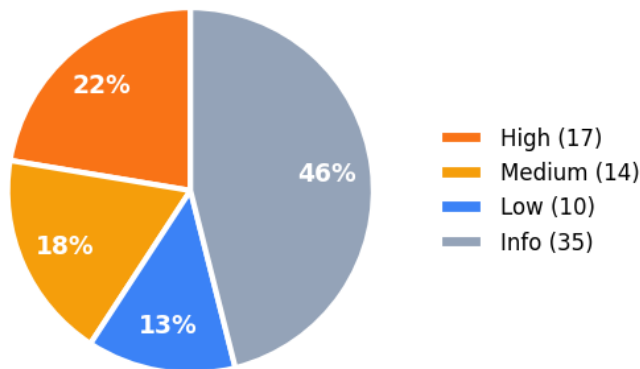


Executive Security Summary

Scope: Vulnerable Demo Sites • Generated: February 16, 2026 at 13:24 UTC



Findings by Severity



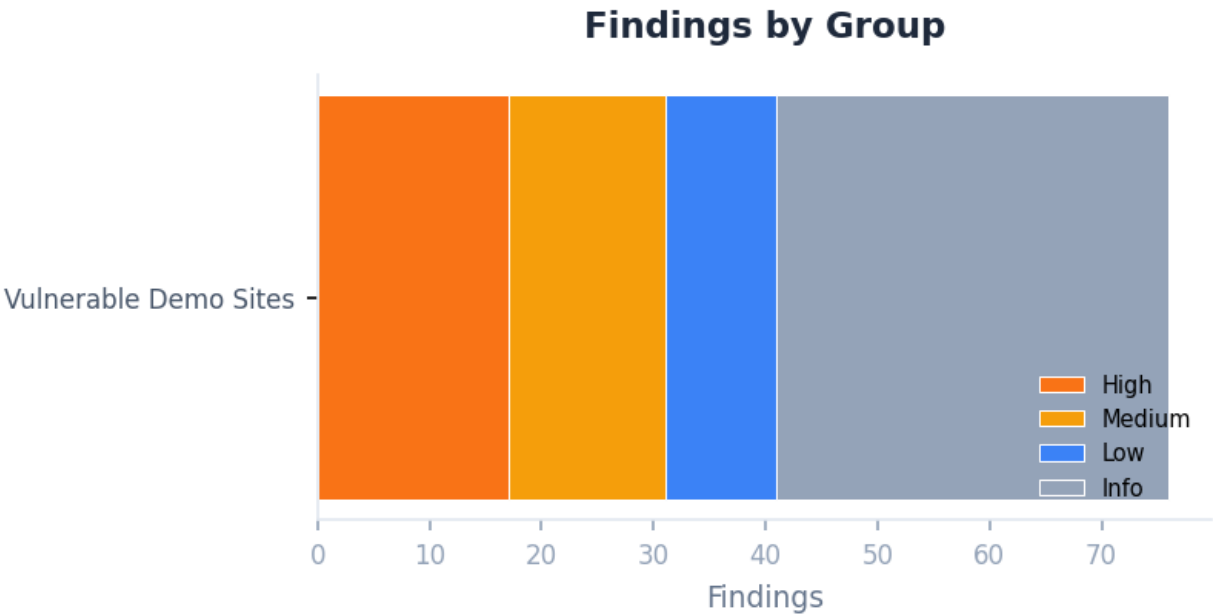
98.1	76	0	17	5
Exposure Score	Total Findings	Critical	High	Assets

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high	Outdated Php 5.6.40 on testphp.vulnweb.com	testphp.vulnweb.com	technology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

