FortifyTech
Security Assessment Findings Report

Business Confidential

Date: May 28th, 2019
Project: 897-19
Version 1.0

Table of Contents

Table of Contents 2
Confidentiality Statement 3
Disclaimer 3
Contact Information 3
Assessment Overview 4
Assessment Components 4
External Penetration Test 4
Finding Severity Ratings 5
Scope 6
Scope Exclusions 6
Client Allowances 6
Executive Summary 7
Attack Summary 7
Security Strengths 10
Tidak Ada Raw Password 10
Tidak Ditemukan Data Bocor Pada IP http://10.15.42.36:8888 10
Security Weaknesses 10
Anonymous FTP 10
Mendapatkan Informasi Admin 12
Vulnerabilities by Impact 13
External Penetration Test Findings 14

Confidentiality Statement

This document is the exclusive property of Demo Company (DC) and TCM Security (TCMS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both DC and TCMS.

TCMS 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

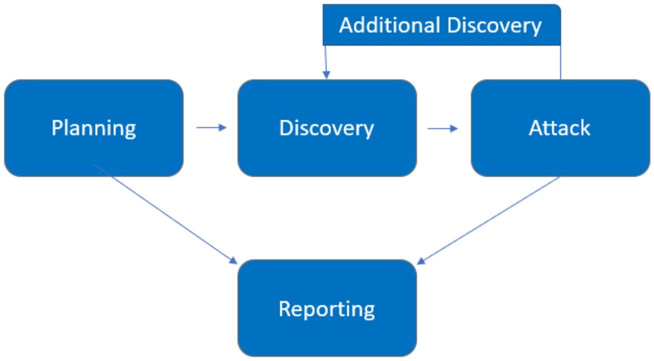
Name	Title	Contact Information
Demo Company		
EH	Praktikum 2	WhatsApp: 08x-xxx-xxx-xxx Email: michaelxxxxxxxxxxxxx@gmail.com

Assessment Overview

Pada kesempatan kali ini, praktikan diminta untuk melakukan Penetration Testing pada website yang telah disedikan oleh asisten laboratorium mata kuliah Ethical Hacking.

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, 10.15.42.7

- Full scope information provided in “**Demo Company-867-19 Full Findings.xslx”**

Scope Exclusions

Per client request, TCMS did not perform any Denial of Service attacks during testing.

Client Allowances

DC did not provide any allowances to assist the testing.

Executive Summary

Anda adalah seorang ahli keamanan yang ditugaskan oleh perusahaan konsultan keamanan CyberShield untuk melakukan penetration testing terhadap infrastruktur perusahaan FortifyTech. FortifyTech adalah startup perusahaan teknologi dan mereka telah menyewa layanan CyberShield untuk mengevaluasi keamanan sistem mereka.

Temukan kerentanan pada perusahaan FortifyTech dengan menerapkan prinsip Ethical Hacking dan buatlah laporan pada setiap kerentanan yang telah anda temukan, dengan begitu celah kerentanan tersebut dengan cepat bisa diproses oleh mereka.

Attack Summary

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

Step	Action	Recommendation
1	**nmap -sV -sC -oN nmaplog.log 10.15.42.36** *Nmap merupakan tools powerful* yang dapat digunakan untuk port dan *service scanning*. *Output* hasil *scanning* cukup lengkap, dilengkapi dengan NSE *script* yang mempermudah untuk validasi *vulnerability* Ditemukan informasi bahwa pihak luar dapat melakukan login ftp menggunakan username anonymous	-
2	Menjalankan **nmap -sV -O 10.15.42.36** untuk mendapatkan informasi mengenai port 8888 yang terbuka	-

3	Login melalui **ftp 10.15.42.36** dengan username anonymous dan tidak ada password	Ditemukan data backup.sql yang mengarah ke server 10.15.42.32 dan dapat diakses secara public. Dengan login anonim FTP, penyediaan akses publik ke file dimungkinkan tanpa memerlukan nama pengguna atau kata sandi yang unik. Keterbukaan ini menghilangkan hambatan masuk yang mungkin ada, dan memungkinkan pengguna untuk mengakses informasi secara bebas.
4	Menggunakan *tools Nuclei* untuk mendapatkan vulnerability pada IP 10.15.42.36:888 **nuclei -u http://10.15.42.36:8888 -o ip1.txt**	-

5	Menggunakan *tools Nuclei* untuk mendapatkan vulnerability pada IP 10.15.42.7 **nuclei -u http://10.15.42.7 -o ip2.txt**	Terdapat beberapa directory yang terbuka pada IP http://10.15.42.7, salah satunya adalah http://10.15.42.7/wp-json/wp/v2/users/. Sebaiknya menggunakan authorization dan authentication

