



# **FortifyTech**

## Security Assessment Findings Report

Business Confidential

*Date: May 8<sup>th</sup>, 2024*  
*Project: DC-001*  
*Version 1.0*

# Table of Contents

- Table of Contents..... 2
- Confidentiality Statement..... 4
- Disclaimer..... 4
- Contact Information ..... 4
- Assessment Overview ..... 5
- Assessment Components ..... 5
  - Internal Penetration Test..... 5
- Finding Severity Ratings ..... 6
- Risk Factors..... 6
  - Likelihood ..... 6
  - Impact..... 6
- Scope..... 7
  - Scope Exclusions ..... 7
  - Client Allowances ..... 7
- Executive Summary ..... 8
  - Scoping and Time Limitations ..... 8
  - Testing Summary ..... 8
  - Tester Notes and Recommendations ..... 9
- Technical Findings ..... 13

---

## Confidentiality Statement

Dokumen ini merupakan milik eksklusif Fortify Tech. Dokumen ini berisi informasi hak milik dan bersifat rahasia. Duplikasi, redistribusi, atau penggunaan, seluruhnya atau sebagian, dalam bentuk apa pun, memerlukan izin dari Fortify Tech.

Fortify Tech dapat membagikan dokumen ini dengan auditor berdasarkan perjanjian kerahasiaan untuk menunjukkan kepatuhan persyaratan uji penetrasi.

## Disclaimer

Pentester memprioritaskan penilaian ini untuk mengidentifikasi kontrol keamanan terlemah yang dapat dieksploitasi oleh penyerang. Pentester merekomendasikan dilakukannya penilaian serupa setiap tahun oleh penilai internal atau pihak ketiga untuk memastikan keberhasilan pengendalian yang berkelanjutan.

## Contact Information

Name	Title	Contact Information
Fortify Tech		
Bintang Ryan	Pentester	Email : bintangryn@gmail.com

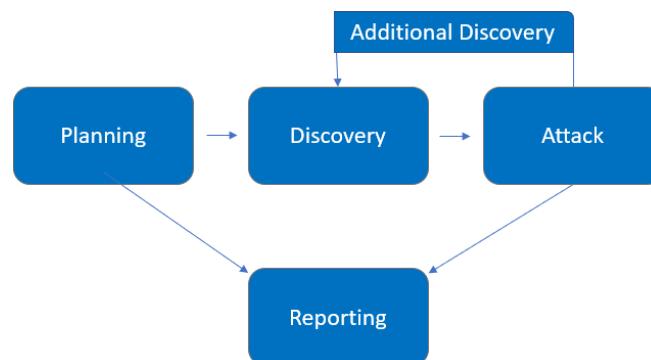
---

## Assessment Overview

Evaluasi keamanan infrastruktur Fortify Tech oleh Pentester dilakukan sejak 7 Mei 2024 hingga 8 Mei 2024, Fortify Tech melibatkan Pentester untuk melakukan praktik terbaik saat ini yang mencakup uji penetrasi jaringan internal. Semua pengujian yang dilakukan didasarkan pada Panduan Teknis NIST SP 800-115 untuk Pengujian dan Penilaian Keamanan Informasi, Panduan Pengujian OWASP (v4), dan kerangka pengujian yang disesuaikan.

Tahapan kegiatan pengujian penetrasi antara lain sebagai berikut:

- Planning – Melakukan perencanaan Pentest terhadap Fortify Tech.
- Discovery – Melakukan pemindaian dan enumerasi terhadap IP 10.15.42.36 dan 10.15.42.7 untuk mengidentifikasi potensi kerentanan, area lemah, dan eksploitasi.
- Attack – Melakukan eksploitasi kerentanan yang ada pada infrastruktur Fortify Tech
- Reporting – Mendokumentasikan semua kerentanan dan eksploitasi yang ditemukan, upaya yang gagal, serta kekuatan dan kelemahan perusahaan.



## Assessment Components

### Internal Penetration Test

Tes penetrasi internal mengemulasi peran penyerang dari dalam jaringan. Pentester akan memindai jaringan untuk mengidentifikasi potensi kerentanan host dan melakukan serangan jaringan internal yang umum dan tingkat lanjut. Pentester akan berusaha mendapatkan akses ke host melalui pergerakan lateral, melakukan penyusupan ke akun pengguna dan admin domain, dan mengumpulkan data sensitive atau pun segala bentuk Informasi penting yang dimiliki oleh Fortify Tech.

