# FortifyTech Security Assessment Findings Report

Business Confidential

*Date : May 8th, 2024 Project: Version 1.0*

# Table of Contents

## Confidentiality Statement

This document is the exclusive property of FortifyTech 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 FortifyTech and .

FortifyTech 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. prioritized the assessment to identify the weakest security controls an attacker would exploit.  recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

## Contact Information

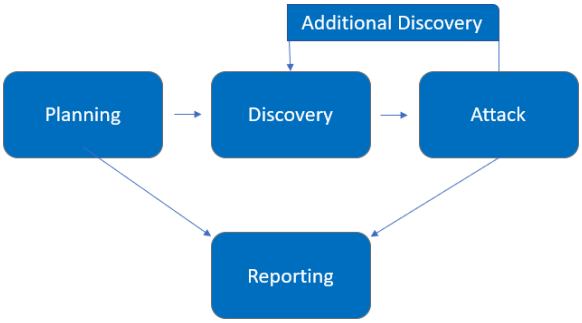
| Name | Title | Contact Information |
|---|---|---|
| FortifyTech | | |
| Azzahra Sekar Rahmadina | Penetration Tester | Email: zaraxxxxx@gmail.com |

# Assessment Overview

From May 6th, 2024 to May 8th, 2024, Fortify Tech engages CyberShield to evaluate its infrastructure security posture against current industry best practices, including external penetration testing

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. |

# 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 |
| --- | --- |
| Internal Penetration Test | - 10.15.42.36<br>- 10.15.42.7 |

## Scope Exclusions

As per the client's request, CyberShield refrains from conducting attacks on unethical targets during testing. Pentesting can only be done using the ITS network (use ITS VPN or ITS wifi).

## Client Allowances

Fortify Tech doesn't provide any allowances to assist with testing.

# Executive Summary

CyberShield evaluated FortifyTech's internal security posture through penetration testing from May 6th, 2024 to May 8th, 2024. By leveraging a series of attacks, CyberShield identified several moderate-level vulnerabilities. It is advised to create an action plan and patch after addressing the highest priority issues.

## Scoping and Time Limitations

Scoping during the engagement did not permit things that violate ethics. Time limitations were in place for testing. Penetration testing was permitted for four (4) days.

## Testing Summary

Using Nmap to gather information about services, applications, devices, and other elements that we will test for security vulnerabilities.

## Security Strengths and Weaknesses

### Anonymous FTP Login

Vulnerability found in FTP Login, The FTP service allows anonymous login (FTP code 230), which could lead to unauthorized access to sensitive files or data if not properly secured.

### Network Configuration Discrepancy

The Passive Mode (PASV) IP address reported by the FTP server is inconsistent. The reported PASV IP address, 172.19.0.2, differs from the expected IP address of 10.15.42.36. This inconsistency indicates a potential vulnerability or misconfiguration in the network setup. Such discrepancies could lead to confusion, misrouting of traffic, or unauthorized access attempts.

### Open SSH Version

The SSH service is running an older version of OpenSSH (8.2p1), which may contain known vulnerabilities that could be exploited by attackers to gain unauthorized access or execute arbitrary command

### Outdated WordPress Plugin (Forminator)

Identified by the template: [wordpress-forminator:outdated_version] [http] [info]
Explanation: This line indicates the detection of an outdated version of the Forminator plugin (1.24.6) on the scanned URL, with information about the last known version (1.28.0).

### Exposed WordPress Usernames Enumeration

Identified by the template: [wp-user-enum:usernames] [http] [low]
Explanation: This line indicates the detection of a low-risk vulnerability related to WordPress usernames enumeration through the WordPress REST API endpoint (/wp-json/wp/v2/users/).

### HTTP Service

The HTTP service is running on port 8888 and presents a login page, suggesting a web application that may be vulnerable to authentication bypass, SQL injection, or other web-based attacks.

# Vulnerability Summary & Report Card

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

## Internal Penetration Test Findings

| 0 | 1 | 4 | 1 | 0 |
|---|---|---|---|---|
| Critical | High | Moderate | Low | Informational |

| Finding | Severity | Recommendation |
|---|---|---|
| Internal Penetration Test | | |
| IPT-001: Network Configuration Discrepancy | Moderate | Disable anonymous FTP login or restrict access to authorized users only. |
| IPT-002: Open SSH Version | High | Update the OpenSSH service to the latest version to mitigate known vulnerabilities. |
| IPT-003: HTTP Service | Moderate | Perform a thorough security assessment of the HTTP service to identify and patch any vulnerabilities in the web application. |
| IPT-004: Anonymous FTP Login | Moderate | Restrict token delegation. |
| IPT-005: Outdated WordPress Plugin (Forminator) | Moderate | Update the Forminator plugin to the latest version (1.28.0) to address any known vulnerabilities. |

| | | |
|---|---|---|
| IPT-006: Exposed WordPress Usernames Enumeration | Low | Disable or restrict access to the WordPress REST API endpoints to prevent enumeration of user information. |