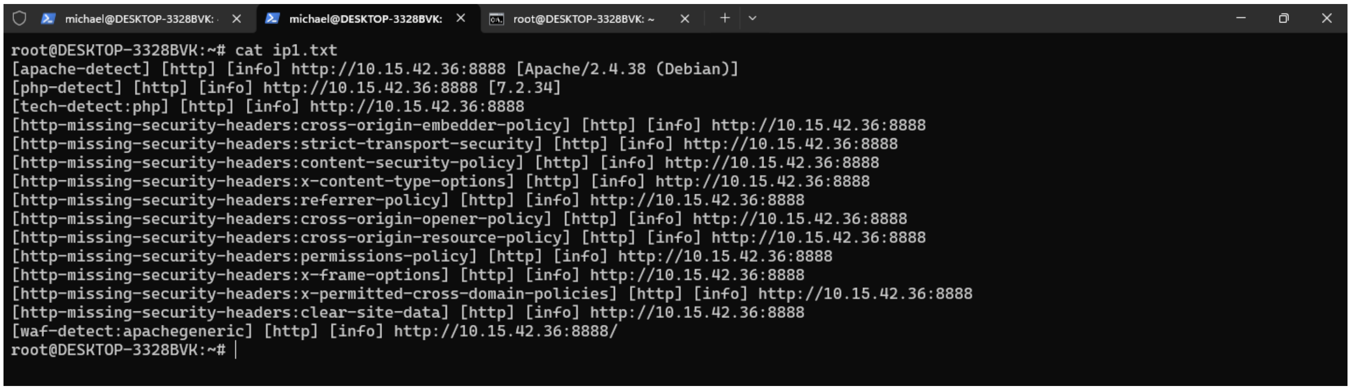
Security Strengths

Tidak Ada Raw Password

Tidak ditemukan *raw* password pada http://10.15.42.7 dan http://10.15.42.36.

Tidak Ditemukan Data Bocor Pada IP http://10.15.42.36:8888

Saat melakukan scanning menggunakan Nuclei, tidak ditemukan directory yang bocor pada IP di atas



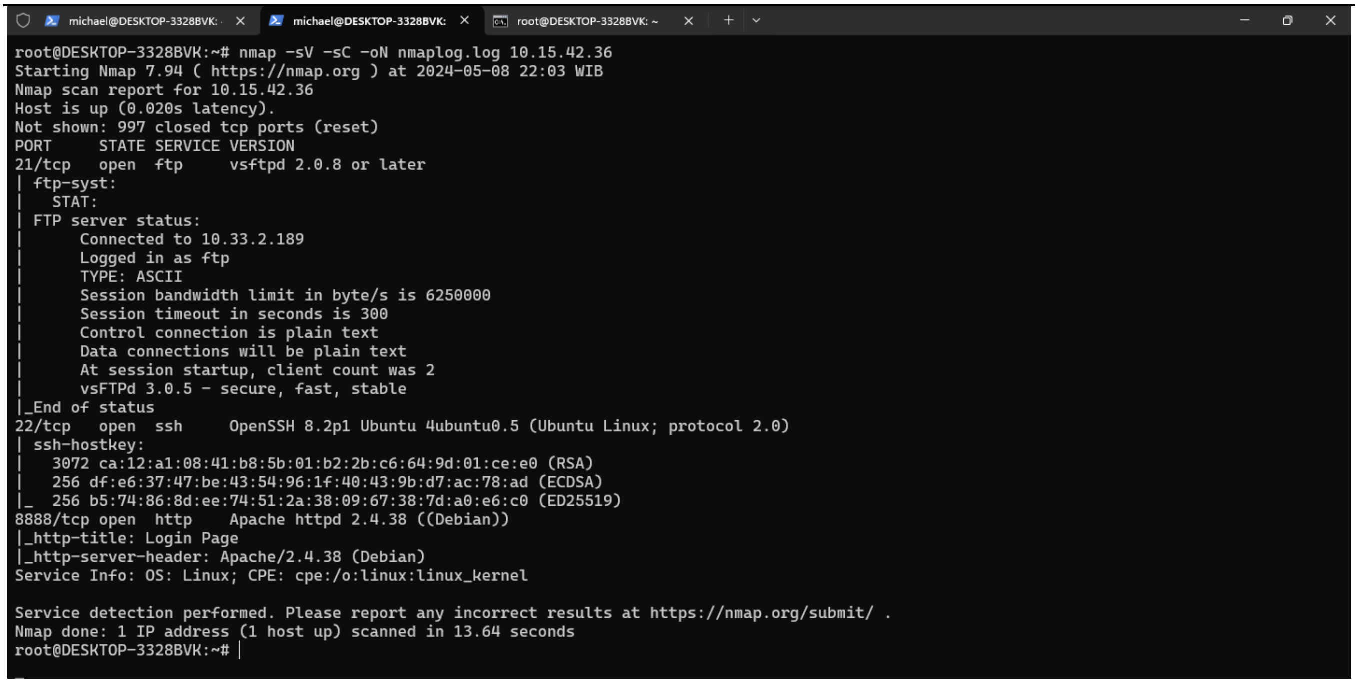
```
root@DESKTOP-3328BVK:~# cat ip1.txt
[apache-detect] [http] [info] http://10.15.42.36:8888 [Apache/2.4.38 (Debian)]
[php-detect] [http] [info] http://10.15.42.36:8888 [7.2.34]
[tech-detect:php] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:content-security-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:referrer-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:permissions-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:x-frame-options] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:clear-site-data] [http] [info] http://10.15.42.36:8888
[waf-detect:apachegeneric] [http] [info] http://10.15.42.36:8888/
root@DESKTOP-3328BVK:~# |
```

