Fortify Tech
Security Assessment Findings Report

Business Confidential

Date: May 8th, 2024
Project: 38-5027
Version 1.0

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

Uji penetrasi dianggap sebagai snapshot dalam waktu tertentu. Temuan dan rekomendasi mencerminkan informasi yang dikumpulkan selama penilaian dan bukan perubahan atau modifikasi yang dilakukan di luar periode tersebut.

Keterlibatan yang dibatasi waktu tidak memungkinkan untuk evaluasi penuh terhadap semua kontrol keamanan. CyberShield memprioritaskan penilaian untuk mengidentifikasi kontrol keamanan terlemah yang akan dieksploitasi oleh penyerang. CyberShield merekomendasikan untuk melakukan penilaian serupa setiap tahun oleh penilai internal atau pihak ketiga untuk memastikan keberhasilan kontrol yang berkelanjutan.

Informasi Kontak

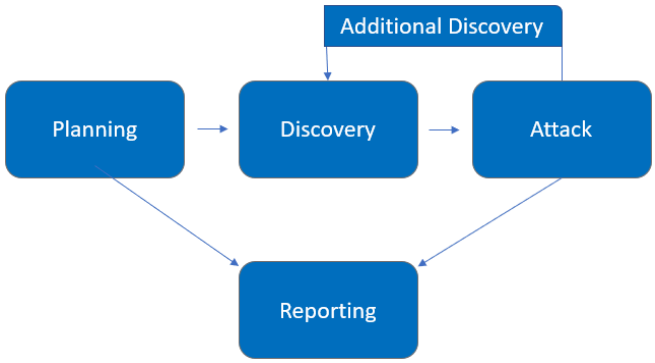
Name	Title	Contact Information
Fortify Tech		
John Smith	VP, Information Security (CISO)	Office: (555) 555-5555 Email: john.smith@demo.com
Jim Smith	IT Manager	Office: (555) 555-5555 Email: jim.smith@demo.com
Joe Smith	Network Engineer	Office: (555) 555-5555 Email: joe.smith@demo.com
CyberShield		
Heath Adams	Lead Penetration Tester	Office: (555) 555-5555 Email: hadams@tcm-sec.com
Bob Adams	Penetration Tester	Office: (555) 555-5555 Email: badams@tcm-sec.com
Rob Adams	Account Manager	Office: (555) 555-5555 Email: radams@tcm-sec.com

Overview Penilaian

Dari tanggal 5 Mei 2024 hingga 8 Mei 2024, Fortify Tech melibatkan CyberShield untuk mengevaluasi postur keamanan infrastrukturnya dibandingkan dengan praktik terbaik industri saat ini yang mencakup uji penetrasi eksternal

Fase kegiatan pengujian penetrasi meliputi hal-hal berikut:

- Perencanaan - Tujuan pelanggan dikumpulkan dan aturan main diperoleh.
- Penemuan - Melakukan pemindaian dan enumerasi untuk mengidentifikasi potensi kerentanan, area yang lemah, dan eksploitasi.
- Serangan - Mengonfirmasi kerentanan potensial melalui eksploitasi dan melakukan penemuan tambahan setelah mendapatkan akses baru.
- Pelaporan - Mendokumentasikan semua kerentanan dan eksploitasi yang ditemukan, percobaan yang gagal, serta kekuatan dan kelemahan perusahaan.



Komponen Penilaian

Uji Penetrasi Eksternal

Uji penetrasi eksternal meniru peran penyerang yang mencoba mendapatkan akses ke jaringan internal tanpa sumber daya internal atau pengetahuan orang dalam. Seorang teknisi CyberShield berusaha mengumpulkan informasi sensitif yang bisa dimanfaatkan untuk melawan sistem eksternal untuk mendapatkan akses jaringan internal. Teknisi juga melakukan pemindaian dan pencacahan untuk mengidentifikasi potensi kerentanan dengan harapan dapat dieksploitasi.

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 Eksternal	10.15.42.36 10.15.42.7

Scope Exclusions

Sesuai permintaan klien, CyberShield tidak melakukan serangan hal - hal yang melanggar etika selama pengujian.

Client Allowances

Fortify Tech tidak memberikan tunjangan apa pun untuk membantu pengujian.

Executive Summary

CyberShield mengevaluasi postur keamanan eksternal Fortify Tech melalui uji penetrasi jaringan eksternal dari tanggal 5 Mei 2024 hingga 8 Mei 2024. Dengan memanfaatkan serangkaian serangan, CyberShield menemukan beberapa kerentanan tingkat moderat. Disarankan untuk membuat rencana tindakan dan menambal setelah masalah-masalah yang menjadi prioritas utama diselesaikan

Attack Summary

Tabel berikut ini menjelaskan bagaimana CyberShield mendapatkan akses jaringan internal, langkah demi langkah:

Step	Action	Recommendation
1	Menggunakan Nmap untuk mengumpulkan informasi terkait service, aplikasi, device, dan lain-lain yang akan kita uji keamanannya	
2	Menggunakan Gobuster dan Dirbuster untuk scanning directory yang terdapat pada suatu web application.	
3	Menggunakan NSE Script untuk validasi kelemahan, hingga otomasi serangan	.

4	Menggunakan Nikto untuk vuln assessment dan backdoor exploitaion untuk menyerang	

Security Weaknesses

Missing Content-Type Header (10.15.42.36)

Mendeteksi header Jenis Konten yang hilang yang berarti bahwa situs web ini dapat berisiko terkena serangan MIME-sniffing.

Apache Server Outdated (10.15.42.36)

Kerentanan ditemukan di Apache HTTP Server 2.4.38. Dengan menggunakan input jaringan yang tidak jelas, penanganan permintaan http/2 dapat dibuat untuk mengakses memori yang dibebaskan dalam perbandingan string ketika menentukan metode permintaan dan dengan demikian memproses permintaan secara tidak benar.

Bisa Access backup.sql di ftp server 10.15.42.36

Selama penilaian, CyberShield melakukan percobaan untuk masuk ke dalam ftp server untuk mendapatkan file database

Temuan Uji Penetrasi Eksternal

Missing Content-Type Header (Low)

Description:	- Fortify Tech membiarkan Missing Content-Type Header. Masalahnya muncul ketika sebuah situs web mengizinkan pengguna untuk mengunggah konten yang kemudian dipublikasikan di server web. Jika penyerang dapat melakukan serangan XSS (Cross-site Scripting) dengan memanipulasi konten sedemikian rupa agar diterima oleh aplikasi web dan dirender sebagai HTML oleh peramban, maka memungkinkan untuk menyuntikkan kode ke dalam, misalnya, file gambar dan membuat korban menjalankannya dengan melihat gambar tersebut. - Fortify Tech menggunakan layanan server yang tidak diperbarui sehingga kemungkinan kerentanan dan kelemahan bisa dieksploitasi
Impact:	Low
System:	10.15.46.32
References:	- https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/ - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0196

Last Page