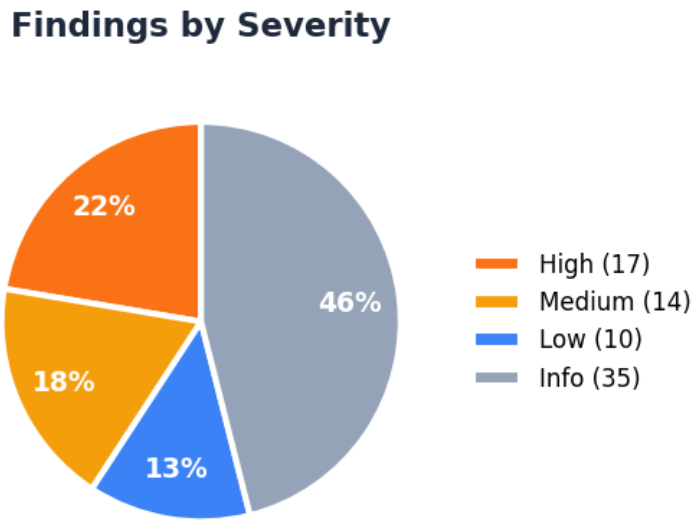
Glablla Coast

Technical Security Report

Scope: Vulnerable Demo Sites • Generated: February 16, 2026 at 13:48 UTC



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

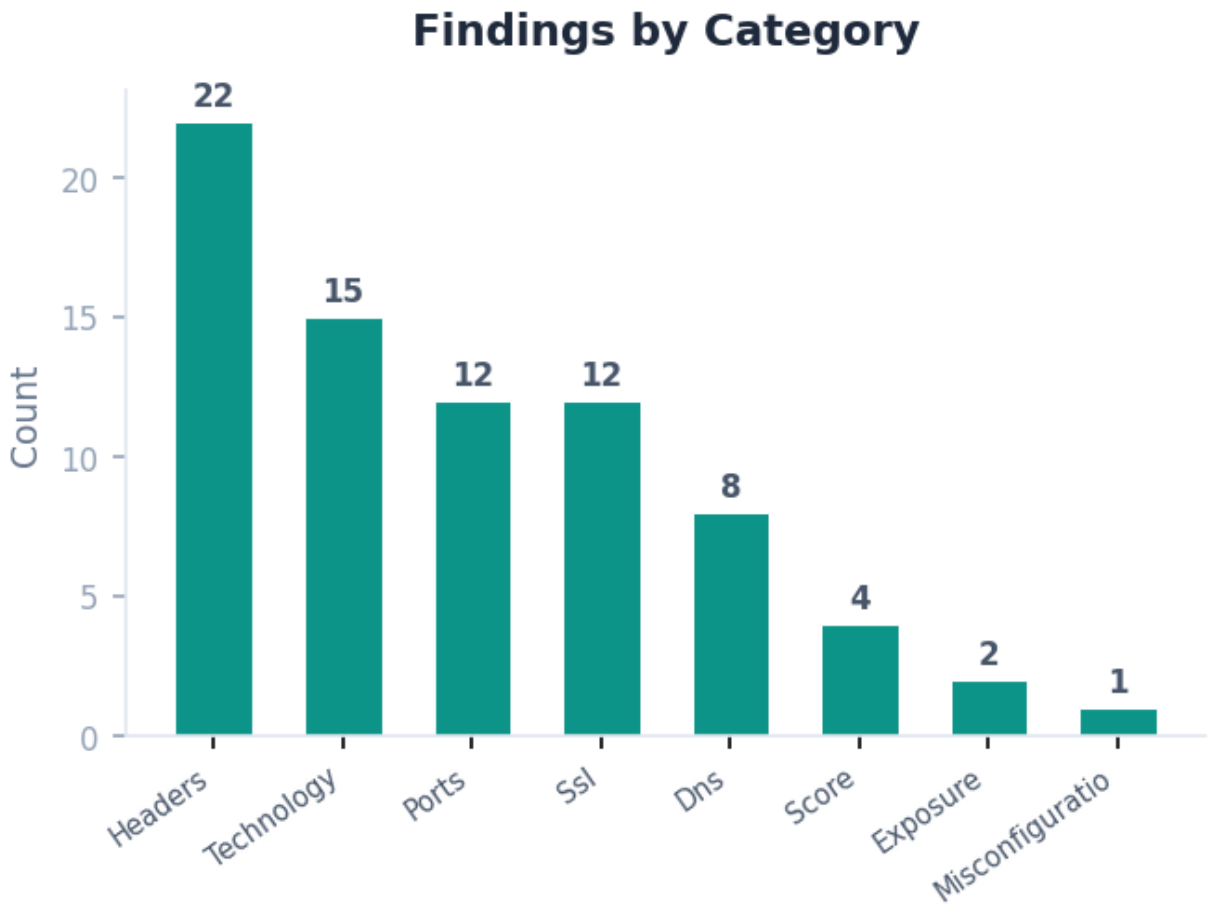
WHO — Team & Responsibility

Name	Email	Role
Desire Iradukunda	contactdesire04@gmail.com	Owner
David	iradudesire100@yahoo.fr	Analyst
Charles G	charles@domain.com	Admin
Jules	jules@homies.com	Viewer

Findings Ownership by Group

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

WHAT — Findings & Vulnerabilities



All Findings (45 total)

Sev	Finding	Asset	Group	Remediation
high	**Outdated Php 5.6.40 on testphp.vulnweb.com** CWE-1104 Php 5.6.40 is running on testphp.vulnweb.com. PHP 5.x is end-of-life since January 2019. No security patches. Outdated software may have unpatched sec	testphp.vulnweb.com technology	Vulnerable Demo Sites	Update Php to the latest supported version. Review the vendor's release notes for security fixes. Test the upgrade in a staging environment first.

high	**SSL certificate hostname mismatch on demo.testfire.net:443** CWE-297 The SSL certificate on demo.testfire.net:443 does not match the target hostname 'demo.testfire.net'. Certificate is issued to: CN=unknown, SANs=none.	demo.testfire.net ssl	Vulnerable Demo Sites	Reissue the SSL certificate to include 'demo.testfire.net' as the Common Name or a Subject Alternative Name (SAN).