Gambar 1. Scan Nuclei pada IP http://10.15.42.36

Security Weaknesses

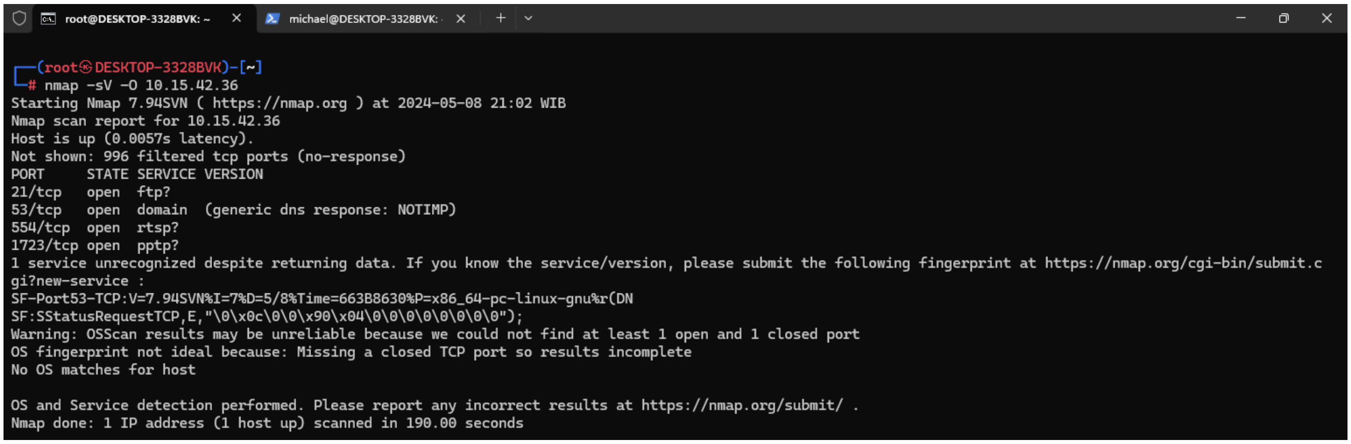
Anonymous FTP

Didapat sebuah output bahwa IP http://10.15.42.36 dapat diakses oleh publik melalui metode ftp dengan username anonymous dan tanpa password.



```
root@DESKTOP-3328BVK:~# nmap -sV -sC -oN nmaplog.log 10.15.42.36
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-08 22:03 WIB
Nmap scan report for 10.15.42.36
Host is up (0.020s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.33.2.189
|      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)
| 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-title: Login Page
|_http-server-header: Apache/2.4.38 (Debian)
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 13.64 seconds
root@DESKTOP-3328BVK:~# 
```

