

CyberShield



FortifyTech

Security Assessment Findings Report

Business Confidential

Date: May 8th, 2024

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 CyberShield.

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.

The penetration was conducted by CyberShield on May 5-8, 2024 focusing on two predefined scopes, with the primary objective of identifying and exposing possible vulnerabilities in the system. The actions were geared towards strengthening security defenses by finding weak points that attackers might exploit.

Contact Information

| Name | Title | Contact Information |
|--------------|-------------------------------------|-----------------------------|
| Fortify Tech | | |
| Fort | Global Information Security Manager | Email: fort@fortifytech.com |
| CyberShield | | |
| Anda | Lead Penetration Tester | Email: anda@cybershield.com |

Assessment Overview

From May 5, 2024 to May 8, 2024, FortifyTech has contracted CyberShield to conduct a security evaluation of the defined scope through a penetration test. This was intended to gain a deep understanding of the security vulnerabilities that may exist and to identify potential attacks that could occur.

Phases of penetration testing activities include the following:

1. Reconnaissance:

- Identify public information about the target, such as IP address, domain name, and company information.
- Network scanning to identify active hosts and running services.
- Further information gathering through open search and other techniques to understand the system architecture.

2. Vulnerability Assessment:

- Identification of weaknesses in the website running on the specified host.
- Automated scanning using specialized software to detect common vulnerabilities

3. Reporting:

- Documentation of all findings related to the reconnaissance phase, including information gathered, targets identified, and potential areas of attack.
- A summary of the results of the vulnerability assessment, including a list of vulnerabilities found, their severity, as well as appropriate remediation recommendations

Assessment Components

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man-in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer 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 |
|---------------------------|-------------------------------|
| Internal Penetration Test | 10.15.42.36 10.15.42.7 |

Scope Exclusions

CyberShield adheres to the highest ethical standards, including the avoidance of Denial of Service (DoS) and Phishing/Social Engineering. All other non-lossful attack techniques are permitted by FortifyTech.

Client Allowances

FortifyTech provided CyberShield the following allowances:

- Internal access to network via ITS VPN

Executive Summary

TCMS evaluated Demo Corp's internal 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. Internal network penetration testing was permitted for 4 (four) days.

Testing Summary

In testing using nmap on the Linux platform, the focus was on finding vulnerabilities in two specific scopes. The test results indicated a vulnerability in a particular system, where an FTP service with anonymous login was discovered that could grant access without authentication. This resulted in potential information leakage or misuse of access that could compromise system security. In addition, through analysis of the WordPress platform version 6.5.2, potential weaknesses were detected that could be exploited for XSS (Cross-Site Scripting) attacks, which could lead to the injection of malicious scripts and threaten the integrity and security of user data.

In this context, the discovery of vulnerabilities through nmap demonstrates the urgency of taking remedial action and strengthening security on affected systems. Enhancing FTP security by eliminating anonymous logins and implementing appropriate updates and countermeasures on the WordPress platform are crucial steps to mitigate the risk of attacks and maintain overall system integrity and security. By understanding and addressing the vulnerabilities detected, we can minimize the potential negative impact and protect the system from threats that may arise.

Tester Notes and Recommendations

It is necessary to immediately address the vulnerabilities found, such as disabling anonymous login on FTP services and performing security updates and security enhancements on the WordPress platform version 6.5.2. In addition, it is recommended to regularly perform security scans and active monitoring of the system to detect and address emerging vulnerabilities, as well as implement strong security practices, such as

the use of strong passwords and regular software updates, to minimize the potential risk of attacks and maintain continuous system security.

Key Strengths and Weaknesses

- The following identifies the key strengths identified during the assessment:

Using the latest version of wordpress and apache so that to attack requires adequate skills and tools.

- The following identifies the key weaknesses identified during the assessment:

The system is vulnerable to exploitation due to using anonymous login on ftp service.