## Technical Findings

Network Configuration Discrepancy

| | |
|---|---|
| Description | |
| Risk | Likelihood: Moderate - The likelihood of this discrepancy being exploited depends on various factors such as the attacker's knowledge, intent, and the existence of other vulnerabilities in the network<br><br>Impact: Moderate - Inconsistent configurations pose risks of service disruption and unauthorized access, impacting network integrity. |
| System | 10.15.42.36 |
| Tools Used | Nmap |
| References | - |

Evidence

```
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 172.19.0.2 is not the same as 10.15.42.36
```

Remediation

To address this issue, ensure consistency in the network configuration by verifying and correcting the PASV IP address in the FTP server settings. Conduct regular audits of network configurations to prevent similar discrepancies in the future

Open SSH Version

| | |
|---|---|
| Description | The likelihood of exploitation is high as older versions of OpenSSH may contain known vulnerabilities that are actively exploited by attackers. Exploiting these vulnerabilities could result in unauthorized access, data theft, or system compromise. The impact is high as SSH is a critical service for remote access, and a successful attack could lead to significant data breaches or system compromise. |
| Risk | Likelihood: HIgh<br><br>Impact: High |
| System | 10.15.42.36 |
| Tools Used | Nmap |
| References | - |

Evidence

```
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))
```

Remediation

To address this issue, Update the OpenSSH service to the latest version to mitigate known vulnerabilities.

HTTP Service

| | |
|---|---|
| Description | The likelihood of exploitation is moderate as web applications are commonly targeted by attackers. The impact could be moderate to high depending on the specific vulnerabilities present in the web application, such as authentication bypass, SQL injection, or remote code execution. Successful exploitation could lead to unauthorized access, data theft, or compromise of the web server, impacting confidentiality, integrity, and availability. |

| | |
|---|---|
| Risk | Likelihood: Moderate<br><br>Impact: Moderate to High |
| System | 10.15.42.36 |
| Tools Used | Nmap |
| References | - |

Evidence

```
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Login Page
```

Remediation

Perform a thorough security assessment of the HTTP service to identify and patch any vulnerabilities in the web application.

Anonymous FTP Login

| | |
|---|---|
| Description | Vulnerability found in FTP Login, The FTP service allows anonymous login (FTP code 230), which could lead to unauthorized access to sensitive files or data if not properly secured. |
| Risk | Likelihood: Moderate<br><br>Impact: Moderate |
| System | 10.15.42.36 |
| Tools Used | Nmap |
| References | - |

Evidence

```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

Remediation

Restrict token delegation.

Outdated WordPress Plugin (Forminator)

| | |
|---|---|
| Description | Identified by the template: [wordpress-forminator:outdated_version] [http] [info]. The presence of an outdated plugin (Forminator 1.24.6) increases the likelihood of exploitation by attackers targeting known vulnerabilities. The impact could range from unauthorized access to data breaches, depending on the severity of the vulnerabilities present in the outdated plugin. |
| Risk | Likelihood: Moderate<br><br>Impact: Moderate |
| System | 10.15.42.7 |
| Tools Used | Nuclei |
| References | - |

Evidence


Remediation

Update the Forminator plugin to the latest version (1.28.0) to address any known vulnerabilities.

Exposed WordPress Usernames Enumeration

| | |
|---|---|
| Description | Identified by the template: [wp-user-enum:usernames] [http] [low]. While the enumeration of usernames exposes information about users registered on the WordPress site, the impact is mitigated as it does not directly lead to unauthorized access or compromise of sensitive data. However, it still poses a privacy risk to site users and may aid attackers in crafting targeted attacks |
| Risk | Likelihood: Low<br><br>Impact: Low |
| System | 10.15.42.7 |
| Tools Used | Nuclei |
| References | - |

Evidence

```
[metatag-cms] [http] [info] http://10.15.42.7 [WordPress 6.5.2]
[wordpress-rdf-user-enum] [http] [info] http://10.15.42.7/feed/rdf/ [admin]
```

Remediation

Disable or restrict access to the WordPress REST API endpoints to prevent enumeration of user information.

\

# Last Page