Fortify Tech
Security Assessment Findings Report

Business Confidential

Table of Contents

Confidentiality Statement

Dokumen ini merupakan dokumen confidential yang dibuat oleh pentester dan berisi hasil report dari proses percobaan External Penetration Test.

Disclaimer

Penetration Test ini sudah memperoleh izin dari pihak perusahaan untuk mencoba dan mencari kerentanan yang dimiliki oleh website.

Contact Information

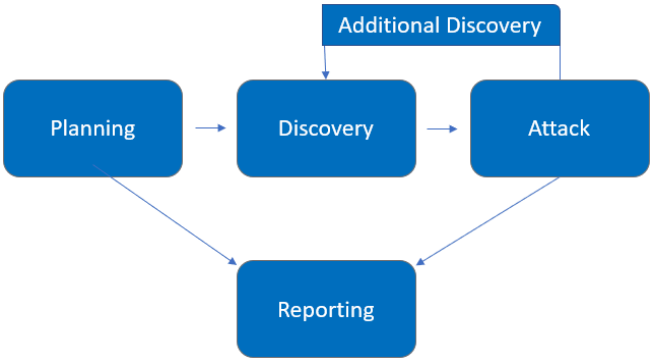
Name	Title	Contact Information
Demo Company		
Aslab	VP, Information Security (CISO)	Office: (555) 555-5555 Email: john.smith@demo.com
Aslab	IT Manager	Office: (555) 555-5555 Email: jim.smith@demo.com
Aslab	Network Engineer	Office: (555) 555-5555 Email: joe.smith@demo.com
Pentest Rawr		
Wikri Cahya	Mahasiswa	Nrp: 5027221020 Email:wikrinew@gmail.com

Assessment Overview

Penetration test dilakukan pada tanggal 7 Mei 2024-8 Mei 2024

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A TCMS engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
Scanning Vulnerability Test	10.15.42.36 10.15.42.7

Scope Exclusions

Tidak boleh melakukan hal yang melanggar etika

Client Allowances

DC did not provide any allowances to assist the testing.

Executive Summary

Sesuai dengan notes diatas, pentester melakukan uji coba keamanan website fortify tech untuk mencari akses kerentanan terhadap websitenya.as

Scanning Summary

Tabel ini menjelaskan bagaimana scanning menggunakan wasp untuk keamanan website di 10.15.42.7 menggunakan OWasp Zap

No	Scanning	Description
1	Alert Counts By Site and Risk	Menunjukkan jumlah peringatan yang dihasilkan untuk setiap situs yang satu atau lebih peringatan telah dibuat, berdasarkan tingkat risiko masing-masing peringatan. Peringatan dengan tingkat keyakinan "False Positive" telah dikecualikan dari perhitungan ini. (Angka dalam tanda kurung adalah jumlah peringatan yang dihasilkan untuk situs tersebut pada tingkat risiko tersebut atau di atasnya.)
2	Alert Counts by Alert type	Menunjukkan jumlah peringatan dari setiap jenis peringatan, bersama dengan tingkat risiko jenis peringatan tersebut. (Persen dalam tanda kurung mewakili setiap hitungan sebagai persentase, dibulatkan ke satu tempat desimal, dari total jumlah peringatan yang disertakan dalam laporan ini.)

3	Alert Counts by Alert Type	Menunjukkan jumlah peringatan untuk setiap tingkat risiko dan tingkat keyakinan yang disertakan dalam laporan. (Persen dalam tanda kurung mewakili jumlah sebagai persentase dari total jumlah peringatan yang disertakan dalam laporan, dibulatkan ke satu tempat desimal.)

Security Strengths

Dari hasil scan owasp, nuclei, nmap dan alat yang saya gunakan, security strength dari website tersebut lemah terhadap kerentanan. Dengan demikian kekuatan website tersebut bisa dibilang nihil.

Security Weaknesses

Header Lost

Temuan tentang kehilangan beberapa header keamanan HTTP, seperti Strict-Transport-Security (HSTS), Content-Security-Policy (CSP), dan X-Frame-Options, menunjukkan kekurangan dalam implementasi kontrol keamanan pada server web. Tanpa header ini, risiko serangan seperti man-in-the-middle (MITM) dan clickjacking meningkat karena kurangnya mekanisme perlindungan yang diterapkan oleh browser.