Gambar 2. Hasil Scan Menggunakan Nmap

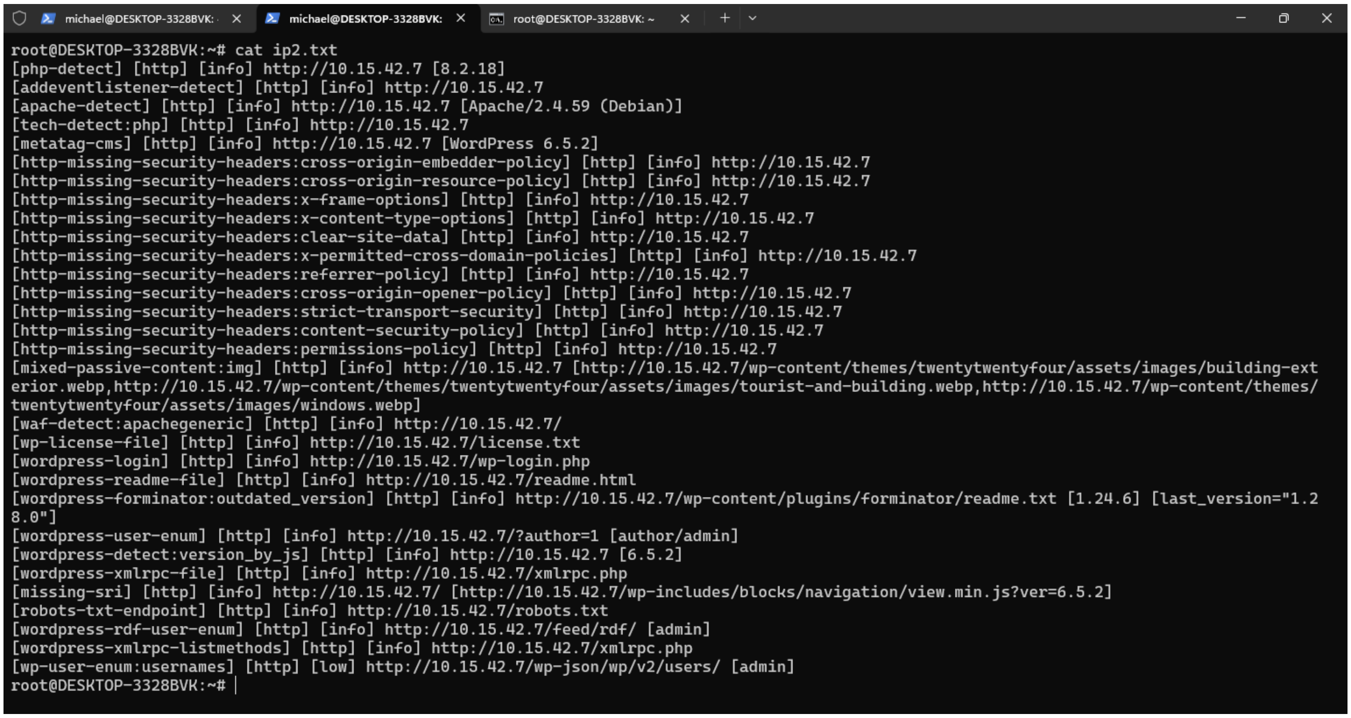


```
┌──(root㉿DESKTOP-3328BVK)-[~]
└─# nmap -sV -O 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 21:02 WIB
Nmap scan report for 10.15.42.36
Host is up (0.0057s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp?
53/tcp   open  domain  (generic dns response: NOTIMP)
554/tcp  open  rtsp?
1723/tcp open  pptp?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.c
gi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7%D=5/8%Time=663B8630%P=x86_64-pc-linux-gnu%r(DN
SF:SStatusRequestTCP,E,"\0\x0c\0\0\x90\x04\0\0\0\0\0\0\0\0");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

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 190.00 seconds
```

Gambar 3. Hasil Scan Menggunakan Nmap untuk Melihat Port yang Dibuka

Mendapatkan Informasi Admin

Saat melakukan *scanning* CVE menggunakan Nuclei, didapat bahwa IP dan directory http://10.15.42.7/wp-json/wp/v2/users/ mengarah ke data JSON atau *back-end* yang mana seharusnya tidak boleh diakses oleh publik

