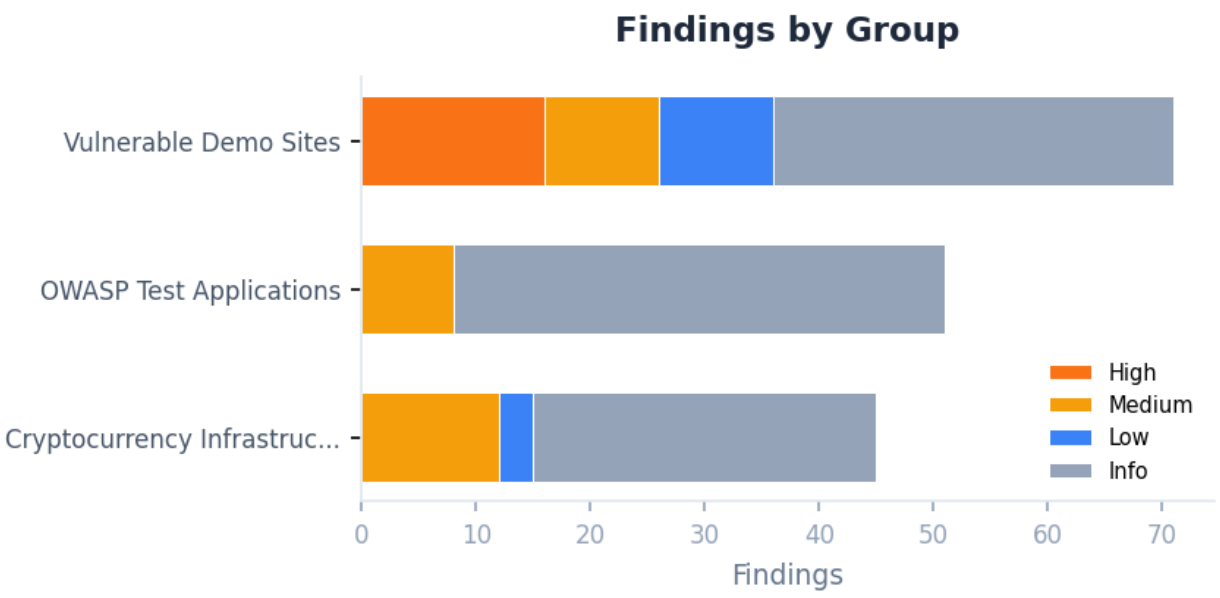
100.0	167	0	16	18
Exposure Score	Total Findings	Critical	High	Assets

Top Risks

Severity	Finding	Asset	Category
high	Outdated Php 5.6.40 on testphp.vulnweb.com	testphp.vulnweb.com	technology
high	SSL certificate hostname mismatch on demo.testfire.net:443	demo.testfire.net	ssl
high	Server header exposes version: Apache-Coyote/1.1	demo.testfire.net	headers

high	HTTP does not redirect to HTTPS on demo.testfire.net	demo.testfire.net	headers
high	Missing X-Frame-Options header on demo.testfire.net:443	demo.testfire.net	headers
high	No SPF record for demo.testfire.net	demo.testfire.net	dns
high	No DMARC record for demo.testfire.net	demo.testfire.net	dns

Risk by Group

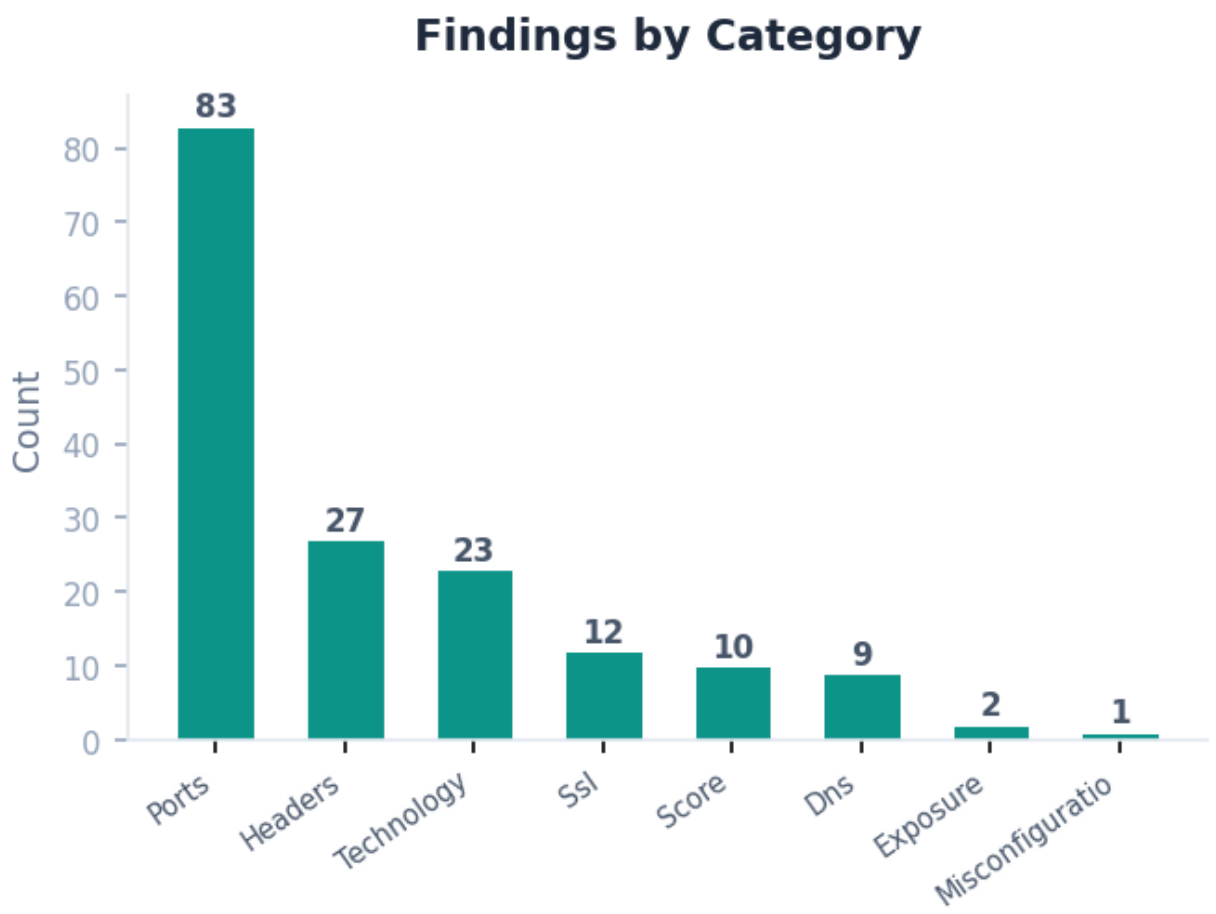


Group	Critical	High	Medium	Low	Total
Vulnerable Demo Sites	0	16	10	10	71
OWASP Test Applications	0	0	8	0	51
Cryptocurrency Infrastructure	0	0	12	3	45

Most Exposed Assets

Asset	Type	Critical	High	Total
demo.testfire.net	domain	0	15	56
etherscan.io	domain	0	0	8
coinbase.com	domain	0	0	29
webgoat.org	domain	0	0	28
owasp.org	domain	0	0	23

Findings by Category



Detection Coverage

Scan engines used: **cookie, cpe, dns, http, http_header, nuclei, orchestrator, shodan, ssl**

Total assets scanned: **18**