PhantomSec Full Penetration Test Report

Prepared for: Sample Client Ltd

Conducted by: PhantomSec

Date: August 2025

Executive Summary

PhantomSec conducted a black-box penetration test on Sample Client Ltd's public web infrastructure. Testing followed industry standards (OWASP Top 10, NIST SP 800-115) to assess external threats. Multiple vulnerabilities of high to low risk were identified, which could lead to data leakage, unauthorized access, or service disruption.

Methodology

- Reconnaissance (Passive + Active)

- Vulnerability Scanning (Automated + Manual)

- Exploitation Attempts (Safe-mode / Non-destructive)

- Post-Exploitation Enumeration (if applicable)

- Reporting & Recommendation Mapping

Tools Used: Nmap, Nikto, Burp Suite, FFUF, WPScan, Gobuster, custom scripts.

Summary of Findings

Vulnerability	Severity	CVSS Score	Status
Outdated WP Plugin (Contact Form 7)	High	8.8	Unpatched
Directory Listing on /uploads	Medium	6.3	Resolved
Missing CSP/X-Frame Headers	Low	4.5	Pending Review
Sensitive .git folder exposed	High	9.0	Unpatched

Detailed Findings

1. Outdated WordPress Plugin - Contact Form 7

Severity: High | *CVSS 8.8*

Version 5.3 of Contact Form 7 is installed, which is vulnerable to unauthenticated file upload leading to remote code execution.

Risk: Complete server takeover, lateral movement, data breach.

Evidence: /wp-content/plugins/contact-form-7/readme.txt

Recommendation: Upgrade immediately to 5.9 or higher.

2. .git Folder Exposed

Severity: High | *CVSS 9.0*

Directory listing and access to /.git/ allows attackers to download the full source code and config history.

Risk: Credential leakage, site clone, full disclosure.

Evidence: https://targetsite.com/.git/config returns valid data.

Recommendation: Add deny rules in .htaccess / NGINX or remove folder from web root.

Conclusion

PhantomSec recommends the client address all High and Medium severity issues immediately, followed by low-risk items. Ongoing security reviews and monitoring are strongly advised.

Contact: phantomsec.team@outlook.com | 07544447903