FORTIFY TECH
Security Assessment Findings Report

Business Confidential

Date: May 8th, 2021
Project: EH-Modul4-7
Version 1.0

Confidentiality Statement

This document is the exclusive property of Fortify Tech and CyberShield. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Fortify Tech and Modul 4-7 Ethical Hacking.

Fortify Tech may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. CyberShield prioritized the assessment to identify the weakest security controls an attacker would exploit. CyberShield recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

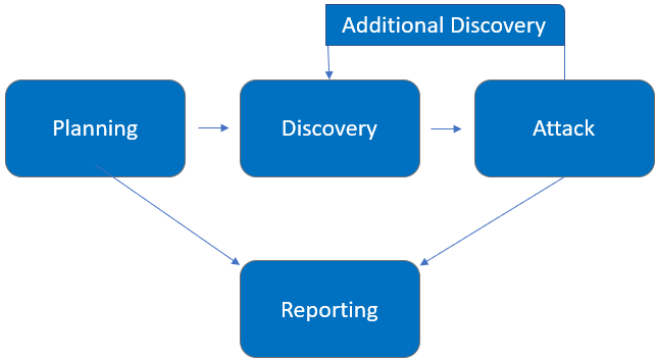
Name	Title	Contact Information
Fortify Tech		
Admin	Fortify Tech Website Admin	Email: admin@fortifytech.com
CyberShield		
Muhammad Afif	Penetration Practicum Tester	Email: afifsdi@gmail.com

Assessment Overview

From May 5th, 2024 to May 8th, 2024, Fortify Tech engaged CyberShield to evaluate the security posture of its infrastructure compared to current industry best practices that included an external network penetration test. All testing performed is based on the 4th to 7th module of Ethical Hacking Practicum by KCKS Lab.

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 from outside the network. An outsider will scan the network to identify potential host vulnerabilities and perform common and advanced blackbox network attacks, such as: man-in-the-middle attacks, password brute force, and more. The outsider will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

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.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
External Penetration Test	• 10.15.42.36 • 10.15.42.7

Scope Exclusions

Per client request, CyberShield did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by Fortify Tech.

Client Allowances

Fortify Tech provided CyberShield the following allowances:

- Default access to the scope IP

Executive Summary

CyberShield evaluated Fortify Tech's security posture through penetration testing from May 5th, 2024 to May 8th, 2024. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. External network penetration testing was permitted for four (4) business days.

Testing Summary

The network assessment evaluated Fortify Tech's external network security posture. From an outsider perspective, the CyberShield team performed vulnerability scanning against all IPs provided by Fortify Tech to evaluate the overall patching health of the network. The team also performed common brute force password attacks. Beyond vulnerability scanning and brute force attack, the CyberShield evaluated other potential risks, such as open file shares, default credentials on servers/devices, and sensitive information disclosure to gain a complete picture of the network's security posture.

The CYBERSHIELD team discovered that wordpress user enumeration was activated (Finding PT-001), which permit outsider to get all registered user on the website. This finding can make it easier for outside attacker to carry out brute force attack since the possibility scope become smaller. Brute force usually used to find access by guessing the matched username and password, but since the usernames is already discovered, attacker only need to guess the password.

With default vulnerability scan (Finding PT-002), the team was able to discover a vulnerability that able to lower the network security by the help of man in the middle.

Unfortunately, the CYBERSHIELD team was not able to receiving admin access in both provided Ips. More information and time are needed to get more valuable information. The remainder of the findings were high, moderate, low, or informational. For further information on findings, please review the Technical Findings section.

Tester Notes and Recommendations

During testing, the easiest vulnerability to be accessed is wordpress user enumeration, which can be accessed through the website route, while the MITM (man-in-the-middle) vulnerability still need another party to be fully useful.

We recommended that Fortify Tech patch the current wordpress website route and add some popular wordpress plugin such as Stop User Enumeration to prevent the vulnerability.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Observed some scanning of common enumeration tools (Nuclei)

The following identifies the key weaknesses identified during the assessment:

1. User enumeration is activated in wordpress
2. SSH is open for MITM attack

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

13	5	6	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
External Penetration Test		
PT-001: Wordpress User Enumeration	Low	Use Stop User Enumeration Wordpress plugin
PT-002: CVE-2023-48795 in 10.15.42.7	Moderate	Update Open SSH and improve security.

