

# Security Assessment Finding Report



**FortifyTech**

Date: May 06th, 2024

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

## Assessment Overview

From May 5th, 2019 to May 6th, 2024, Parkitkan engaged Praktikan to evaluate the security posture of its infrastructure compared to module best practices that included an external penetration test. All testing performed is based on the Module 4-6 customized testing frameworks.

Phases of penetration testing activities include the following:

- 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.

## Contact Information

Name	Title	Contact Information
Technology Information - ITS		
Dwiyasa Nakula	Praktikan EH	5027221001

## 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	Detail
External Penetration Test	10.15.42.36 10.15.42.7

## Scope Exclusions

Per client request, Praktikan did not perform any Denial of Service attacks or any illegal activities during testing.

## Client Allowances

DC did not provide any allowances to assist the testing

## Executive Summary

Praktikan evaluated DC's external security posture through an external network penetration test from May 5th, 2024 to May 7th, 2024. By leveraging a series of recon method, Praktikan found low to Medium level vulnerabilities that access to the target IP. It is highly recommended that DC 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 TCMS gained internal network access, step by step:

Step	Action	Recommendation
1	Berhasil Mendapatkan backup.sql dimana itu adalah hasil export sql database yang ada user admin dan passwordnya melalui ftp 10.15.42.36 dan dari hasil nmap didapatkan bahwa user anonymous di bolehkan lewat tanpa password	<p>Disable FTP Anonymous.</p> <p>Disable standard FTP, use FTPS or SFTP instead. Update your SSH software to use strong ciphers and the latest version of TLS (no SSL). Disable anonymous FTP if possible.</p>
2	WordPress Username Enumeration	<p>To prevent attackers to enumerate WordPress usernames using this method, we need to install and activate "Unified Login Error Messages" WordPress plugin. When "Unified Login Error Messages" WordPress plug-in is activated, the login error message is changed to "ERROR: Invalid username/password combination." Regardless if the username submitted is correct or not, the authentication error message remains the same. This fixes the problem of username enumeration from the login page authentication error message inconsistency.</p>
3	Vulnerable to Terrapin	<p>To mitigate CVE-2023-48795, disable the vulnerable ChaCha20-Poly1305 cipher in the OpenSSH client and server configurations.</p> <p>Specifically, add the following to /etc/ssh/ssh(d)_config:</p> <p>Ciphers -chacha20-poly1305@openssh.com</p>

		<p>Note the `` at the start of the chacha20 cipher string.</p> <p>Then, restart your SSH server for it to take effect.</p> <p>In addition, ensure you're not explicitly enabling any aes(128 192 256)-cbc ciphers in your OpenSSH configuration while using the default MACs (these ciphers are disabled by default).</p>
4	Robots.txt	<p>Be Careful When Using Both Noindex and Robots.txt Disallow at the Same Time</p> <p>Use Noindex, Not Disallow, for Pages That Need to Be Private yet Publicly Accessible</p> <p>Disallow Directories, Not Specific Pages</p> <p>Set up a Honeypot for IP Blacklisting</p>

## Security Strengths

### Database Password are hash

During the assessment, We are able to view the ftp access of 10.15.42.36 where there is a backup.sql fill with the user database table backup with the admin login, the username is stored in string while the password is saved encrypted with hash.

```

7:100000 ALTER TABLE `users` DISABLE KEYS ;
INSERT INTO `users` VALUES (1,'admin','$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K');
8:140000 ALTER TABLE `users` ENABLE KEYS ;

```

### Latest version services

Using Apache 2.4.59 where many of the major vulnerabilities are patch.

## Security Weaknesses

### Anonymous FTP is enabled

During the recon nmap, Praktikan dapatkan bahwa ftp 10.15.42.36 memperbolehkan user anonymous dapat masuk tanpa password.

# External Penetration Test Findings

Anonymous FTP is enabled – 10.15.42.36 (Medium)

Description:	During the recon nmap, Praktikan dapatkan bahwa ftp 10.15.42.36 memperbolehkan user anonymous dapat masuk tanpa password. Hal ini memberikan akses ke siapapun untuk mengakses ftp protocol IP.  Anonymous FTP is enabled.
Impact:	Moderate
System:	10.15.42.36
References:	<a href="#">CVE-1999-0497</a> - Anonymous FTP is enabled.

## Exploitation Proof of Concept

Melalui recon nmap Praktikan dapatkan bahwa **ftp 10.15.42.36** memperbolehkan user anonymous dapat masuk tanpa password. Menggunakan **nmap -sV -sC -oN nmaplog.log 10.15.42.36**

```
Not shown: 997 filtered tcp ports (no-resp)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: PASV IP 172.18.0.3 is not the same as 10.15.42.36
```

Figure 1: hasil laporan nmap pada 10.15.42.7

Praktikan leveraged the valid celah ini untuk log melalui gain access ke directory tersebut. Dan mendapatkan backup.sql user

```
(ilak@kali)~$ nmap -sV -sC -oN nmaplog.log 10.15.42.36
$ ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:ilak): 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 (|||65510|)
150 Here comes the directory listing.
-rwxrwxr-x 1 ftp ftp 1997 May 04 15:40 backup.sql
226 Directory send OK.
ftp>
```

Figure 2: Successful login ftp pada 10.15.42.7

Dari Backup.sql itu kita dapat tahu bahwa ada user admin dengan passwordnya di hash. Seseorang dapat berusah crack password tersebut menggunakan john the ripper atau hashcat namun itu akan menghabiskan waktu yang lama.