high	**Server header exposes version: Apache-Coyote/1.1** CWE-200 The Server header reveals software and version: 'Apache-Coyote/1.1'. This information helps attackers identify known vulnerabilities for the specific	demo.testfire.net headers	Vulnerable Demo Sites	Remove or minimize the Server header. For nginx: server_tokens off; For Apache: ServerTokens Prod and ServerSignature Off
high	**HTTP does not redirect to HTTPS on demo.testfire.net** CWE-319 Accessing demo.testfire.net over HTTP (port 80) does not redirect to HTTPS. Users who type the URL without 'https://' will use an unencrypted connecti	demo.testfire.net headers	Vulnerable Demo Sites	Configure your web server to redirect all HTTP requests to HTTPS. For nginx: return 301 https://$host$request_uri; For Apache: RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=301,L]
high	**Missing X-Frame-Options header on demo.testfire.net:443** CWE-1021 The X-Frame-Options header is missing. This allows the page to be embedded in iframes on other sites, enabling clickjacking attacks where users are tr	demo.testfire.net headers	Vulnerable Demo Sites	Add the header: X-Frame-Options: DENY (or SAMEORIGIN if you need to embed the page on your own site). CSP frame-ancestors directive is the modern replacement.
high	**No SPF record for demo.testfire.net** CWE-290 No SPF (Sender Policy Framework) record was found for demo.testfire.net. Without SPF, anyone can send email pretending to be from your domain. This en	demo.testfire.net dns	Vulnerable Demo Sites	Add an SPF TXT record to your DNS. A basic record looks like: "v=spf1 include:_spf.google.com -all" (adjust for your email provider). Use -all (hardfail) to reject unauthorized senders.