Technical Findings

External Penetration Test Findings

Finding PT-001: Wordpress User Enumeration (Low)

Description:	User enumeration is activated, which allow outsider to receive all registered user
Risk:	Low – the data is not really useful since it still require brute force to gain access
System:	10.15.42.7
Tools Used:	nuclei
References:	https://hackertarget.com/wordpress-user-enumeration/

Evidence

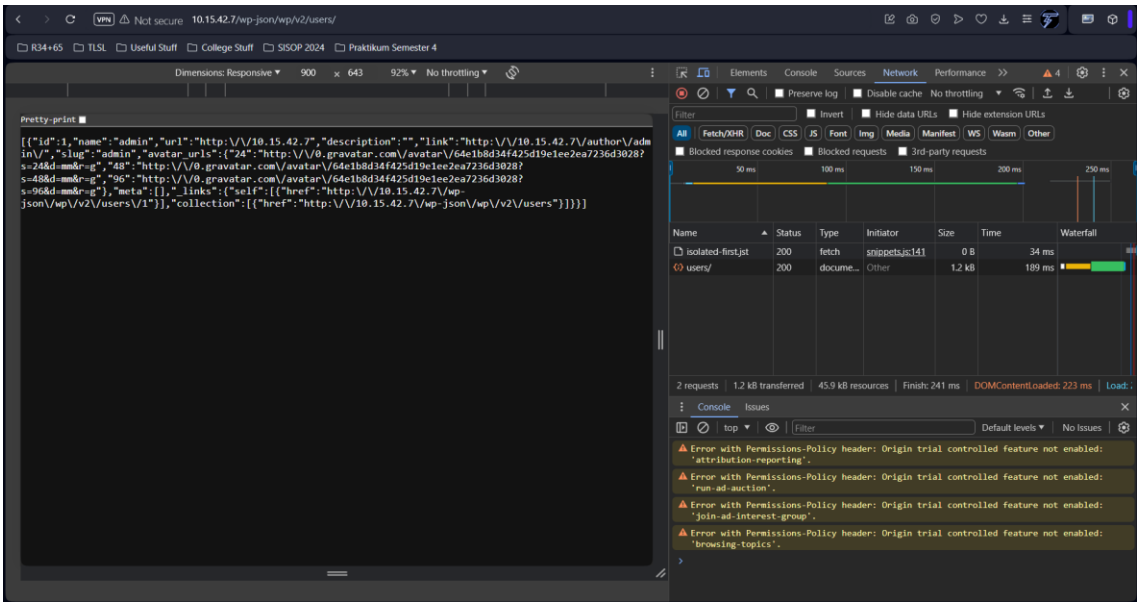


Figure 1: Captured Id and name of user admin

Remediation

Use Stop User Enumeration plugin for Wordpress

Finding PT-002: CVE-2023-48795 in 10.15.42.7 (Moderate)

Description:	Vulnerability in SSH which allow MITM attack called Tatapin that can allow attacker to lower SSH security and get easier access to SSH
Risk:	Moderate – the vulnerability can allow outsider to gain access through MITM
System:	10.15.42.7
Tools Used:	Nuclei
References:	https://packetstormsecurity.com/search/files/page2/?q=CVE-2023-48795

Evidence

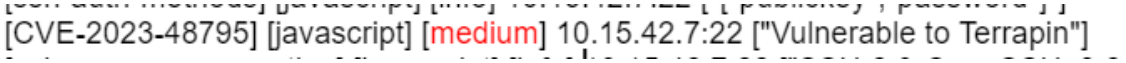


Figure 2: Nuclei Scan Screenshot

Remediation

Update OpenSSH and improve security

Additional Scans and Reports

CYBERSHIELD provides all clients with all report information gathered during testing. This includes Nessus files and full vulnerability scans in detailed formats. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by CYBERSHIELD.

The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depth opportunities. For more information, please see the documents in this repo folder labeled “additionals”.

Last Page