Risk by Group

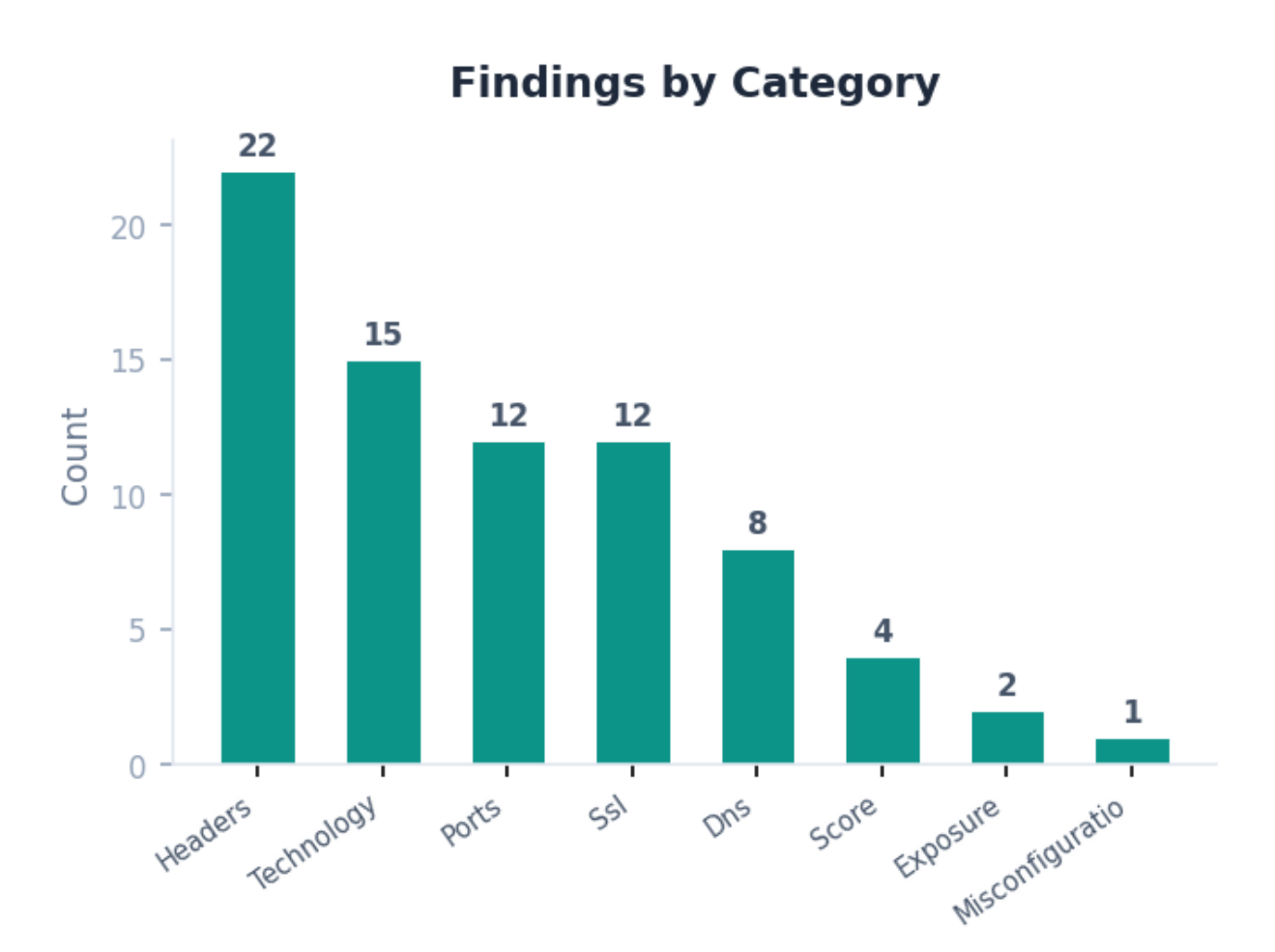


Group	Critical	High	Medium	Low	Total
Vulnerable Demo Sites	0	17	14	10	76

Most Exposed Assets

Asset	Type	Critical	High	Total
demo.testfire.net	domain	0	16	61
testphp.vulnweb.com	domain	0	1	5
scanme.nmap.org	domain	0	0	10

Findings by Category



Detection Coverage

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

Total assets scanned: **5**

Generated by XternSec • Glablla Coast • February 16, 2026 at 13:24 UTC
This is a confidential security report. Distribution should be limited to authorized personnel.