high	**No DMARC record for demo.testfire.net** CWE-290 No DMARC record was found for demo.testfire.net. DMARC (Domain-based Message Authentication, Reporting & Conformance) tells receiving servers what to	demo.testfire.net dns	Vulnerable Demo Sites	Add a DMARC TXT record at _dmarc.demo.testfire.net. Start with: "v=DMARC1; p=none; rua=mailto:dmarc-reports@demo.testfire.net" to collect reports, then move to p=quarantine or p=reject.
medium	**HTTP Proxy/Alt exposed on 65.61.137.117:8080/tcp (Apache Tomcat/Coyote JSP engine 1.1)** An HTTP service is running on a non-standard port (8080). This is often an admin panel, development server, or proxy that may have weaker security tha	demo.testfire.net ports	Vulnerable Demo Sites	Determine what service is running on 8080. If it's an admin panel, restrict access by IP. If it's a development server, take it offline or move behind authentication.
medium	**Missing Strict-Transport-Security header on demo.testfire.net:443** CWE-319 The Strict-Transport-Security (HSTS) header is missing. Without HSTS, users can be downgraded from HTTPS to HTTP via man-in-the-middle attacks. HSTS t	demo.testfire.net headers	Vulnerable Demo Sites	Add the header: Strict-Transport-Security: max-age=31536000; includeSubDomains. Start with a short max-age (e.g., 300) for testing, then increase to 1 year.
medium	**Missing Content-Security-Policy header on demo.testfire.net:443** CWE-79 The Content-Security-Policy (CSP) header is missing. CSP prevents cross-site scripting (XSS) and data injection attacks by controlling which resources	demo.testfire.net headers	Vulnerable Demo Sites	Add a Content-Security-Policy header. Start with a report-only policy to identify issues: Content-Security-Policy-Report-Only: default-src 'self'. Then tighten based on your application's needs.
medium	**Missing X-Content-Type-Options header on demo.testfire.net:443** CWE-16 The X-Content-Type-Options header is missing. Without it, browsers may MIME-sniff responses, potentially treating non-script files as scripts, enablin	demo.testfire.net headers	Vulnerable Demo Sites	Add the header: X-Content-Type-Options: nosniff

medium	**Missing Referrer-Policy header on demo.testfire.net:443** The Referrer-Policy header is missing. By default, browsers send the full URL (including query parameters) as the Referer header when navigating, pote	demo.testfire.net headers	Vulnerable Demo Sites	Add the header: Referrer-Policy: strict-origin-when-cross-origin (recommended) or no-referrer for maximum privacy.
medium	**Missing Permissions-Policy header on demo.testfire.net:443** The Permissions-Policy (formerly Feature-Policy) header is missing. This header controls which browser features (camera, microphone, geolocation, etc.	demo.testfire.net headers	Vulnerable Demo Sites	Add a Permissions-Policy header disabling features you don't need: Permissions-Policy: camera=(), microphone=(), geolocation=()
medium	**Cookie 'JSESSIONID' missing SameSite attribute** CWE-1275 The cookie 'JSESSIONID' does not have a SameSite attribute. Without SameSite, the cookie is sent with cross-site requests, which can enable CSRF attac	demo.testfire.net headers	Vulnerable Demo Sites	Set SameSite=Lax or SameSite=Strict on the 'JSESSIONID' cookie. Use Lax for most cases; Strict if the cookie is security-sensitive.
low	**TLS 1.3 not supported on demo.testfire.net** TLS 1.3 is not supported on this server. TLS 1.3 provides improved security and performance (faster handshake, forward secrecy by default). While TLS	demo.testfire.net ssl	Vulnerable Demo Sites	Enable TLS 1.3 in your server configuration. For nginx: ssl_protocols TLSv1.2 TLSv1.3; Ensure your OpenSSL version is 1.1.1+ for TLS 1.3 support.
low	**No DKIM records found for demo.testfire.net** No DKIM (DomainKeys Identified Mail) records were found for common selectors on demo.testfire.net. DKIM adds a digital signature to outgoing emails, p	demo.testfire.net dns	Vulnerable Demo Sites	Configure DKIM signing for your email provider. Most providers (Google Workspace, Microsoft 365, etc.) have guides for setting up DKIM DNS records.
low	**No IPv6 (AAAA) records for demo.testfire.net** No AAAA records were found for demo.testfire.net. IPv6 adoption is growing, and some networks are IPv6-only. Not having AAAA records means the domain	demo.testfire.net dns	Vulnerable Demo Sites	If your hosting provider supports IPv6, add AAAA records pointing to the IPv6 address. Most modern providers support dual-stack.