---

## Finding Severity Ratings

Tabel berikut menjelaskan bagaimana tingkat keparahan dan rentang skor CVSS terkait yang digunakan di seluruh dokumen untuk menilai kerentanan dan dampak risiko.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Eksplorasi langsung yang mengakibatkan kerentanan pada tingkat sistem dan sebaiknya diatasi segera dengan membuat rencana tindakan dan melakukan perbaikan.
High	7.0-8.9	Eksplorasi yang parah yang dapat menyebabkan peningkatan hak istimewa dan potensial kehilangan data atau waktu tidak aktif. Disarankan untuk membuat rencana tindakan dan segera melakukan penambalan.
Moderate	4.0-6.9	Ada kerentanan tetapi tidak dapat dieksplorasi atau memerlukan langkah tambahan seperti rekayasa sosial. Disarankan untuk membuat rencana tindakan dan melakukan penambalan setelah isu-isu yang memiliki prioritas tinggi telah diselesaikan.
Low	0.1-3.9	Kerentanan tidak dapat dieksplorasi tetapi akan mengurangi permukaan serangan organisasi. Disarankan untuk membuat rencana tindakan dan melakukan penambalan selama jendela perawatan berikutnya.
Informational	N/A	Tidak ada kerentanan yang ada. Informasi tambahan disediakan mengenai hal-hal yang diperhatikan selama pengujian, kontrol yang kuat, dan dokumentasi tambahan.

## Risk Factors

Risiko didasarkan pada dua factor : Likelihood and Impact

### Likelihood

Kemungkinan mengukur potensi kerentanan untuk dieksplorasi. Penilaian diberikan berdasarkan pada kesulitan serangan, alat yang tersedia, tingkat keahlian penyerang, dan lingkungan klien.

### Impact

Dampak mengukur efek potensial kerentanan terhadap operasi, termasuk kerahasiaan, integritas, dan ketersediaan sistem dan/atau data klien, kerugian reputasi, dan kerugian keuangan.

---

## Scope

Assessment	Details
Internal Penetration Test	10.15.42.36 10.15.42.7

## Client Allowances

Fortify Tech mempersilakan Pentester untuk melakukan hal berikut :

- Akses internal ke jaringan melalui Dropbox dan izin port.

---

## Executive Summary

Pada tanggal 7 Mei 2024 hingga 8 Mei 2024, Pentester mengevaluasi postur keamanan internal Fortify Tech melalui pengujian penetrasi. Bagian-bagian berikut memberikan gambaran tingkat tinggi tentang kerentanan yang ditemukan, upaya yang berhasil dan gagal, serta kekuatan dan kelemahan.

### Testing Summary

Sesuai dengan keterangan pada Assessment Overview, Pentester melakukan serangkaian proses untuk mengevaluasi keamanan infrastruktur Fortify Tech. Setelah melakukan serangkaian proses tersebut, Pentester hanya menemukan Informasi umum yang dapat ditemukan oleh siapapun termasuk attacker seperti port yang terbuka, service yang digunakan serta kerentanan yang ada pada infrastruktur Fortify Tech.

### Tester Notes and Recommendations

Setelah melakukan serangkaian proses, Pentester tidak menemukan Informasi yang sensitive karena tidak dapat mengakses ataupun melakukan penyusupan Sebagai admin atau pemilik akses. Pentester hanya menemukan Informasi umum yang dapat ditemukan oleh attacker. Oleh karena itu, tidak ada rekomendasi atau Solusi yang dapat diberikan Pentester kepada Fortify Tech terkait keamanan infrastruktur mereka.

