# FortifyTech
# Security Assessment Findings Report

Business Confidential

*Date: May 8th, 2024*

# Table of Contents

# Confidentiality Statement

This document is the exclusive property of FortifyTech. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of FortifyTech

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

# Contact Information

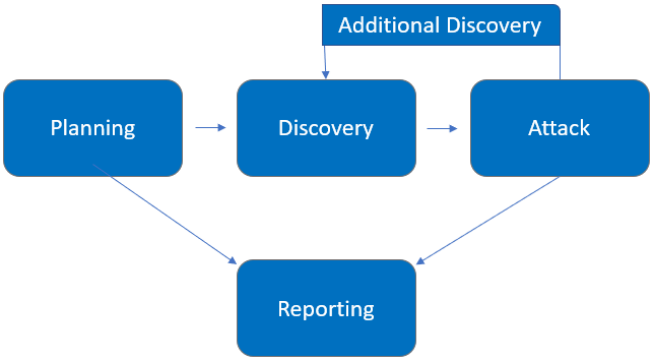
| Name | Title | Contact Information |
|---|---|---|
| Pentester | | |
| Etha Felisya Br Purba | Lead Penetration Tester | Office: (555) 555-5555<br>Email: felisyaetha@gmail.com |

# Assessment Overview

From May 5th, 2024 to May 8th, 2024, DC engaged TCMS to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

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. |

# Scope

| Assessment | Details |
| --- | --- |
| External Penetration Test | 10.15.42.36<br>10.15.42.7 |

# Executive Summary

FortifyTech underwent an external network penetration test conducted by an IT student from May 5th to May 8th, 2024. The assessment revealed vulnerabilities categorized at medium and low levels of severity.

Key Findings:

- Medium-level vulnerabilities pose a moderate risk to FortifyTech's security posture and require immediate attention.

- Low-level vulnerabilities, while less severe, still contribute to the overall risk landscape and should be addressed.

Recommendations:

- Prioritize mitigation of medium-level vulnerabilities to prevent potential security breaches.

- Address low-level vulnerabilities systematically to enhance overall security posture.

- Implement robust security controls and practices to fortify defenses against potential threats.

Conclusion:

Addressing the identified vulnerabilities promptly and implementing robust security measures will strengthen FortifyTech's defenses and mitigate the risk of security incidents. Ongoing monitoring and periodic assessments are essential for maintaining an effective security posture.

## Attack Summary

The following table describes how I gained internal network access, step by step:

| Step | Action | Recommendation |
|---|---|---|
| 1 | Obtained historical breached account credentials to leverage against all company login pages | Discourage employees from using work e-mails and usernames as login credentials to other services unless necessary |
| 2 | Attempted a "credential stuffing" attack against Outlook Web Access (OWA), which was unsuccessful. However, OWA provided username enumeration, which allowed TCMS to gather a list of valid usernames to leverage in further attacks. | Synchronize valid and invalid account messages. |
| 3 | Performed a "password spraying" attack against OWA using the usernames discovered in step 2. TCMS used the password of Summer2018! (season + year + special character) against all valid accounts and gained access into the OWA application. | OWA permitted authenticated with valid credentials. TCMS recommends DC implement Multi-Factor Authentication (MFA) on all external services.<br><br>OWA permitted unlimited login attempts. TCMS recommends DC restrict logon attempts against their service.<br><br>TCMS recommends an improved password policy of: 1) 14 characters or longer 2) Use different passwords for each account accessed. 3) Do not use words and proper names in passwords, regardless of language<br><br>Additionally, TCMS recommends that DC:<br>▪ Train employees on how to create a proper password |
| 4 | Leveraged valid credentials to log into VPN | OWA permitted authenticated with valid credentials. TCMS recommends DC implement Multi-Factor Authentication (MFA) on all external services. |

# Security Strengths

## SIEM alerts of vulnerability scans

During the assessment, the DC security team alerted TCMS engineers of detected vulnerability scanning against their systems. The team was successfully able to identify the TCMS engineer's attacker IP address within minutes of scanning and was capable of blacklisting TCMS from further scanning actions.

# Security Weaknesses

## FTP Server Detection

An FTP server is listening on a remote port. It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