low	**Nuclei: Weak Cipher Suites Detection at demo.testfire.net:443** A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an en	demo.testfire.net ssl	Vulnerable Demo Sites	—
low	**SSH exposed on 45.33.32.156:22/tcp** SSH is exposed to the internet. While SSH is encrypted, it is a common target for brute-force attacks. Password authentication should be disabled in f	scanme.nmap.org ports	Vulnerable Demo Sites	Disable password authentication (PasswordAuthentication no). Use key-based auth only. Consider changing the default port and using fail2ban to block brute-force attempts.
low	**Open port 123/udp on 45.33.32.156 (ntpd 3)** Port 123/udp is open on 45.33.32.156. Running ntpd 3. Review whether this service needs to be internet-facing.	scanme.nmap.org ports	Vulnerable Demo Sites	Verify that port 123 needs to be publicly accessible. Close unnecessary ports using firewall rules.
info	**HTTP exposed on 44.228.249.3:80/tcp (nginx 1.19.0)** Standard HTTP web server. Check that HTTPS redirect is in place.	testphp.vulnweb.com ports	Vulnerable Demo Sites	Ensure HTTP redirects to HTTPS. Check security headers.
info	**Technology detected: nginx 1.19.0** Web Server 'nginx' version 1.19.0 detected on testphp.vulnweb.com. Detected via shodan with high confidence.	testphp.vulnweb.com technology	Vulnerable Demo Sites	—
info	**Technology detected: Php 5.6.40** Other 'Php' version 5.6.40 detected on testphp.vulnweb.com. Detected via cpe with high confidence.	testphp.vulnweb.com technology	Vulnerable Demo Sites	—