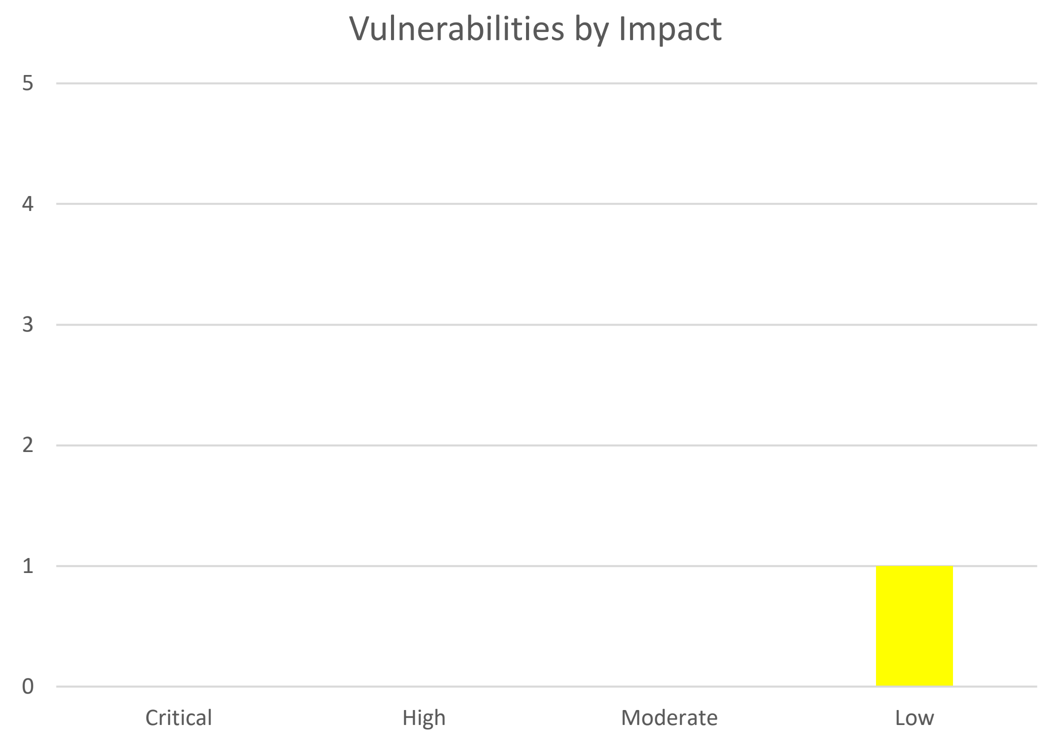


```
root@DESKTOP-3328BVK:~# cat ip2.txt
[php-detect] [http] [info] http://10.15.42.7 [8.2.18]
[addeventlistener-detect] [http] [info] http://10.15.42.7
[apache-detect] [http] [info] http://10.15.42.7 [Apache/2.4.59 (Debian)]
[tech-detect:php] [http] [info] http://10.15.42.7
[metatag-cms] [http] [info] http://10.15.42.7 [WordPress 6.5.2]
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-frame-options] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.15.42.7
[http-missing-security-headers:clear-site-data] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.15.42.7
[http-missing-security-headers:referrer-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.15.42.7
[http-missing-security-headers:content-security-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:permissions-policy] [http] [info] http://10.15.42.7
[mixed-passive-content:img] [http] [info] http://10.15.42.7 [http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/building-ext
erior.webp,http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/tourist-and-building.webp,http://10.15.42.7/wp-content/themes/
twentytwentyfour/assets/images/windows.webp]
[waf-detect:apachegeneric] [http] [info] http://10.15.42.7/
[wp-license-file] [http] [info] http://10.15.42.7/license.txt
[wordpress-login] [http] [info] http://10.15.42.7/wp-login.php
[wordpress-readme-file] [http] [info] http://10.15.42.7/readme.html
[wordpress-forminator:outdated_version] [http] [info] http://10.15.42.7/wp-content/plugins/forminator/readme.txt [1.24.6] [last_version="1.2
8.0"]
[wordpress-user-enum] [http] [info] http://10.15.42.7/?author=1 [author/admin]
[wordpress-detect:version_by_js] [http] [info] http://10.15.42.7 [6.5.2]
[wordpress-xmlrpc-file] [http] [info] http://10.15.42.7/xmlrpc.php
[missing-sri] [http] [info] http://10.15.42.7/ [http://10.15.42.7/wp-includes/blocks/navigation/view.min.js?ver=6.5.2]
[robots-txt-endpoint] [http] [info] http://10.15.42.7/robots.txt
[wordpress-rdf-user-enum] [http] [info] http://10.15.42.7/feed/rdf/ [admin]
[wordpress-xmlrpc-listmethods] [http] [info] http://10.15.42.7/xmlrpc.php
[wp-user-enum:usernames] [http] [low] http://10.15.42.7/wp-json/wp/v2/users/ [admin]
root@DESKTOP-3328BVK:~#
```

Gambar 4. Scan pada IP http://10.15.42.7

Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:



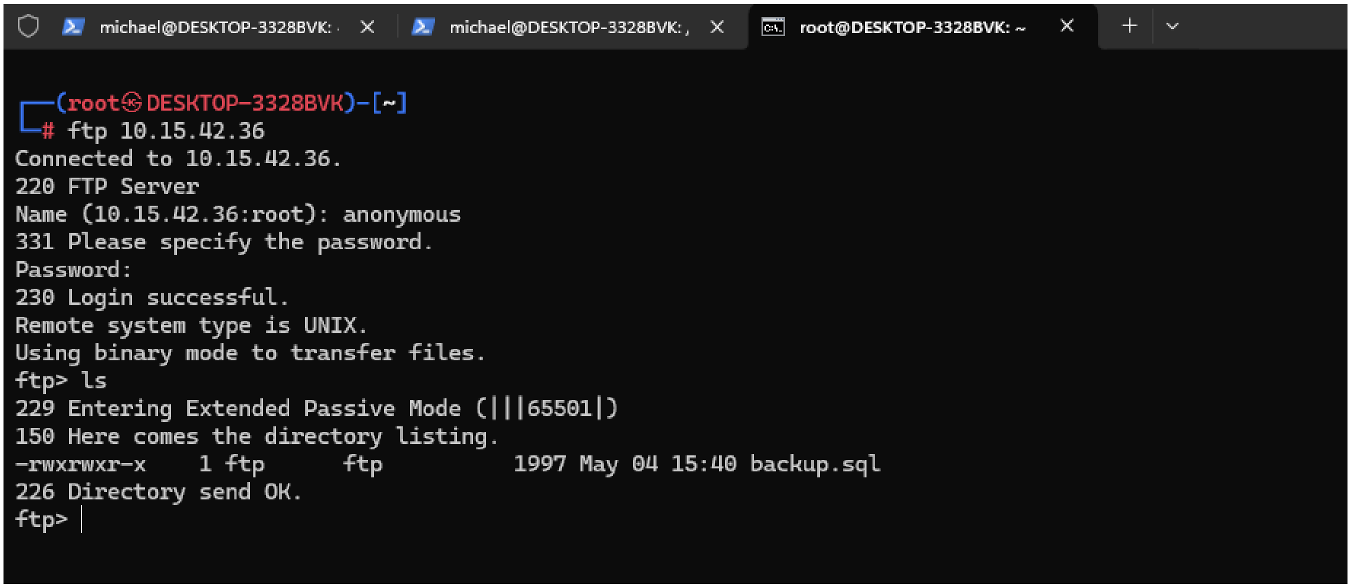
External Penetration Test Findings

Unlimited Login Attempts

Description:	Pihak luar dapat melakukan attempt login berkali-kali tanpa ada batasan tertentu
Impact:	Low
System:	http://10.15.42.7/wp-json/wp/v2/users/
References:	NIST SP800-53r4 AC-7(1)