Hilangnya Anti CSRF Token

Kehadiran CSRF token biasanya penting dalam mencegah serangan Cross-Site Request Forgery (CSRF) yang memungkinkan penyerang menjalankan tindakan yang tidak diinginkan atas nama pengguna yang sudah di autentikasi. Kehilangan CSRF token pada aplikasi web WordPress meningkatkan risiko serangan CSRF, memungkinkan penyerang

untuk mengeksploitasi perilaku otentikasi pengguna dan melakukan tindakan berbahaya seperti mengubah kata sandi atau posting konten palsu.

Server Leaks Information

Temuan terkait dengan OpenSSH versi 8.2p1 dan PHP versi 8.2.18 pada server memberikan informasi sensitif kepada penyerang tentang lingkungan teknis yang digunakan. Dengan mengeksploitasi kerentanan yang diketahui terhadap versi perangkat lunak tertentu, penyerang dapat mengarahkan serangan mereka secara lebih efektif, menggali informasi lebih lanjut tentang konfigurasi sistem, dan merencanakan serangan yang lebih canggih. Itu menyoroti pentingnya memperbarui perangkat lunak secara teratur untuk mengatasi kerentanan yang diketahui dan mengurangi risiko eksposur informasi.

Bruteforce Vulnerability

Masalah ini mengindikasikan bahwa ada potensi celah keamanan atau kelemahan dalam proses otentikasi pengguna pada halaman login WordPress. Ini bisa berarti bahwa ada risiko serangan brute force, di mana penyerang mencoba untuk menebak kombinasi kata sandi atau mengambil alih akun dengan menggunakan teknik otentikasi yang lemah atau tidak terlindungi.

Furminator Vulnerability

Forminator Vulnerability yaitu kelemahan versi plugin Forminator yang terinstall menunjukkan bahwa ada celah keamanan dalam plugin Forminator yang digunakan dalam instalasi WordPress. Celah keamanan semacam itu dapat dieksploitasi oleh penyerang untuk memanipulasi atau merusak situs web, mencuri data sensitif, atau bahkan mendapatkan akses ke server secara keseluruhan. Ini menekankan pentingnya untuk selalu memperbarui plugin WordPress ke versi terbaru dan memantau pembaruan keamanan untuk mengurangi risiko eksploitasi celah keamanan.

Rekomendasi Langkah yang Tepat

Remediation

Who:	IT Team
Vector:	Remote

Recommendation	Bruteforce Vulnerability 1. Gunakan plugin keamanan WordPress yang dapat membatasi jumlah upaya login yang gagal. 2. Gunakan kombinasi kata sandi yang kuat dan unik untuk akun pengguna. 3. Aktifkan autentikasi dua faktor (2FA) untuk meningkatkan lapisan keamanan. Forminator Vulnerability 1. Perbarui plugin Forminator secara teratur ke versi terbaru. 2. Periksa ulasan dan pembaruan keamanan plugin sebelum menginstalnya. 3. Gunakan plugin keamanan WordPress yang dapat mendeteksi dan mencegah eksploitasi celah keamanan pada plugin. Header Lost 1. Tambahkan header keamanan HTTP yang diperlukan, seperti Strict-Transport-Security (HSTS), Content-Security-Policy (CSP), dan X-Frame-Options melalui konfigurasi server. 2. Gunakan plugin keamanan WordPress yang dapat secara otomatis menambahkan header keamanan ke setiap permintaan HTTP. Anti CSRF Token Lost 1. Pastikan setiap formulir atau tindakan yang sensitif di situs web WordPress dilindungi oleh token CSRF. 2. Gunakan plugin keamanan WordPress yang secara otomatis menyertakan token CSRF pada setiap permintaan yang memerlukan otentikasi. Server Leaks Information 1. Nonaktifkan opsi untuk mengungkapkan informasi tentang versi perangkat lunak yang digunakan pada server. 2. Perbarui perangkat lunak server secara teratur ke versi terbaru untuk memperbaiki kerentanan yang diketahui. 3. Gunakan firewall dan perangkat lunak keamanan jaringan untuk mengamankan server dari serangan luar.

Last Page