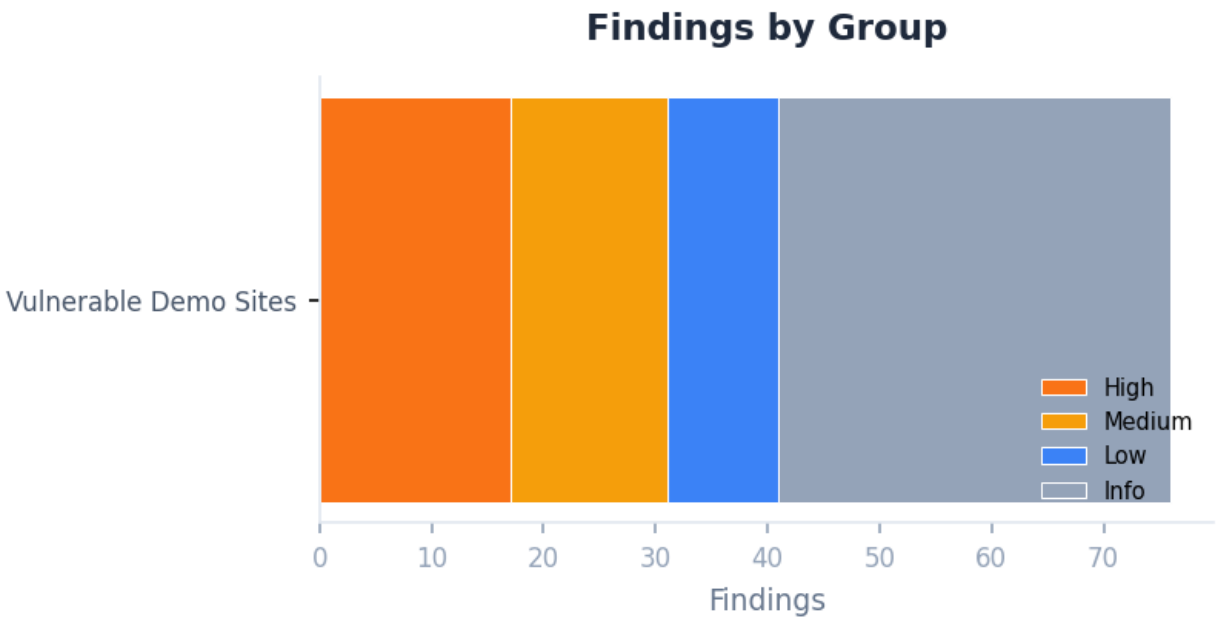
info	**Exposure Score: 15/100 (Grade B) — 4 findings, 1 actionable** Overall exposure assessment for testphp.vulnweb.com. Grade: B — Good — minor issues found. Found 0 critical, 1 high, 0 medium, 0 low, and 3 informatio	testphp.vulnweb.com score	Vulnerable Demo Sites	Address 1 high-severity finding(s) this week.
info	**HTTP exposed on 65.61.137.117:80/tcp (Apache Tomcat/Coyote JSP engine 1.1)** Standard HTTP web server. Check that HTTPS redirect is in place.	demo.testfire.net ports	Vulnerable Demo Sites	Ensure HTTP redirects to HTTPS. Check security headers.
info	**HTTPS exposed on 65.61.137.117:443/tcp (Apache Tomcat/Coyote JSP engine 1.1)** Standard HTTPS web server.	demo.testfire.net ports	Vulnerable Demo Sites	Verify SSL/TLS configuration is secure. Check security headers.
info	**SSL certificate on demo.testfire.net:443: unknown (issued by Unknown CA)** SSL/TLS certificate details for demo.testfire.net:443. Subject: unknown. Issuer: Unknown CA. Valid: None to None. SANs: none.	demo.testfire.net ssl	Vulnerable Demo Sites	—
info	**Technology detected: Apache** Web Server 'Apache' detected on demo.testfire.net. Detected via http_header with high confidence.	demo.testfire.net technology	Vulnerable Demo Sites	—
info	**Technology detected: Java** Framework/Language 'Java' detected on demo.testfire.net. Detected via cookie with medium confidence.	demo.testfire.net technology	Vulnerable Demo Sites	—
info	**Nuclei: Public Swagger API - Detect at https://demo.testfire.net/swagger/index.html** cwe-200 Public Swagger API was detected.	demo.testfire.net exposure	Vulnerable Demo Sites	—

