Fortify Tech

Fortify Tech
Security Assessment Findings Report

Business Confidential

Date: May 5th, 2024
Project: 897-19
Version 1.0

Table of Contents

Confidentiality Statement

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

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

Contact Information

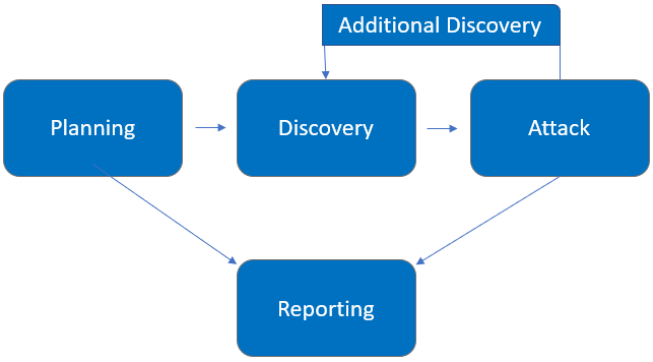
Name	Title	Contact Information
FortifyTech		
Muhammad Azril	CEO	azril@gmail.com
CyberShield		
Gabriella Erlinda	Penetration Tester	gabriella8803@gmail.com

Assessment Overview

From May 5th, 2024 to May 8th, 2024, FT engaged CS 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 CS 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.
Medium	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, 10.15.42.7

- The only scope information provided by FT was two IP Address mentioned above

Executive Summary

CS evaluated FT's external security posture through an external network penetration test from May 5th, 2024 to May 8th, 2024. By leveraging a series of attacks, CS found critical level vulnerabilities that allowed full internal network access to the FT headquarter office. It is highly recommended that FT address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

Attack Summary

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

Step	Action	Recommendation
1	Gained access through FTP server of **10.15.42.36**	Disable access to the FTP standard server by anonymous if possible. Use FTPS
2	Vulnerable to Terrapin	Ensure that all including web servers, frameworks, and CMS platforms, is up-to-date with the latest security patches. Vulnerabilities often arise from outdated software versions.
3	Found that Content Security Policy (CSP) Header not set	Utilize security headers such as Content Security Policy (CSP), X-Content-Type-Options, X-Frame-Options, and X-XSS-Protection to mitigate common web vulnerabilities.
4	Performed brute-force on **http://10.15.42.7/wp-login.php** Unfortunately due to time limitation, brute-force was unsuccessful	Use rate limiting to restrict the number of login attempts from a single IP address within a specific time period. This helps mitigate brute force attacks by slowing down or blocking repeated login attempts from suspicious sources. Another recommendation is by using CAPTCHA or 2FA (Two-Factort Authentication) to help prevent automated brute-force attacks

Security Strengths

Hashed Logon Password

During the assessment, the CS engineers managed to find a database of login information for the website http://10.15.42.36:8888 but thankfully it is secured by bycrypt hashing which will protect user's login information from the attacker. It is possible to reverse the hash to its original password, but it will be time consuming.

Security Weaknesses

Missing Multi-Factor Authentication

CS leveraged multiple attacks against FT login forms using valid credentials harvested through open-source intelligence. Successful logins included employee e-mail accounts through Outlook Web Access and internal access via Active Directory login on the VPN. The use of multi-factor authentication would have prevented full access and required CS to utilize additional attack methods to gain internal network access.

Weak Password Policy

CS successfully performed password guessing attacks against FT login forms, providing internal network access. A predictable password format of Summer2018! (season + year + special character) was attempted and successful.

