Fortify Tech
Security Assessment Findings Report

Table of Contents

Pernyataan Kerahasiaan

Dokumen ini adalah milik eksklusif Fortify Tech dan CyberShield. Dokumen ini berisi informasi yang bersifat kepemilikan dan rahasia. Duplikasi, distribusi ulang, atau penggunaan, secara keseluruhan atau sebagian, dalam bentuk apa pun, memerlukan persetujuan dari Fortify Tech dan CyberShield.

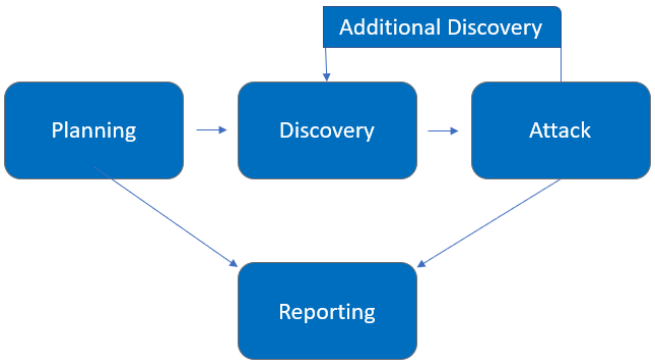
Disclaimer

Informasi Kontak

Name	Title	Contact Information
Fortify Tech		
CyberShield		
Imam Nurhadi	Penetration Tester	Email: adigaming015@gmail.com

Overview Penilaian

- Perencanaan – Sasaran pelanggan dikumpulkan dan aturan keterlibatan diperoleh.
- Discovery – Melakukan pemindaian dan enumerasi untuk mengidentifikasi potensi kerentanan, area lemah, dan eksploitasi.
- Serangan – Konfirmasikan potensi kerentanan melalui eksploitasi dan lakukan penemuan tambahan pada akses baru.
- Pelaporan – Mendokumentasikan semua kerentanan dan eksploitasi yang ditemukan, upaya yang gagal, serta kekuatan dan kelemahan perusahaan.



Komponen Penilaian

Uji Penetrasi Internal

Komponen Penilaian untuk Uji Penetrasi Internal mencakup evaluasi kerentanan yang ditemukan selama pengujian, kategorisasi tingkat kritisitas kerentanan, serta metode penetrasi yang digunakan dalam identifikasi celah keamanan. Selain itu, penting juga untuk menilai kemampuan sistem dalam mencegah dan mendeteksi serangan yang terjadi selama uji penetrasi, serta mengidentifikasi risiko potensial yang terkait dengan kerentanan yang ditemukan. Perlu disusun laporan hasil uji penetrasi yang mendetail, dengan rekomendasi yang jelas untuk memperbaiki kerentanan yang teridentifikasi.

Klasifikasi Tingkat Keparahan

Tabel berikut ini mendefinisikan tingkat keparahan dan rentang skor CVSS yang sesuai yang digunakan di seluruh dokumen untuk menilai kerentanan dan dampak risiko.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Eksploitasi sangat mudah dan biasanya menghasilkan kompromi tingkat sistem. Disarankan untuk membuat rencana tindakan dan segera menambalnya.
High	7.0-8.9	Eksploitasi lebih sulit tetapi dapat menyebabkan peningkatan hak istimewa dan berpotensi kehilangan data atau waktu henti. Disarankan untuk membuat rencana tindakan dan menambal sesegera mungkin.
Moderate	4.0-6.9	Kerentanan ada tetapi tidak dapat dieksploitasi atau memerlukan langkah ekstra seperti rekayasa sosial. Disarankan untuk membuat rencana tindakan dan menambal setelah masalah-masalah yang menjadi prioritas utama diselesaikan.
Low	0.1-3.9	Kerentanan tidak dapat dieksploitasi tetapi akan mengurangi permukaan serangan organisasi. Disarankan untuk membuat rencana tindakan dan menambal selama masa pemeliharaan berikutnya.
Informational	N/A	Tidak ada kerentanan. Informasi tambahan disediakan mengenai hal-hal yang diperhatikan selama pengujian, kontrol yang kuat, dan dokumentasi tambahan.

Scope

Assessment	Details
Uji Penetrasi Internal	10.15.42.36 10.15.42.7

Scope Exclusions

Berdasarkan permintaan klien, kami tidak melakukan kegiatan apapun yang melanggar etika dan tetap mennjalankan kegiatan melalui jaringan its melalui OpenVPN melalui akun myits.