info	**Nuclei: WAF Detection at https://demo.testfire.net** cwe-200 A web application firewall was detected.	demo.testfire.net technology	Vulnerable Demo Sites	—
info	**Nuclei: Deprecated TLS Detection at demo.testfire.net:443** Both TLS 1.1 and SSLv3 are deprecated in favor of stronger encryption.	demo.testfire.net ssl	Vulnerable Demo Sites	Update the web server's TLS configuration to disable TLS 1.1 and SSLv3.
info	**Nuclei: TLS Version - Detect at demo.testfire.net:443** TLS version detection is a security process used to determine the version of the Transport Layer Security (TLS) protocol used by a computer or server.	demo.testfire.net ssl	Vulnerable Demo Sites	—
info	**Nuclei: Apache Detection at https://demo.testfire.net** Some Apache servers have the version on the response header. The OpenSSL version can be also obtained	demo.testfire.net technology	Vulnerable Demo Sites	—
info	**Exposure Score: 100/100 (Grade F) — 29 findings, 15 actionable** Overall exposure assessment for demo.testfire.net. Grade: F — Failing — critical exposure, immediate action needed. Found 0 critical, 8 high, 7 medium	demo.testfire.net score	Vulnerable Demo Sites	Address 8 high-severity finding(s) this week. Plan fixes for 7 medium finding(s).
info	**Nuclei: HTTP Missing Security Headers at https://demo.testfire.net** This template searches for missing HTTP security headers. The impact of these missing headers can vary.	demo.testfire.net misconfiguration	Vulnerable Demo Sites	—

info	**Exposure Score: 100/100 (Grade F) — 30 findings, 15 actionable** Overall exposure assessment for demo.testfire.net. Grade: F — Failing — critical exposure, immediate action needed. Found 0 critical, 8 high, 7 medium	demo.testfire.net score	Vulnerable Demo Sites	Address 8 high-severity finding(s) this week. Plan fixes for 7 medium finding(s).
info	**HTTP exposed on 45.33.32.156:80/tcp (Apache httpd 2.4.7)** Standard HTTP web server. Check that HTTPS redirect is in place.	scanme.nmap.org ports	Vulnerable Demo Sites	Ensure HTTP redirects to HTTPS. Check security headers.
info	**Open port 9929/tcp on 45.33.32.156** Port 9929/tcp is open on 45.33.32.156. Review whether this service needs to be internet-facing.	scanme.nmap.org ports	Vulnerable Demo Sites	Verify that port 9929 needs to be publicly accessible. Close unnecessary ports using firewall rules.
info	**Open port 31337/tcp on 45.33.32.156** Port 31337/tcp is open on 45.33.32.156. Review whether this service needs to be internet-facing.	scanme.nmap.org ports	Vulnerable Demo Sites	Verify that port 31337 needs to be publicly accessible. Close unnecessary ports using firewall rules.
info	**Technology detected: Apache httpd 2.4.7** Web Server 'Apache httpd' version 2.4.7 detected on scanme.nmap.org. Detected via shodan with high confidence.	scanme.nmap.org technology	Vulnerable Demo Sites	—
info	**Technology detected: Http Server 2.4.7** Other 'Http Server' version 2.4.7 detected on scanme.nmap.org. Detected via cpe with high confidence.	scanme.nmap.org technology	Vulnerable Demo Sites	—
info	**Technology detected: ntpd 3** Other 'ntpd' version 3 detected on scanme.nmap.org. Detected via shodan with high confidence.	scanme.nmap.org technology	Vulnerable Demo Sites	—

info	**Technology detected: Ntp 3** Other 'Ntp' version 3 detected on scanme.nmap.org. Detected via cpe with high confidence.	scanme.nmap.org technology	Vulnerable Demo Sites	—
info	**Exposure Score: 6/100 (Grade A) — 9 findings, 0 actionable** Overall exposure assessment for scanme.nmap.org. Grade: A — Excellent — minimal exposure. Found 0 critical, 0 high, 0 medium, 2 low, and 7 information	scanme.nmap.org score	Vulnerable Demo Sites	No critical issues found.

WHERE — Asset Inventory



Assets by Risk (5 assets across 1 groups)

Asset	Type	Critical	High	Medium	Low	Total
demo.testfire.net	domain	0	16	14	8	61
testphp.vulnweb.com	domain	0	1	0	0	5
scanme.nmap.org	domain	0	0	0	2	10

WHEN — Timeline

Report generated: **February 16, 2026 at 13:48 UTC**

Historical trending data (MTTR, findings over time) will be available once the Historical Trending module is implemented.

HOW — Detection Methods

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

Total assets scanned: **5**