#### WordPress Username Enumeration – 10.15.42.7 (Low)

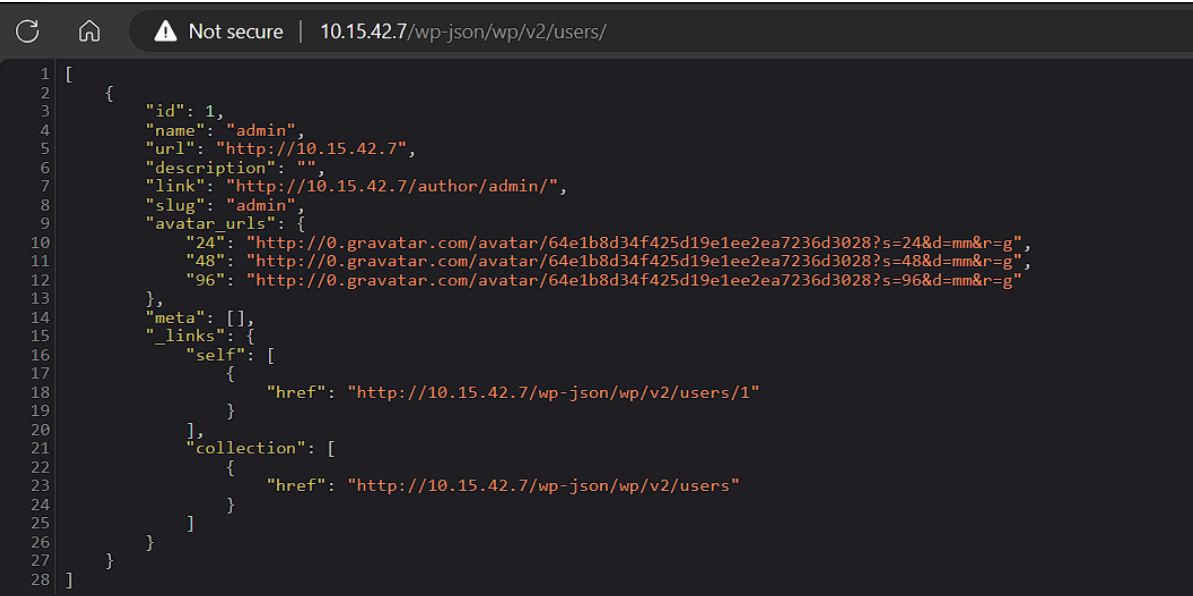
Description:	wp-includes/rest-api/endpoints/class-wp-rest-users-controller.php in the REST API implementation in WordPress 4.7 before 4.7.1 does not properly restrict listings of post authors, which allows remote attackers to obtain sensitive information via a wp-json/wp/v2/users request.
Impact:	Low
System:	10.15.42.7
References:	<a href="#">CVE-2017-5487</a> - WordPress Username Enumeration

#### Exploitation Proof of Concept

```
[wp-user-enum:username] [http] [low] http://10.15.42.7/wp-json/wp/v2/users/ ["admin"]
```

Figure 3: potongan hasil laporan nuclei pada 10.15.42.7

Pada hasil nuclei terdapat laporan low bahwa wp-user-enum:username.



```

1  [
2  {
3    "id": 1,
4    "name": "admin",
5    "url": "http://10.15.42.7",
6    "description": "",
7    "link": "http://10.15.42.7/author/admin/",
8    "slug": "admin",
9    "avatar_urls": {
10     "24": "http://0.gravatar.com/avatar/64e1b8d34f425d19e1ee2ea7236d3028?s=24&d=mm&r=g",
11     "48": "http://0.gravatar.com/avatar/64e1b8d34f425d19e1ee2ea7236d3028?s=48&d=mm&r=g",
12     "96": "http://0.gravatar.com/avatar/64e1b8d34f425d19e1ee2ea7236d3028?s=96&d=mm&r=g"
13   },
14   "meta": [],
15   "_links": {
16     "self": [
17       {
18         "href": "http://10.15.42.7/wp-json/wp/v2/users/1"
19       }
20     ],
21     "collection": [
22       {
23         "href": "http://10.15.42.7/wp-json/wp/v2/users"
24       }
25     ]
26   }
27 }
28 ]

```

Figure 4: Hasil penelusuran web page yang diberikan

## Vulnerable to Terrapin – 10.15.42.36 (Medium)

Description:	<p>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. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGO before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.</p>
Impact:	Medium
System:	10.15.42.36
References:	<a href="#">CVE-2023-48795</a> - Vulnerable to Terrapin

## Exploitation Proof of Concept

```
[CVE-2023-48795] [javascript] [medium] 10.15.42.36:22 ["Vulnerable to Terrapin"]
```

Figure 5: potongan hasil laporan nuclei pada 10.15.42.36



## Vulnerable to Terrapin – 10.15.42.7 (Medium)

Description:	<p>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. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGO before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.</p>
Impact:	Medium
System:	10.15.42.7
References:	<a href="#">CVE-2023-48795</a> - Vulnerable to Terrapin

## Exploitation Proof of Concept

[CVE-2023-48795] [javascript] [medium] 10.15.42.7:22 ["Vulnerable to Terrapin"]

Figure 6: potongan hasil laporan nuclei pada 10.15.42.7

Eobots.txtn – 10.15.42.7 (Low)

Description:	Virtual Robots.txt before 1.10 does not block HTML tags in the robots.txt field.
Impact:	Low
System:	10.15.42.7
References:	<a href="#">CVE-2021-28121</a> - robots.txt

### Exploitation Proof of Concept

```
[+] robots.txt found: http://10.15.42.7/robots.txt
| Interesting Entries:
| - /wp-admin/
| - /wp-admin/admin-ajax.php
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%
```

Figure 3: potongan hasil laporan wpscan pada 10.15.42.7

Pada hasil wpscan penembuan robots.txt yang menunjukkan Html webpage yang tersembunyi