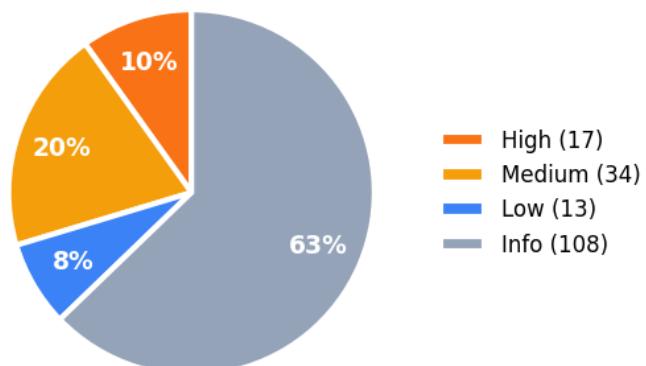


# Executive Security Summary

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



**Findings by Severity**



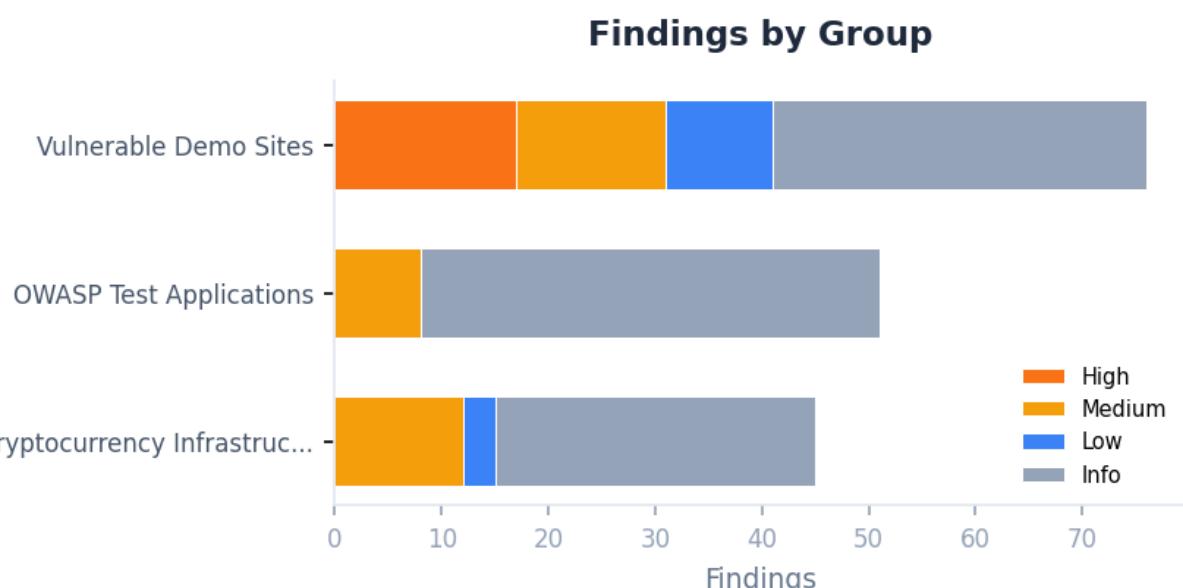
100.0	172	0	17	18
Exposure Score	Total Findings	Critical	High	Assets

## 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high	Outdated Php 5.6.40 on testphp.vulnweb.com	testphp.vulnweb.com	technology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

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

## Risk by Group



Group	Critical	High	Medium	Low	Total
Vulnerable Demo Sites	0	17	14	10	76
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	16	61
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

Findings by Category



## Detection Coverage

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

Total assets scanned: **18**

---

Generated by XternSec • Glablla Coast • February 16, 2026 at 14:13 UTC  
This is a confidential security report. Distribution should be limited to authorized personnel.