Fortify Tech
Security Assessment Findings Report

Business Confidential

Date: May 8th, 2024

Copyright © TCM Security (tcm-sec.com)

Confidentiality Statement

This document is the exclusive property of Fortify Tech. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Demo Corp and TCMS.

Demo Corp 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	NRP	Contact Information
Alma Amira Dewani	5027221054	Email: almaaamirad@gmail.com

Copyright © TCM Security (tcm-sec.com)

Assessment Overview

From May 5th, 2024 to March 8th, 2024, Demo Corp engaged TCMS to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network 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.

Copyright © TCM Security (tcm-sec.com)

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.

Copyright © TCM Security (tcm-sec.com)

Scope

Assessment	Details
Internal Penetration Test	10.15.42.36 10.15.42.7

Scope Exclusions

Tidak diperbolehkan melakukan hal yang melanggar etika

Client Allowances

Internal access to network via dropbox and port allowances

Copyright © TCM Security (tcm-sec.com)

Executive Summary

Dilakukan pentesting kepada Fortify Tech dari tanggal 5 May 2024 – 8 May 2024. Berikut akan menampilkan high-level overview of vulnerabilities discovered, successful and unsuccessful attempts.

Testing Summary

Dilakukan recon kepada ip target, disini saya menggunakan gobuster untuk menemukan direktori tersembunyi, nama file, atau entitas lainnya. Selain itu, pentester juga menggunakan nikto, nuclei dan owasp untuk mengetahui vulnerability.

Copyright © TCM Security (tcm-sec.com)

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

0	1	3	5	4
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
Absence of Anti-SCRF Tokens	Moderate	
Content Security Policy (CSP) Header Not Set	High	
Missing Anti-clickjacking Header	Moderate	
Cookie No HttpOnly Flag	Low	
Cookie without SameSite Attribute	Low	
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	
X-Content-Type-Options Header Missing	Low	
Information Disclosure - Suspicious Comments	Informational	
Modern Web Application	Informational	.
Session Management Response Identified	Informational	
User Controllable HTML Element Attribute (Potential XSS)	Informational	
Vulnerable to Terrapin	Moderate	

Copyright © TCM Security (tcm-sec.com)

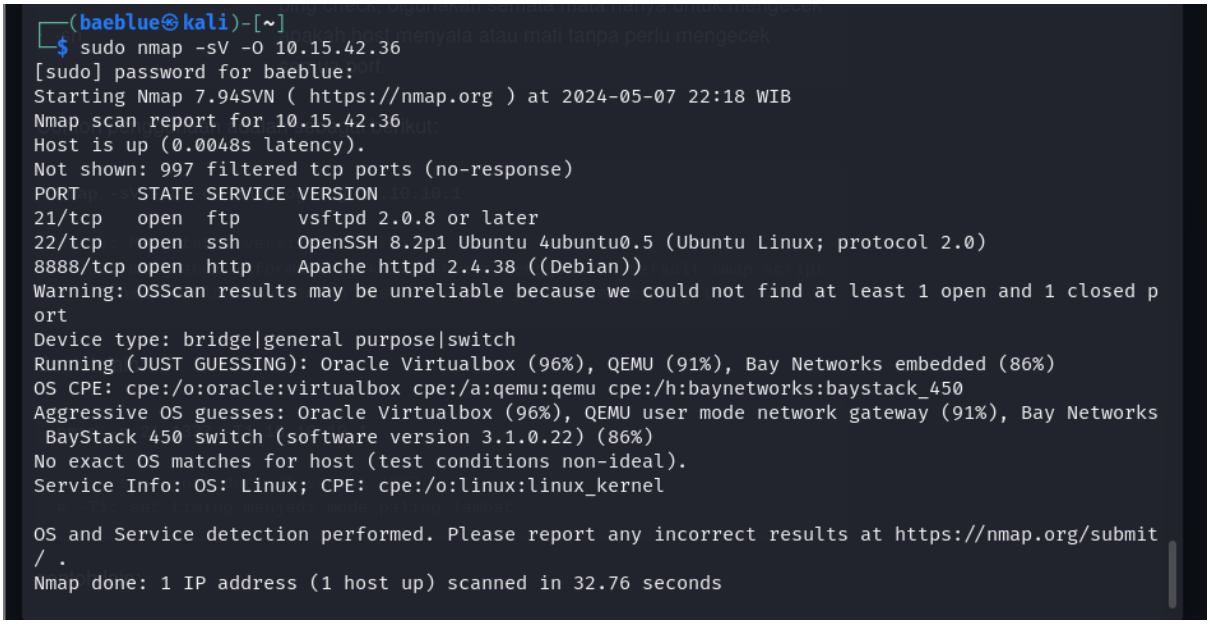
Technical Findings

Internal Penetration Test Findings

Finding Open Port

Description:	Saat menjalankan nmap ditemukan open port yang mengarah we login page. Selain itu juga ditemukan file backup.sql yang Ketika dibuka ditemukan user dan password. Namun passwordnya masih berbentuk kode hash
Risk:	Low
System:	10.15.42.36
Tools Used:	Nmap ftp
References:	

