Vulnerability Assessment Report

Executive Summary

This report presents the findings of a vulnerability assessment conducted on the client's web servers using Nessus. The assessment identified several issues, the most critical being the use of an unsupported PHP version. Additionally, there are medium-risk issues such as potential clickjacking vulnerabilities. The report provides detailed findings along with recommendations to address each identified issue to enhance the overall security posture of the web servers.

Critical Severity	High Severity	Medium Severity	Low Severity
1	0	2	0

Findings

ID	Vulnerability	Port	Description	Risk	Recommendation
1	TTP Server Type and Version	80, 443	The remote web server is identified as Apache.	None	No action required.
2	Web Server No 404 Error Code Check	80	The web server does not return 404 error codes for non-existent URLs.	None	Ensure the web server is configured to return 404 error codes for non-existent files.
3	Web Mirroring	443	Nessus mirrored the website and extracted CGI scripts.	None	Review the discovered CGI scripts to ensure they are secure.
4	Web Server Directory Enumeration	80, 443	Possible to enumerate directories.	None	Ensure directories are in compliance with security standards. Restrict access if necessary.
5	Nessus SYN Scanner	80, 443	Open TCP ports identified.	None	Protect your target with an IP filter to restrict unauthorized access.
6	HTTP Methods Allowed (per directory)	80, 443	Various HTTP methods are allowed.	None	Limit allowed HTTP methods to only those necessary.

					Block insecure methods such as PUT, DELETE, CONNECT, TRACE, and HEAD.
7	PHP Version Detection	443	PHP version 8.0.30 detected.	None	Ensure PHP is up to date and supported.
8	External URLs	443	External links found on the website.	None	Review external links to ensure they are safe and intended.
9	Missing or Permissive Content-Security-Policy Header	443	Missing or permissive CSP frame-ancestors header.	None	Set a strict Content-Security-Policy frame-ancestors header for all resources.
10	Missing or Permissive X-Frame-Options Header	443	Missing or permissive X-Frame-Options header.	None	Set a properly configured X-Frame-Options header to mitigate clickjacking attacks.
11	PHP Unsupported Version Detection	443	Unsupported PHP version 8.0.30 detected.	Critical	Upgrade to a currently supported version of PHP (8.1.x, 8.2.x, or 8.3.x).
12	HSTS Missing From HTTPS Server	443	HSTS not enforced.	None	Configure the server to use HSTS to prevent downgrade attacks and enhance security.
13	Web Application Potentially Vulnerable to Clickjacking	443	Missing X-Frame-Options or CSP frame-ancestors header.	Medium	Implement X-Frame-Options or CSP frame-ancestors header to prevent clickjacking.
14	Web Application Sitemap	443	Sitemap created from crawling the target host.	None	Review the sitemap and ensure all linked content is secure.
15	jQuery Detection	443	jQuery version 1.8.3 detected.	None	Ensure jQuery is up to date.
16	jQuery UI Detection	443	jQuery UI version 1.7.3 detected.	None	Ensure jQuery UI is up to date.

Summary of Critical Issues

PHP Unsupported Version Detection (Critical)

Description: Unsupported PHP version 8.0.30 detected.

Port: 443

Recommendation: Upgrade PHP to a supported version (8.1.x, 8.2.x, or 8.3.x).

Summary of Medium Issues

Web Application Potentially Vulnerable to Clickjacking

Description: Missing X-Frame-Options or CSP frame-ancestors header.

Port: 443

Recommendation: Implement X-Frame-Options or CSP frame-ancestors header to prevent clickjacking.