Client Allowances

Akses internal ke jaringan its melalui OpenVPN untuk mengakses ip 10.15.42.7 dan 10.15.42.36

Executive Summary

Pada tanggal 5 Mei 2024, dilakukan uji penetrasi tahap analisis kerentanan menggunakan beberapa alat seperti Nmap, Dirb, dan Nikto pada sistem operasi Parrot VMware. Tujuan dari uji penetrasi ini adalah untuk mengevaluasi keamanan sistem dan aplikasi yang terpasang dalam lingkungan dengan alamat IP 10.15.42.36 dan 10.15.42.7. Hasil dari pemindaian tersebut dievaluasi kembali melalui berbagai sumber di internet seperti MITRE CVE, exploit-db, dan sumber lainnya.

Scoping and Time Limitations

Uji penetrasi ini memiliki batasan pada skop dan waktu. Skop pengujian mencakup evaluasi keamanan sistem pada ip 10.15.42.36 dan 10.15.42.7. Batasan waktu pengujian adalah 4 hari mulai dari tanggal 5 sampai 8 mei 2024.

Testing Summary

Untuk alamat IP 10.15.42.36, penggunaan Nmap mengungkapkan bahwa sistem menjalankan server web Apache versi 2.4.38 pada Debian Linux. Informasi ini berpotensi membantu dalam identifikasi kerentanan spesifik yang terkait dengan versi Apache tersebut, bersama dengan beberapa versi Linux yang dijalankan, meskipun distribusi Linux spesifik tidak teridentifikasi. Selain itu, layanan Sun AnswerBook pada port 8888 terkait dengan CVE-2002-2425. Pencarian kerentanan terhadap Apache yang outdated mengungkapkan CVE-2019-0211, sementara versi PHP 7.2.34 rentan terhadap CVE-2020-7069 dan CVE-2020-7070. Percobaan pencarian file pada web server tidak berhasil menemukan file shell.php yang diperlukan untuk melakukan eksploitasi reverse shell. Selain itu, versi PHP yang digunakan pada web server di IP 10.15.42.36 adalah versi 10.1. Melalui percobaan masuk ke FTP port 21, berhasil mendapatkan file backup.sql yang kemudian ditelusuri isinya namun tidak ada yang berarti.

Sementara itu, untuk alamat IP 10.15.42.7, pemindaian menggunakan Nmap menunjukkan bahwa server web menjalankan Apache versi 2.4.59 dan menggunakan WordPress versi 6.5.2. Temuan ini berpotensi terkait dengan kerentanan CVE-2023-38709 pada Apache HTTP Server dan CVE-2024-4439 pada WordPress Core. Selain itu, layanan SSH berjalan pada OpenSSH versi 8.2p1 pada Ubuntu 4ubuntu0.5.

Kelebihan dan Kekurangan

Kelebihan:

1. **Lingkungan Sistem yang Beragam:** Kedua alamat IP, 10.15.42.36 dan 10.15.42.7, menampilkan lingkungan sistem yang beragam, menjalankan berbagai layanan dan aplikasi seperti server web Apache dan OpenSSH, menandakan infrastruktur yang kuat.
2. **Identifikasi Kerentanan yang Sukses:** Melalui penggunaan Nmap dan alat pemindaian lainnya, kerentanan seperti versi perangkat lunak yang kedaluwarsa dan risiko keamanan potensial berhasil diidentifikasi, memberikan wawasan berharga untuk langkah-langkah perbaikan keamanan.
3. **Pengumpulan Informasi yang Efektif:** Penjelajahan yang cermat terhadap server web dan layanan FTP memungkinkan ekstraksi data penting seperti versi PHP dan file cadangan, memberikan pemahaman menyeluruh tentang konfigurasi sistem dan potensi kelemahan.

Kelemahan:

1. **Perangkat Lunak yang Kedaluwarsa:** Kedua IP menunjukkan kerentanan karena menjalankan versi perangkat lunak yang kedaluwarsa, termasuk Apache dan PHP, yang dapat mengekspos sistem terhadap eksploitasi yang dikenal dan ancaman keamanan.
2. **Keamanan File yang Tidak Lengkap:** Tidak dapatnya menemukan file penting seperti shell.php melalui pemindaian server web pada IP 10.15.42.36 menunjukkan potensi kekurangan dalam langkah-langkah keamanan file, menimbulkan kekhawatiran tentang akses yang tidak sah dan kemungkinan eksploitasi.
3. **Identifikasi Sistem yang Terbatas:** Meskipun berhasil mengidentifikasi kerentanan, distribusi Linux yang tepat yang berjalan pada sistem tidak teridentifikasi, yang dapat menghambat upaya mitigasi yang ditargetkan dan penilaian keamanan menyeluruh.