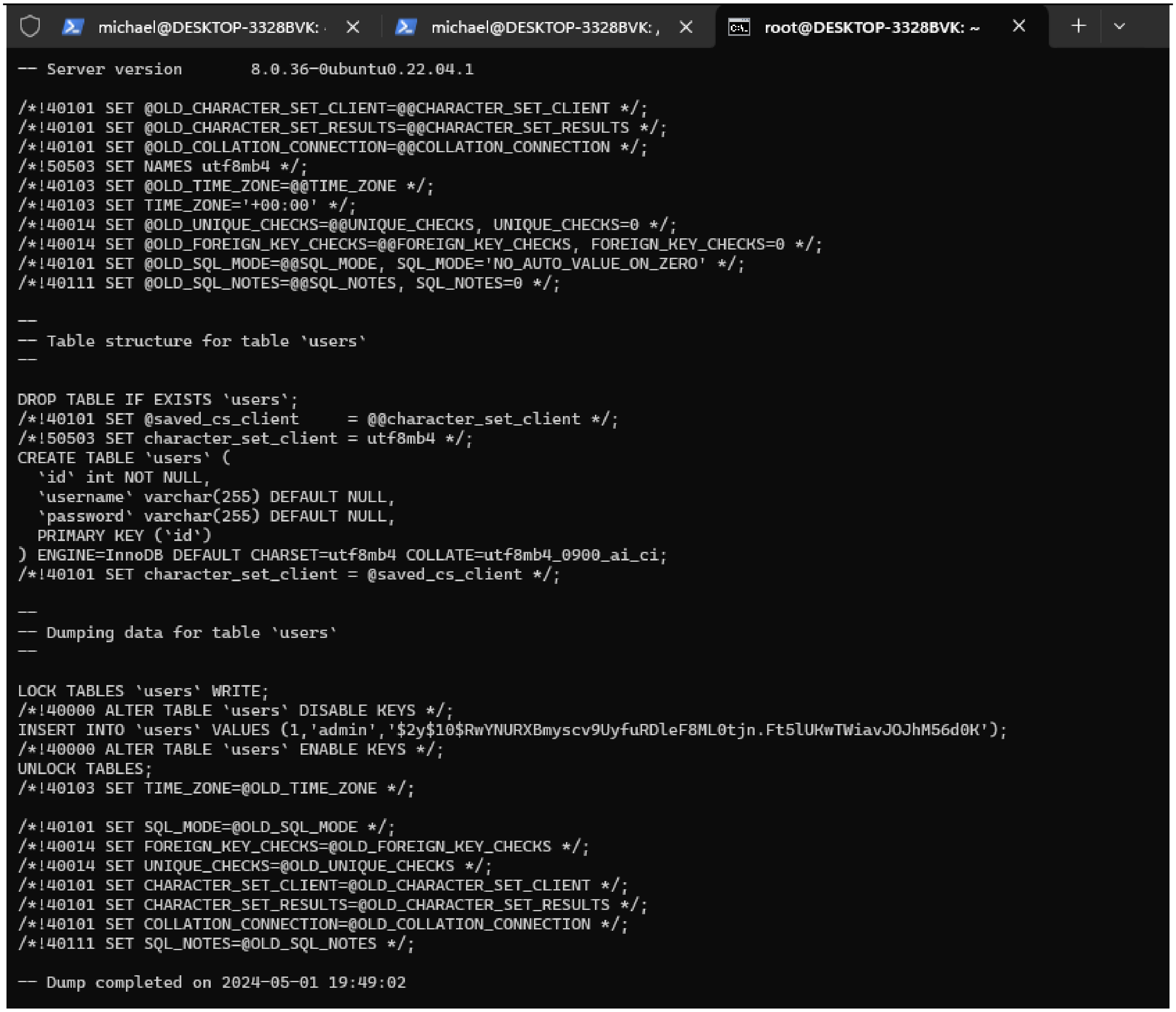
Exploitation Proof of Concept

Berikut adalah lampiran data yang berhasil dipaparkan ketika melakukan proses login



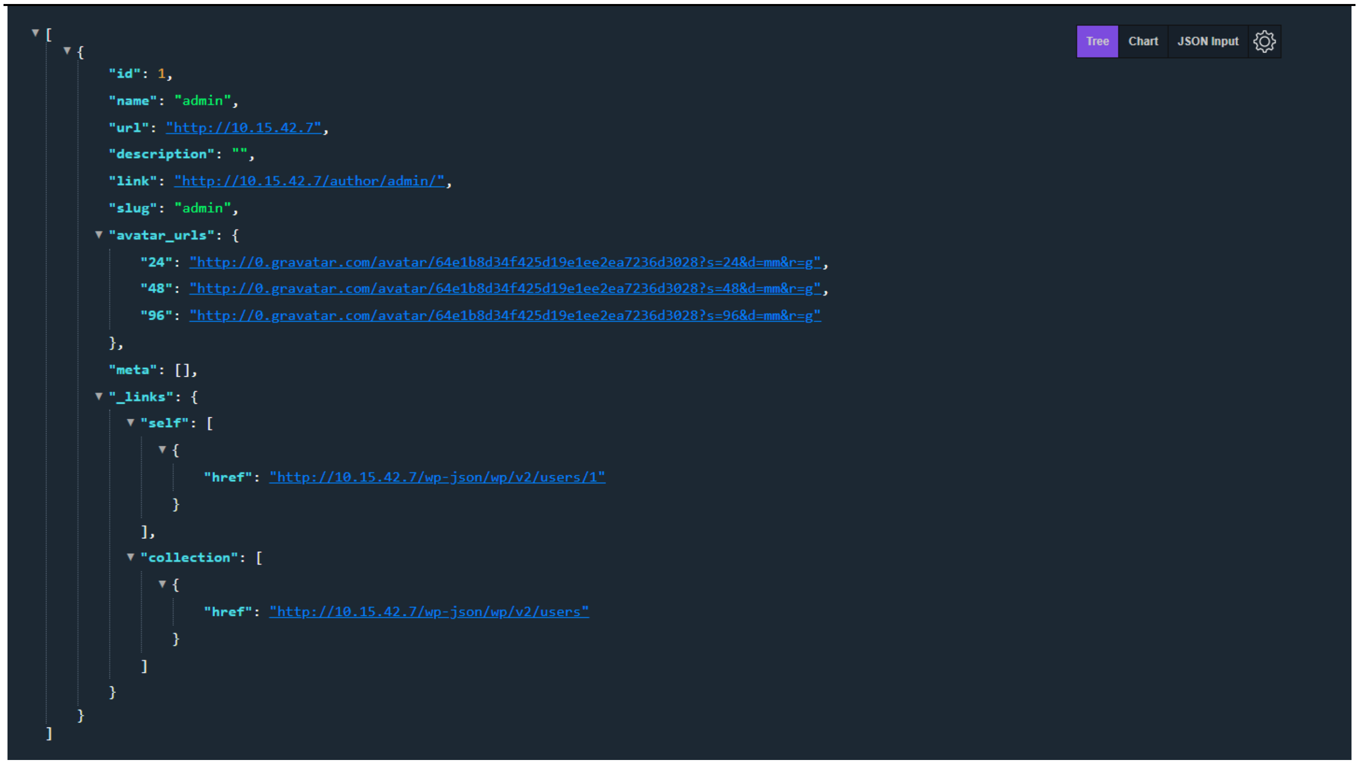
```
┌──(root㉿DESKTOP-3328BVK)-[~]
└─# ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||65501|)
150 Here comes the directory listing.
-rwxrwxr-x    1 ftp      ftp          1997 May 04 15:40 backup.sql
226 Directory send OK.
ftp> 
```