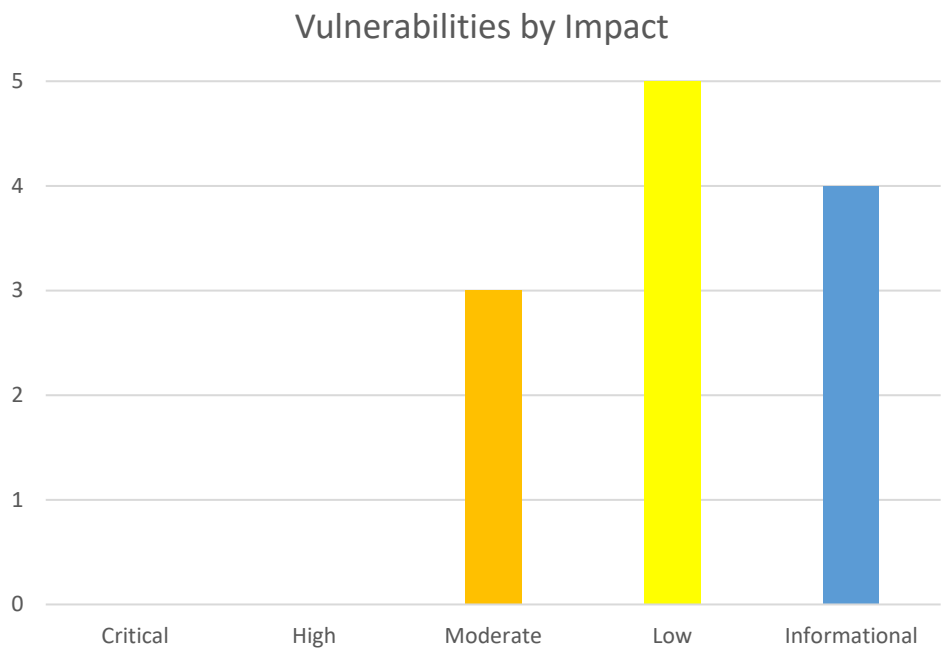
## Vulnerable to Terappin

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack.

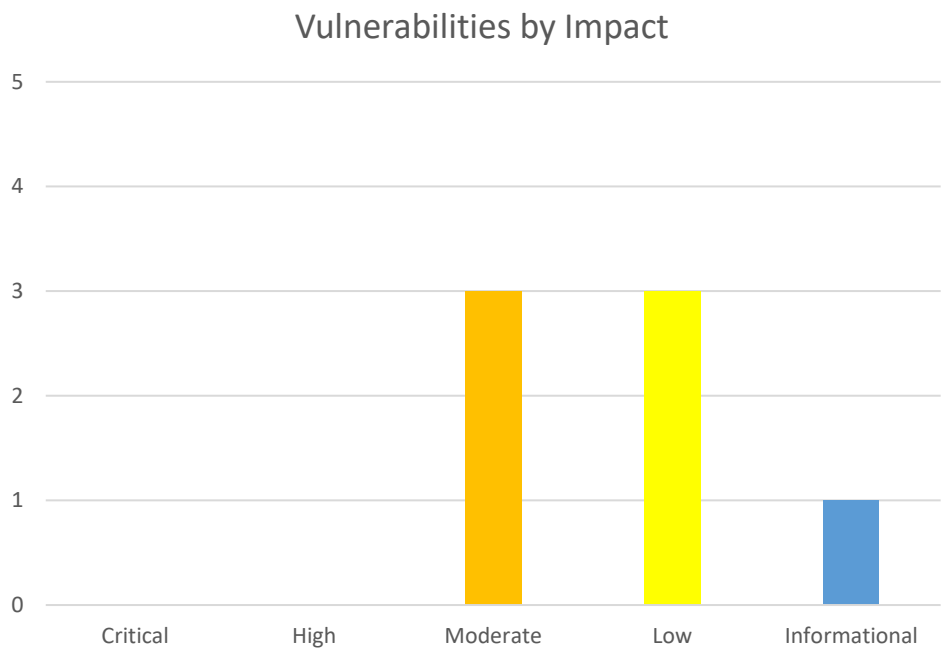
# Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:

http://10.15.42.7



http://10.15.42.36:8888



## External Penetration Test Findings

Through scanning by using OWASP-ZAP, Nuclei, and WPscan, there are several security vulnerabilities found on the server.

### Absence of Anti-CSRF Tokens (Medium)

| | |
|---|---|
| **Description:** | The web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request. |
| **Impact:** | Medium |
| **System:** | 10.15.42.7 |
| **References:** | CWE - CWE-352: Cross-Site Request Forgery (CSRF) (4.14) (mitre.org) |

### Content Security Policy (CSP) Header Not Set (Medium)

| | |
|---|---|
| **Description:** | The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. |
| **Impact:** | Medium |
| **System:** | 10.15.42.7 |
| **References:** | CWE - CWE-693: Protection Mechanism Failure (4.14) (mitre.org) |

### Missing Anti-clickjacking Header (Medium)

| | |
|---|---|
| **Description:** | The web application does not restrict or incorrectly restricts frame objects or UI layers that belong to another application or domain, which can lead to user confusion about which interface the user is interacting with. |
| **Impact:** | Medium |
| **System:** | 10.15.42.7 |
| **References:** | CWE - CWE-1021: Improper Restriction of Rendered UI Layers or Frames (4.14) (mitre.org) |

### Cookie No HttpOnly Flag (Low)

| | |
|---|---|
| **Description:** | The product uses a cookie to store sensitive information, but the cookie is not marked with the HttpOnly flag. |
| **Impact:** | Low |
| **System:** | 10.15.42.7 |
| **References:** | CWE - CWE-1004: Sensitive Cookie Without 'HttpOnly' Flag (4.14) (mitre.org) |