Kelemahan Keamanan

1. **Apache Server yang Outdated (CVE-2019-0211)**
   Kerentanan pada versi Apache yang kedaluwarsa, seperti yang ditemukan pada alamat IP yang ditentukan, meningkatkan risiko terhadap serangan yang memanfaatkan celah keamanan yang sudah diketahui. CVE-2019-0211 adalah kerentanan yang memungkinkan penyerang untuk melakukan serangan Remote Code Execution (RCE) pada server Apache yang rentan, membuka pintu bagi serangan yang merusak dan potensial
2. **Versi PHP yan Outdated (CVE-2020-7069, CVE-2020-7070)**
   Temuan kerentanan pada versi PHP yang kedaluwarsa, seperti yang terdeteksi pada alamat IP yang ditentukan, menyiratkan potensi risiko eksploitasi terhadap kerentanan yang diketahui. CVE-2020-7069 dan CVE-2020-7070 adalah kerentanan yang dapat dimanfaatkan oleh penyerang untuk mengeksploitasi server yang menjalankan PHP, mengakibatkan kerentanan dalam keamanan aplikasi web yang menggunakan PHP.
3. **Terdeteksi port 8888 dengan service sun-answerbooks (CVE 2002-2425)**
   Keberadaan layanan sun-answerbooks pada port 8888 yang terdeteksi dapat menimbulkan risiko keamanan, terutama jika layanan tersebut rentan terhadap serangan yang diketahui. CVE-2002-2425 adalah kerentanan yang berkaitan dengan layanan Sun AnswerBook yang memungkinkan penyerang untuk mengakses skrip administratif secara tidak sah, membuka potensi serangan yang tidak sah dan penggunaan yang merugikan dari layanan tersebut.
4. **Apache HTTP Server: HTTP response splitting (CVE-2023-38709)**
   Kerentanan HTTP response splitting pada server Apache, seperti yang diidentifikasi pada alamat IP yang ditentukan, membuka celah keamanan yang memungkinkan penyerang untuk memanipulasi tanggapan HTTP yang dikeluarkan oleh server, menyebabkan serangan XSS dan serangan terkait lainnya.
5. **WordPress Core < 6.5.2 - Unauthenticated & Authenticated (Contributor+) Stored Cross-Site Scripting via Avatar Block (CVE-2024-4439)**
   Temuan kerentanan pada versi WordPress yang kedaluwarsa, seperti yang terdeteksi pada alamat IP yang ditentukan, menunjukkan risiko terhadap serangan XSS yang disimpan yang memanfaatkan kerentanan yang diketahui dalam WordPress Core. CVE-2024-4439 memungkinkan penyerang untuk menyisipkan skrip berbahaya dalam blok avatar WordPress, membuka potensi eksploitasi terhadap pengguna yang mengakses situs yang terinfeksi.
6. **Missing Content-Type Header (CVE-2019-19089)**
   Kehadiran kerentanan Missing Content-Type Header, seperti yang teridentifikasi pada alamat IP yang ditentukan, meningkatkan risiko terhadap serangan MIME-sniffing. CVE-2019-19089 adalah kerentanan yang memungkinkan penyerang untuk memanfaatkan ketidakhadiran header Jenis Konten untuk menyusupkan konten berbahaya atau tidak diinginkan ke dalam situs web yang rentan.

Temuan Uji Penetrasi Eksternal

Missing Content-Type Header

Description:	Kerentanan ini terjadi karena ketidakhadiran header Content-Type pada permintaan HTTP, yang dapat memungkinkan serangan MIME-sniffing dan penyisipan konten berbahaya.
Impact:	Medium
System:	10.15.46.36
References:	- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-19089

Apache Outdated

Description:	Temuan ini mengindikasikan bahwa versi Apache yang digunakan sudah kedaluwarsa, meningkatkan risiko terhadap serangan yang memanfaatkan kerentanan yang sudah diketahui.
Impact:	High
System:	10.15.46.36
References:	- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0211

PHP version 7.2.34

Description:	Temuan ini menunjukkan bahwa versi PHP yang digunakan adalah 7.2.34, yang rentan terhadap serangan yang memanfaatkan kerentanan yang diketahui.
Impact:	Medium
System:	10.15.46.36
References:	- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7069

WordPress Core < 6.5.2

Description:	Kerentanan ini terjadi karena menggunakan versi WordPress yang tidak diperbarui, yang dapat dieksploitasi untuk menyisipkan skrip berbahaya dan mengakibatkan serangan XSS yang disimpan.
Impact:	High
System:	10.15.46.7
References:	- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-4439

Last Page