Gambar 5. Praktikan Melakukan Attempt Login Menggunakan ftp



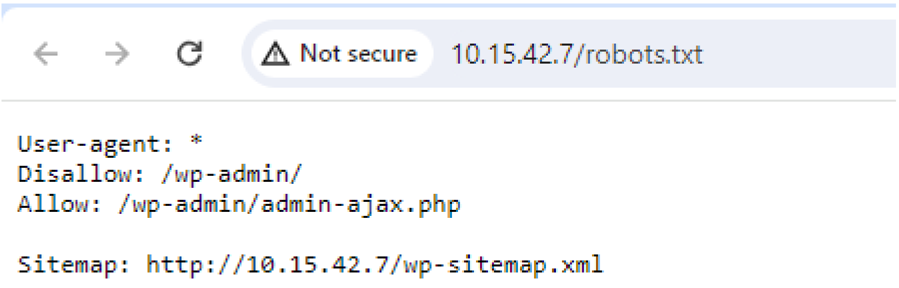
```
-- Server version       8.0.36-0ubuntu0.22.04.1

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!50503 SET NAMES utf8mb4 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `users`
--

DROP TABLE IF EXISTS `users`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!50503 SET character_set_client = utf8mb4 */;
CREATE TABLE `users` (
  `id` int NOT NULL,
  `username` varchar(255) DEFAULT NULL,
  `password` varchar(255) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `users`
--

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 */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

-- Dump completed on 2024-05-01 19:49:02
```

Gambar 6. Praktikan Mendapatkan Raw Data Password pada backup.sql yang Telah DiHash



```
[
    {
        "id": 1,
        "name": "admin",
        "url": "http://10.15.42.7",
        "description": "",
        "link": "http://10.15.42.7/author/admin/",
        "slug": "admin",
        "avatar_urls": {
            "24": "http://0.gravatar.com/avatar/64e1b8d34f425d19e1ee2ea7236d3028?s=24&d=mm&r=g",
            "48": "http://0.gravatar.com/avatar/64e1b8d34f425d19e1ee2ea7236d3028?s=48&d=mm&r=g",
            "96": "http://0.gravatar.com/avatar/64e1b8d34f425d19e1ee2ea7236d3028?s=96&d=mm&r=g"
        },
        "meta": [],
        "_links": {
            "self": [
                {
                    "href": "http://10.15.42.7/wp-json/wp/v2/users/1"
                }
            ],
            "collection": [
                {
                    "href": "http://10.15.42.7/wp-json/wp/v2/users"
                }
            ]
        }
    }
]
```

Gambar 7. Data JSON Admin



```
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php

Sitemap: http://10.15.42.7/wp-sitemap.xml
```

Gambar 8. Directory robots.txt yang Didapat dari Scan Nuclei

Remediation

Who:	IT Team
Vector:	Remote
Action:	Pada IP 10.15.42.36, sebaiknya aksi ftp dapat diperketat dengan menggunakan username dan password yang unik Pada IP http://10.15.42.7/wp-json/wp/v2/users/, sebaiknya data tersebut tidak dapat diakses oleh public. Apabila ingin diakses, back-end developer sebaiknya menambahkan authentication dan authorization.

TCM SECURITY