Evidence;



Copyright © TCM Security (tcm-sec.com)

```
  `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.Ft5lUKwTWiavJOJhM56d0
K');
/*!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
```

CVE -2023-48795

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.
Risk:	Moderate
System:	- 10.15.42.7
Tools Used:	
References:	https://nvd.nist.gov/vuln/detail/CVE-2023-48795

Copyright © TCM Security (tcm-sec.com)

Finding CVE

Description:	Ditemukan file CVE-2023-48795 saat sedang melakukan scanning
Risk:	Moderate
System:	- 10.15.42.7
Tools Used:	Nuclei
References:	

Evidence:

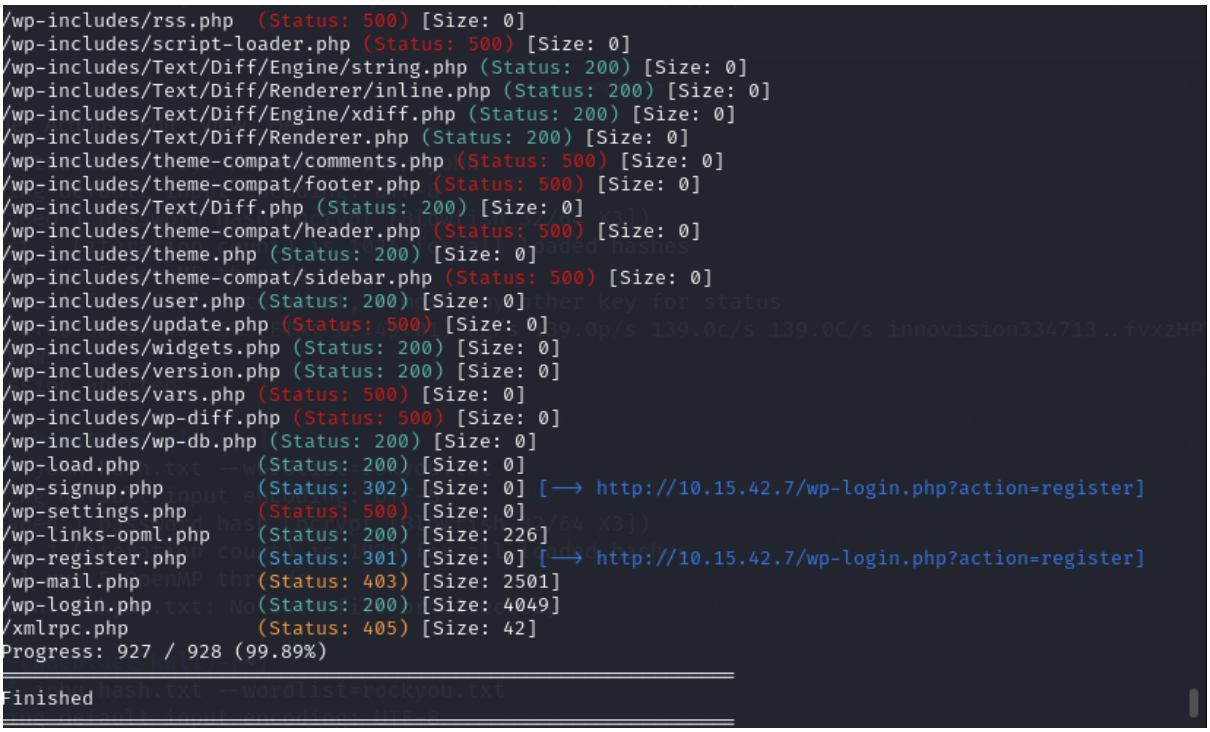
Copyright © TCM Security (tcm-sec.com)

Finding Login Page

Description:	Saat melakukan scanning juga ditemukan port yang mengarah ke login page di wordpress
Risk:	Low
System:	- 10.15.42.7
Tools Used:	Gobuster
References:	

Evidence:

Copyright © TCM Security (tcm-sec.com)



Server Leaks Information via "Server" HTTP Response Header Field(s)

Description:	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Risk:	Low
System:	- 10.15.42.7
Tools Used:	OWASP
References:	https://cwe.mitre.org/data/definitions/200.html

Copyright © TCM Security (tcm-sec.com)