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

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

| Finding | Severity | Recommendation |
|---|----------|---|
| IPT-01: Anonymous login via FTP on 10.15.42.36 | High | Disable the anonymous login option on FTP services |
| IPT-02: XSS vulnerability in 10.15.42.7 running WordPress 6.5.2 | Moderate | Update WordPress to the latest version and implement effective security plugins to protect against XSS attacks. |

Technical Findings

Internal Penetration Test Findings

Finding IPT-001: Anonymous login via FTP on 10.15.42.36 (High)

| | |
|--------------|---|
| Description: | Discovering that a system allows anonymous login via FTP can be a potentially serious security risk. With this loophole, an attacker can easily gain entry into the system without having to provide valid identification, increasing the likelihood of unauthorized access. Through anonymous FTP access, an attacker can steal sensitive information stored in the system. Furthermore, by revealing the possibility of anonymous access, the system also becomes vulnerable to more complex attacks, such as abuse of access rights, malware installation, or ransomware attacks, all of which can have a detrimental impact on the security and operations of the system. |
| Risk: | Likelihood: Low – Requires higher knowledge and skills to exploit attacks Impact: High – May cause loss of sensitive data and downtime |
| System: | All |
| Tools Used: | Nmap on Kali Linux |

Evidence

```
File Actions Edit View Help
(kali@kali)~$ nmap -sV -sC -oN nmaplog.log 10.10.10.1

# -sV: Mengetahui versi dari service
# -sC: mengetahui informasi terkait service menggunakan default nmap script
# -oN nmaplog.log: menyimpan hasil scanning pada file nmaplog.log

(kali@kali)~$ nmap -sV -sC 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 09:19 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.46 seconds

(kali@kali)~$ sudo nmap -sV -sC 10.15.42.36
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 09:20 EDT
Nmap scan report for 10.15.42.36
Host is up (0.0029s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
|_ftp-bounce: bounce working!
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rwxrwxr-x 1 ftp      1997 May 04 15:40 backup.sql
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
| 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-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 25.17 seconds

(kali@kali)~$
```

```
(kali@kali)-[~] * If your computer or network is protected by a firewall or proxy, make sure
$ ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:kali): anonymous
331 Please specify the password.
Password: 230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||65502|)
150 Here comes the directory listing.
drwxrwxr-x  2 ftp      ftp      4096 May 04 15:40 .
drwxrwxr-x  2 ftp      ftp      4096 May 04 15:40 ..
-rwxrwxr-x  1 ftp      ftp      1997 May 04 15:40 backup.sql
226 Directory send OK.
ftp> cd backup.sql
550 Failed to change directory.
```

Remediation

Configure the FTP server to disable anonymous login and ensure that only users with valid credentials can access it. Reinforce credentials by implementing complex passwords and strong authentication practices. Increase monitoring and logging of FTP activity to detect anonymous login attempts and suspicious activity, and use firewalls and filtering features to restrict access to only necessary users and to block anonymous access completely..

Finding IPT-002: XSS vulnerability in 10.15.42.7 running WordPress 6.5.2 (Moderate)