---

# Technical Findings

## 1. NMAP Scanning

Description:	Pentester melakukan scanning terhadap IP Address yang menjadi scope yaitu 10.15.42.36 dan 10.15.42.7
Risk:	Tidak ada risiko yang ditemukan
System:	All
Tools Used:	NMAP
References:	<a href="#">Stern Security</a> - Local Network Attacks: LLMNR and NBT-NS Poisoning <a href="#">NIST SP800-53 r4 IA-3</a> - Device Identification and Authentication <a href="#">NIST SP800-53 r4 CM-6(1)</a> - Configuration Settings

### 1. nmap -Pn -T4

Perintah ini menggunakan Nmap untuk melakukan pemindaian jaringan tanpa ping (menonaktifkan deteksi host) dengan kecepatan tinggi (T4).

```
[user@parrot]-[~]
$ nmap -Pn -T4 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 16:34 UTC
Nmap scan report for 10.15.42.36
Host is up (0.048s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
8888/tcp   open  sun-answerbook
```



```
[user@parrot]-[~]  
$nmap -Pn -T4 10.15.42.7  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 16:36 UTC  
Nmap scan report for 10.15.42.7  
Host is up (0.046s latency).  
Not shown: 999 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
  
Nmap done: 1 IP address (1 host up) scanned in 13.51 seconds
```

## Hasil

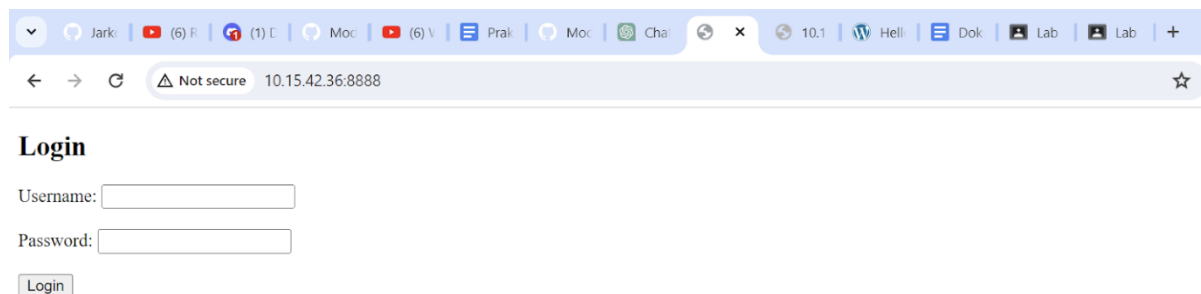
Pada IP 10.15.42.36 ditemukan :

Port : 8888/tcp dengan STATE open dan SERVICE nya sun-answerbook

Pada IP 10.15.42.7 ditemukan :

Port : 22/tcp dengan STATE open dan SERVICE nya ssh

Setelah menemukan port yang terbuka pada IP 10.15.42.36 yaitu 888, saat Pentester mencoba mengakses port tersebut, diarahkan ke Login Page seperti gambar berikut :



Not secure 10.15.42.36:8888

### Login

Username:

Password:

---

## 2. nmap -Sv

Perintah ini menggunakan Nmap untuk melakukan pemindaian versi (SV) dengan mengirim paket SYN ke target.

```
[x]-[root@parrot]-[/home/user]
#nmap -sV 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 04:20 UTC
Nmap scan report for 10.15.42.36
Host is up (0.011s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  vsftpd 2.0.8 or later Ubuntu 0.5 (Ubuntu Linux; protocol 2.0)
22/tcp    open  ssh    OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
8888/tcp  open  http    Apache httpd 2.4.38 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Hasil 1 : 10.15.42.36

SERVICE : http versi Apache httpd 2.4.38 ((Debian))  
OS : Linux yaitu OpenSSH 8.2p1 Ubuntu 4ubuntu0.5

```
[x]-[root@parrot]-[/home/user]
#nmap -sV 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 04:19 UTC
Nmap scan report for 10.15.42.7
Host is up (0.0073s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.59 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Hasil 2 : 10.15.42.7

SERVICE : http versi Apache httpd 2.4.59 ((Debian))  
OS : Linux yaitu OpenSSH 8.2p1 Ubuntu 4ubuntu0.5