Cookie without SameSite Attribute (Low)

| | |
|---|---|
| Description: | The SameSite attribute for sensitive cookies is not set, or an insecure value is used. |
| Impact: | Low |
| System: | 10.15.42.7 |
| References: | CWE - CWE-1275: Sensitive Cookie with Improper SameSite Attribute (4.14) (mitre.org) |

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (Low)

| | |
|---|---|
| Description: | The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information. |
| Impact: | Low |
| System: | 10.15.42.7 |
| References: | CWE - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (4.14) (mitre.org) |

Absence of Anti-CSRF Tokens (Medium)

| | |
|---|---|
| Description: | The web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request. |
| Impact: | Medium |
| System: | 10.15.42.36 |
| References: | CWE - CWE-352: Cross-Site Request Forgery (CSRF) (4.14) (mitre.org) |

Content Security Policy (CSP) Header Not Set (Medium)

| | |
|---|---|
| Description: | The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. |
| Impact: | Medium |
| System: | 10.15.42.36 |
| References: | CWE - CWE-693: Protection Mechanism Failure (4.14) (mitre.org) |

Missing Anti-clickjacking Header (Medium)

| | |
|---|---|
| **Description:** | The web application does not restrict or incorrectly restricts frame objects or UI layers that belong to another application or domain, which can lead to user confusion about which interface the user is interacting with. |
| **Impact:** | Medium |
| **System:** | 10.15.42.36 |
| **References:** | CWE - CWE-1021: Improper Restriction of Rendered UI Layers or Frames (4.14) (mitre.org) |

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (Low)

| | |
|---|---|
| **Description:** | The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information. |
| **Impact:** | Low |
| **System:** | 10.15.42.36 |
| **References:** | CWE - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (4.14) (mitre.org) |

X-Content-Type-Options Header Missing (Low)

| | |
|---|---|
| **Description:** | The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. |
| **Impact:** | Low |
| **System:** | 10.15.42.36 |
| **References:** | CWE - CWE-693: Protection Mechanism Failure (4.14) (mitre.org) |

CVE-2023-48795 - Vulnerable to Terappin (Medium)

| | |
|---|---|
| **Description:** | The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. |
| **Impact:** | Medium |
| **System:** | - 10.15.42.7<br>- 10.15.42.36:22 |
| **References:** | - CVE-2023-48795 |

I successfully gained access to the FTP server of 10.15.42.36 using the command ftp 10.15.42.36. Gaining unauthorized access to the FTP server, can lead to various security risks such as data theft, data manipulation, or unauthorized file uploads/downloads.

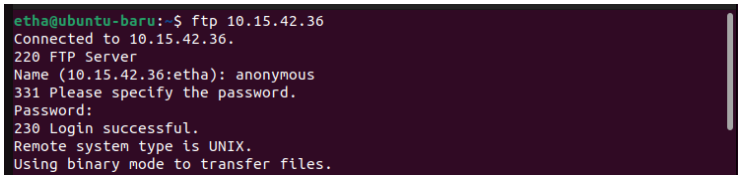



*Figure 1: Connecting to the FTP Server 10.15.42.36*

Here, I found a directory containing a .sql file.

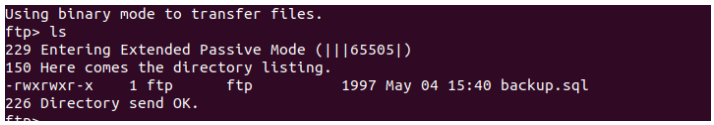



*Figure 2: Listing the directories*

Then, I opened the backup.sql file and found a username and password. Although the password is hashed, it is important to ensure that only authorized users have access to the database.


*Figure 3: Username and hashed password found in 'users' tables*

## Remediation

| | |
|---|---|
| **Who:** | IT Team |
| **Vector:** | Remote |
| **Action:** | Item 1: VPN and OWA login with valid credentials did not require Multi-Factor Authentication (MFA). TCMS recommends DC implement and enforce MFA across all external-facing login services.<br><br>Item 2: OWA permitted unlimited login attempts. TCMS recommends DC restrict logon attempts against their service.<br><br>Item 3: DC permitted a successful login via a password spraying attack, signifying a weak password policy. TCMS recommends the following password policy, per the Center for Internet Security (CIS):<br>▪ 14 characters or longer<br>▪ Use different passwords for each account accessed<br>▪ Do not use words and proper names in passwords, regardless of language<br><br>Item 4: OWA permitted user enumeration. TCMS recommends DC synchronize valid and invalid account messages.<br><br>Additionally, TCMS recommends that DC:<br>▪ Train employees on how to create a proper password<br>▪ Check employee credentials against known breached passwords<br>▪ Discourage employees from using work e-mails and usernames as login credentials to other services unless absolutely necessary |

## Additional Reports and Scans (Informational)

TCMS provides all clients with all report information gathered during testing. This includes vulnerability scans and a detailed findings spreadsheet. For more information, please see the following documents:

- Demo Company-867-19 Full Findings.xslx
- Demo Company-867-19 Vulnerability Scan Summary.xslx
- Demo Company-867-19 Vulnerability Scan by Host.pdf

# Last Page