Unrestricted Logon Attempts

During the assessment, CS performed brute-force attacks against login forms found on the network. For all logins, unlimited attempts were allowed eventhough in this task, CS didn't manage to get the successful login information

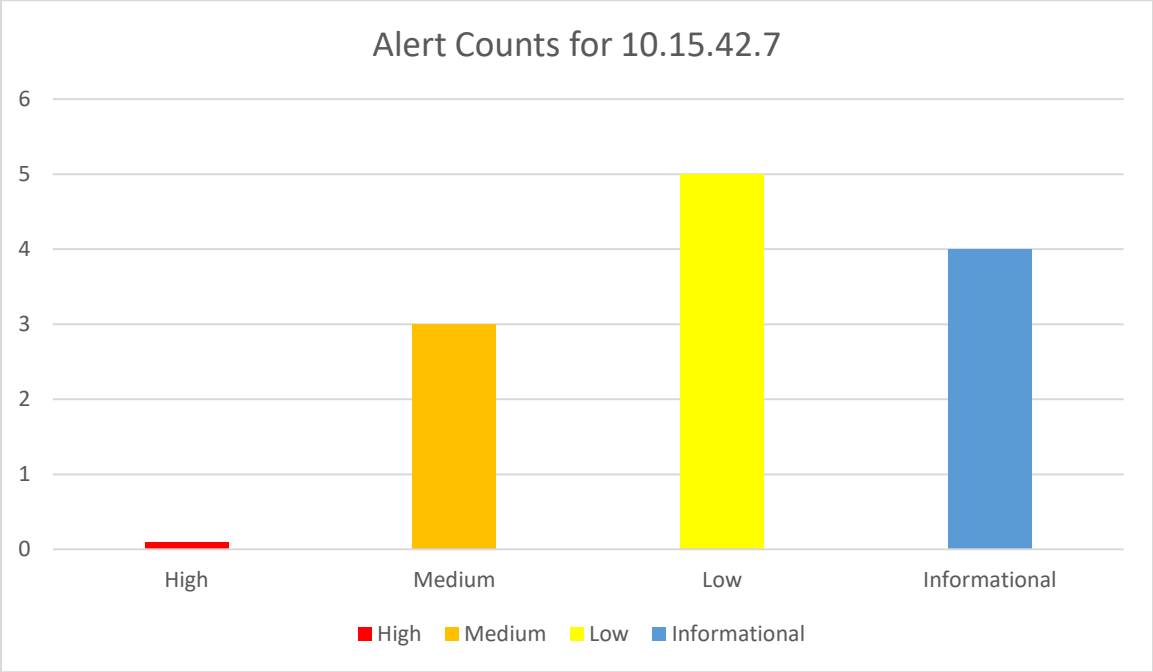
Unprotected FTP server

FTP server can be access through remote port which give attacker the possibility to modify databases or files in the network

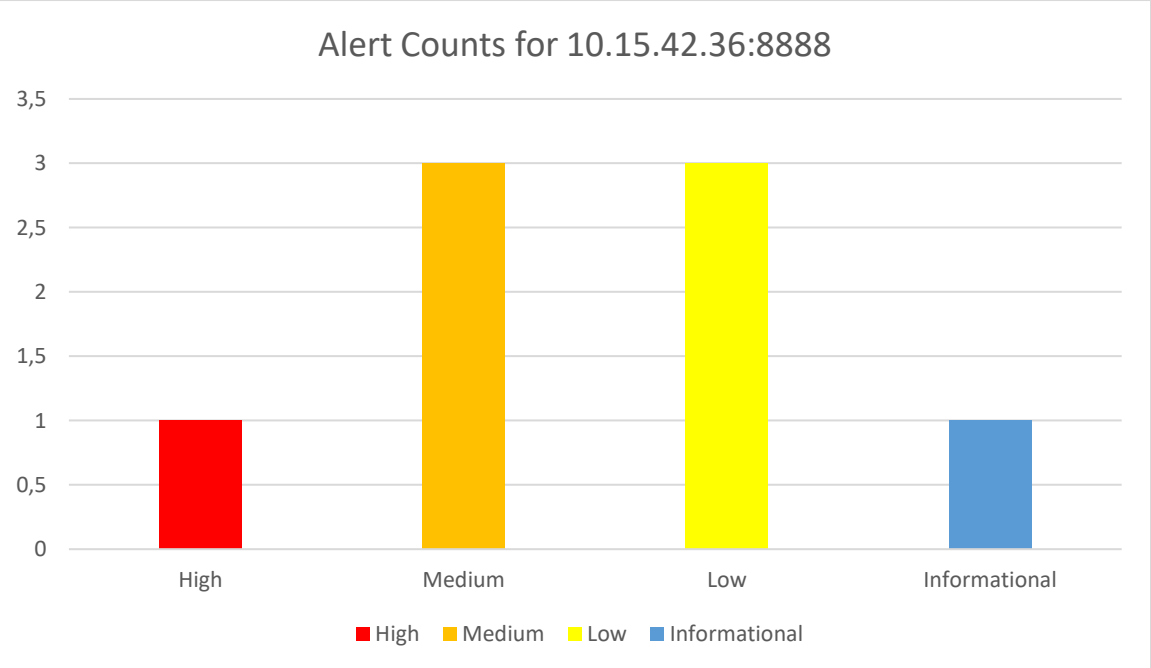
Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:

10.15.42.7



10.15.42.36:8888



External Penetration Test Findings

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-1021: Improper Restriction of Rendered UI Layers or Frames

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. This weakness covers three distinct situations. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.
Impact:	Medium
System:	10.15.42.7
References:	CWE-693: Protection Mechanism Failure

PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability (High)

Description:	According to its self-reported version number, the version of PHP running on the remote web server is 7.2.x or 7.3.x prior to 7.3.21. It is, therefore affected by a memory leak vulnerability in the LDAP component. An unauthenticated, remote attacker could exploit this issue to cause a denial-of-service condition.
Impact:	High
System:	10.15.42.36:8888
References:	CVE-2020-0420

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:	10.15.42.36:8888

References:	CWE-352: Cross-Site Request Forgery (CSRF)

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:	10.15.42.36:8888
References:	CWE-693: Protection Mechanism Failure

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:	10.15.42.36:8888
References:	CWE-1021: Improper Restriction of Rendered UI Layers or Frames

SSH Terrapin Prefix Truncation Weakness (Medium)

Description:	The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security. Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions.
Impact:	Medium
System:	10.15.42.36:8888
References:	CVE-2023-48795: SSH Terrapin Prefix Truncation Weakness

Server Leaks Version Information via "Server" HTTP Response Header Field (Low)

Description:	The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.
Impact:	Low
System:	10.15.42.36:8888
References:	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

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:	10.15.42.36:8888
References:	CWE-693: Protection Mechanism Failure

FTP Server Detection (Informational)

Description:	It is possible to obtain the banner of the remote FTP server by connecting to a remote port.
Impact:	Informational
System:	10.15.42.36:8888
References:	IAVT: 0001-T-0030, 0001-T-0943

Proof of finding

Using ftp command `ftp 10.15.42.36` I managed to gain access through the FTP server and found a database called backup.sql

```
gabriellae11@LAPTOP-QOCL5PUI:~$ ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:gabriellae11): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||65511|)
150 Here comes the directory listing.
-rwxrwxr-x    1 ftp      ftp          1997 May 04 15:40 backup.sql
226 Directory send OK.
```

Figure 1. gain access to ftp server of 10.15.42.36 and found a database file

By using `more backup.sql` I successfully read the database file which contains the username and hashed password of the admin from 10.15.42.36:8888

```
LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
INSERT INTO `users` VALUES (1,'admin','$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K');
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
```

Figure 2. Found the content of the database.sql

The port 8888 was obtain by using nmap -sV -sC 10.15.42.36. It shows that there is a port 8888 directed to a Login Page (http) while if I search only the IP without the port, the web browser didn't show anything

```
gabriellae11@LAPTOP-QOCL5PUI:~$ nmap -sV -sC 10.15.42.36
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-07 15:51 WIB
Nmap scan report for 10.15.42.36
Host is up (0.013s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.33.3.209
|      Logged in as ftp
|      TYPE: ASCII
|      Session bandwidth limit in byte/s is 6250000
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
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))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Login Page
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.18 seconds
```

Figure 3. nmap port scanning 10.15.42.36

Additional Reports and Scans (Informational)

For additionals report and finding, you can refer to my github repository on:

[Github Repository for FortifyTech Pentesting Report]

Fortify Tech

Last Page