---

### 3. nmap -A

Perintah ini menggunakan Nmap dengan opsi agresif (A) untuk melakukan pemindaian yang mencakup deteksi versi (SV), deteksi skrip (script scanning), dan deteksi sistem operasi (OS detection) secara otomatis.

```
[root@parrot]~[/home/user]# nmap -A 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 05:11 UTC
Nmap scan report for 10.15.42.7
Host is up (0.0053s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey: SERVICE VERSION
|_ 3072 9a:ed:52:a9:08:9d:71:6f:d1:24:8f:0b:4a:5b:7a:42 (RSA)
|_ 256 00:9c:a8:13:91:9f:4f:74:fb:9e:15:a2:36:6b:c5:ba (ECDSA)
|_ 256 d7:55:ff:d7:95:e1:06:26:81:bc:f2:b4:b5:29:a9:37 (ED25519)
80/tcp    open  http     Apache httpd 2.4.59 ((Debian))
|_ http-generator: WordPress 6.5.2
|_ http-server-header: Apache/2.4.59 (Debian)
|_ http-title: Hello World
|_ http-robots.txt: 1 disallowed entry
|_ /wp-admin/: header: Apache/2.4.38 (Debian)
```

#### Hasil 1 : 10.15.42.7

Didapatkan informasi berikut :

http-generator : WordPress 6.5.2

http-server-header : Apache/2.4.59 (Debian)

http-title : Hello World

```
[root@parrot]~[/home/user]# nmap -A 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 05:11 UTC
Nmap scan report for 10.15.42.36
Host is up (0.0056s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
|_ 3072 ca:12:a1:08:41:b8:5b:01:b2:2b:c6:64:9d:01:ce:e0 (RSA)
|_ 256 df:e6:37:47:be:43:54:96:1f:40:43:9b:d7:ac:78:ad (ECDSA)
|_ 256 b5:74:86:8d:ee:74:51:2a:38:09:67:38:7d:a0:e6:c0 (ED25519)
8888/tcp  open  http     Apache httpd 2.4.38 ((Debian))
|_ http-title: Login Page
|_ http-server-header: Apache/2.4.38 (Debian)
```

#### Hasil

http-server-header : Apache/2.4.38 (Debian)

http-title : Login Page

## 2. Finding Vulnerability

Description:	Pentester melakukan pencarian kerentanan melalui web CVE. Kerentanan yang dicari adalah berdasarkan perangkat lunak dan service yang digunakan oleh FortifyTech yaitu server Apache/2.4.38 dan http-generator nya yaitu Wordpress 6.5.2
Risk:	Tidak ada risiko yang ditemukan
System:	All
Tools Used:	CVE
References:	<a href="#">Stern Security</a> - Local Network Attacks: LLMNR and NBT-NS Poisoning <a href="#">NIST SP800-53 r4 IA-3</a> - Device Identification and Authentication <a href="#">NIST SP800-53 r4 CM-6(1)</a> - Configuration Settings

### 1. Server Apache/2.4.38

Name	Description
<a href="#">CVE-2019-0220</a>	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
<a href="#">CVE-2019-0217</a>	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
<a href="#">CVE-2019-0211</a>	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
<a href="#">CVE-2019-0196</a>	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

### 2. WordPress 6.5.2

Name	Description
<a href="#">CVE-2024-4439</a>	WordPress Core is vulnerable to Stored Cross-Site Scripting via user display names in the Avatar block in various versions up to 6.5.2 due to insufficient output escaping on the display name. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. In addition, it also makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that have the comment block present and display the comment author's avatar.
<a href="#">CVE-2024-24881</a>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VeronaLabs WP SMS &#8211; Messaging & SMS Notification for WordPress, WooCommerce, GravityForms, etc allows Reflected XSS.This issue affects WP SMS &#8211; Messaging & SMS Notification for WordPress, WooCommerce, GravityForms, etc: from n/a through 6.5.2.
<a href="#">CVE-2023-6883</a>	The Easy Social Feed plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on multiple AJAX functions in all versions up to, and including, 6.5.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to perform unauthorized actions, such as modifying the plugin's Facebook and Instagram access tokens and updating group IDs.
<a href="#">CVE-2023-1400</a>	The Modern Events Calendar Lite WordPress plugin before 6.5.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).

Setelah menemukan kerentanan tersebut, Pentester tidak dapat melakukan eksploitasi terhadap kerentanan tersebut dan proses evaluasi berakhir hanya sampai pencarian kerentanan dengan memanfaatkan CVE records.



Last Page