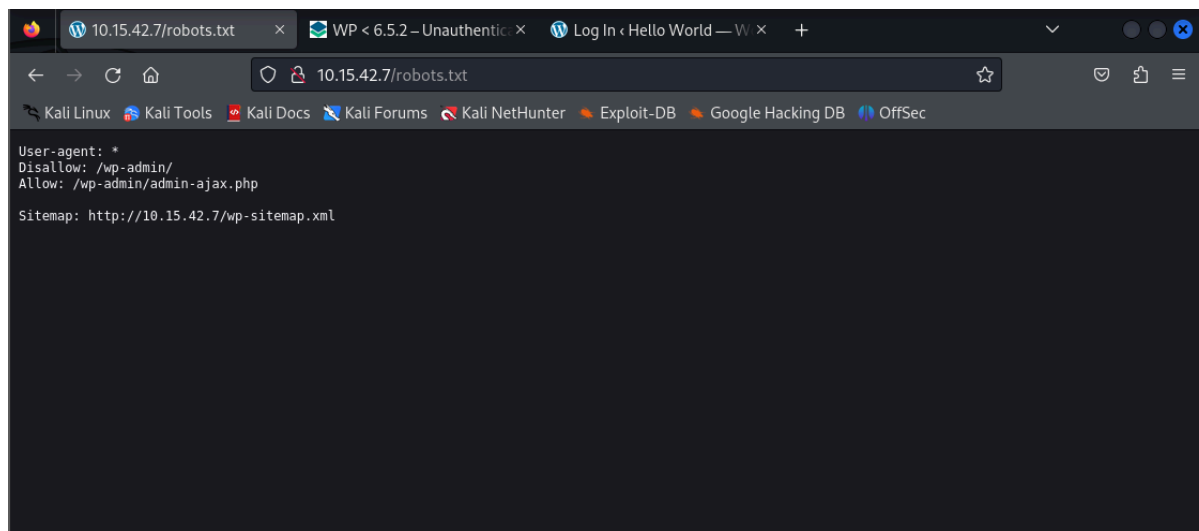
| | |
|--------------|---|
| Description: | A vulnerability was discovered on a system using WordPress 6.5.2, where this security hole occurred through an XSS (Cross-Site Scripting) attack. With this vulnerability, an attacker can insert malicious code into a web page that is then executed by the user's browser, allowing for the theft of sensitive data, redirection of the user to a fake site, or even full control of the page. |
| Risk: | <p>Likelihood: High – The vulnerability is known and can be exploited by an attacker with relative ease..</p> <p>Impact: High – Can cause significant harm such as data loss or takeover of control over the system.</p> |
| System: | All |
| Tools Used: | Nmap on Kali Linux |

Evidence

```
(kali@kali)-[~]
└─$ sudo nmap -T4 --min-rate 10000 -sCV -p- -A -Pn 10.15.42.7 -oN scan_1
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:04 EDT
Warning: 10.15.42.7 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.15.42.7
Host is up (0.017s latency).
Not shown: 40249 filtered tcp ports (no-response), 25284 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   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-robots.txt: 1 disallowed entry
|_ /wp-admin/
|_ http-server-header: Apache/2.4.59 (Debian)
|_ http-title: Hello World
Device type: WAP
Running: Actiontec embedded, Linux
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel
OS details: Actiontec MI424WR-GEN3I WAP
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
TRACEROUTE (using port 16031/tcp)
HOP RTT      ADDRESS
1   1.03 ms   192.168.13.2
2   31.16 ms  10.15.42.7
```


```
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.24 seconds
```



As a reminder, the Wordfence Intelligence Vulnerability Database API is completely free to query and utilize, both personally and commercially, and contains all the same vulnerability data as the user interface. Please review the [API documentation](#) and Webhook [documentation](#) for more information on how to query the vulnerability API endpoints and configure webhooks utilizing all the same data present in the Wordfence Intelligence user interface.

WordPress Core < 6.5.2 - Unauthenticated & Authenticated (Contributor+) Stored Cross-Site Scripting via Avatar Block

[Wordfence Intelligence](#) > [Vulnerability Database](#) > WordPress Core < 6.5.2 - Unauthenticated & Authenticated (Contributor+) Stored Cross-Site Scripting via Avatar Block



7.2

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[CVSS:3.1/AV:N/AC:L/PR:N/UI:N/SC:C/L/I:L/A:N](#)

| | |
|--------------------|---|
| CVE | CVE-2024-4439 |
| CVSS | 7.2 (High) |
| Publicly Published | April 9, 2024 |
| Last Updated | May 3, 2024 |
| Researchers | John Blackburn stealthcopter |

Description

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.

References

- [wordpress.org](#)
- [core.trac.wordpress.org](#)
- [core.trac.wordpress.org](#)
- [www.wordfence.com](#)

Share



Remediation

Implementation of updates to the latest version of WordPress, use of security plugins that counter XSS attacks, as well as strict validation of user input to prevent insertion of malicious scripts

Last Page