FORTIFYTECH
Security Assessment Findings Report

Business Confidential

Date: May 8th, 2024
Project: Praktikum 2
Version 1.0

Confidentiality Statement

This document is the exclusive property of FortifyTech and TCM Security (CYBERSHIELD). 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 CYBERSHIELD.

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

Contact Information

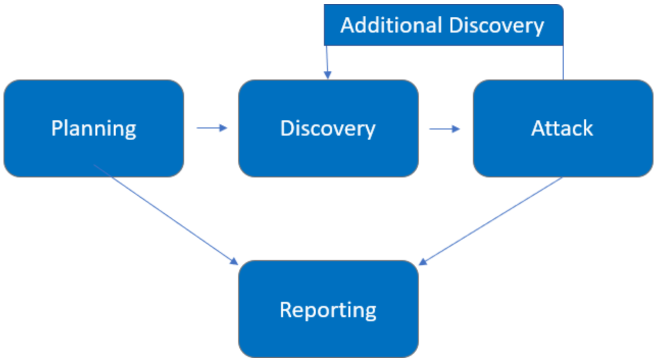
Name	Title	Contact Information
FortifyTech		
John Smith	Global Information Security Manager	Email: jsmith@democorp.com
CyberShield Security		
Monika Damelia Hutapea	Lead Penetration Tester	Email: 5027221011@student.its.ac.id.com

Assessment Overview

From May 5nd, 2024 to May 8th, 2024, FortifyTech engaged CYBERSHIELD 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	• 10.15.42.36 • 10.15.42.7

Scope Exclusions

Per client request, CYBERSHIELD did not perform any of the following attacks during testing:

- Anything that violates ethical hacking

All other attacks not specified above were permitted by FortifyTech.

Client Allowances

FortifyTech provided CYBERSHIELD the following allowances:

- Internal access to network via VPN ITS or ITS Network

Executive Summary

CYBERSHIELD evaluated FortifyTech's internal security posture through penetration testing from May 5th, 2024 to March 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

The penetration testing of FortifyTech's infrastructure, undertaken by CyberShield security consultants, revealed several significant findings. Employing Nmap and FTP, the assessment identified vulnerabilities and potential risks within the system. Notably, examination uncovered an open FTP port with anonymous login capabilities on IP address 10.15.42.36. Despite successful access, a discrepancy in the PASV IP configuration was detected, indicating a potential security lapse. Furthermore, SSH and HTTP services were found open, suggesting various avenues for exploitation. Therefore, the focus of attention lies primarily on addressing vulnerabilities present in other parts of the infrastructure.

Tester Notes and Recommendations

To address the vulnerabilities identified during the penetration testing, CyberShield security consultants recommend prompt action in several key areas. Firstly, it is imperative to address the PASV IP mismatch detected in the FTP configuration, ensuring data connections are established securely. Secondly, a thorough review of the FTP server configuration is advised to enhance security measures, particularly concerning anonymous login permissions. Additionally, measures should be implemented to secure the HTTP login page found on port 8888/tcp to prevent unauthorized access. Lastly, regular security audits are essential to continuously evaluate and strengthen FortifyTech's infrastructure against evolving cyber threats.

Key Strengths and Weaknesses

For IP Address 10.15.42.36

The following identifies the key strengths identified during the assessment:

Strengths:

1. The scan was able to identify the open ports and services running on the target system, providing valuable information for further analysis and exploitation attempts.
2. The version information of the SSH and HTTP services was determined, allowing for research on potential vulnerabilities associated with those specific versions.

3. The operating system was guessed to be Linux, potentially running on a virtualization platform like Oracle VirtualBox or QEMU, providing insights into the target environment.

Weaknesses:

1. The FTP server (vsftpd 2.0.8 or later) is running and allows anonymous login, which is a critical security vulnerability that exposes sensitive data and potentially grants unauthorized access.
2. The PASV IP mismatch detected in the FTP configuration indicates a potential issue with the data connections, which could lead to data leakage or man-in-the-middle attacks.
3. The HTTP service running on port 8888 has a login page accessible, and if not properly secured, it could serve as an entry point for unauthorized access.
4. The scan results indicate that the test conditions were non-ideal, potentially affecting the accuracy of the operating system and service detection.

For IP Address 10.15.42.36

The following identifies the key strengths identified during the assessment:

Strengths:

1. The scan identified an open HTTP service running on port 80, indicating the presence of a web server.
2. The web server was identified as Apache httpd 2.4.59 running on Debian, providing valuable information for further analysis and potential exploitation.
3. The scan detected that the web server is running WordPress 6.5.2, which allows for researching known vulnerabilities associated with that specific version.

Weaknesses:

1. The scan revealed that the /wp-admin/ directory is disallowed in the robots.txt file, suggesting that the WordPress administration area may be accessible and could be a potential entry point for unauthorized access.
2. The test conditions were reported as non-ideal, which may affect the accuracy of the operating system and service detection.
3. No specific vulnerabilities were identified during the scan, but further testing and enumeration may be required to uncover potential weaknesses in the web server or WordPress installation.

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
IPT-001: Anonymous login via FTP on IP Address 10.15.42.36	High	Disable the anonymous login option on FTP services
IPT-002: Vulnerability in IP Address 10.15.42.7 running WordPress 6.5.2	Moderate	Update Wordpress to the latest version and implement effective security plugins to protect against xss attacks.

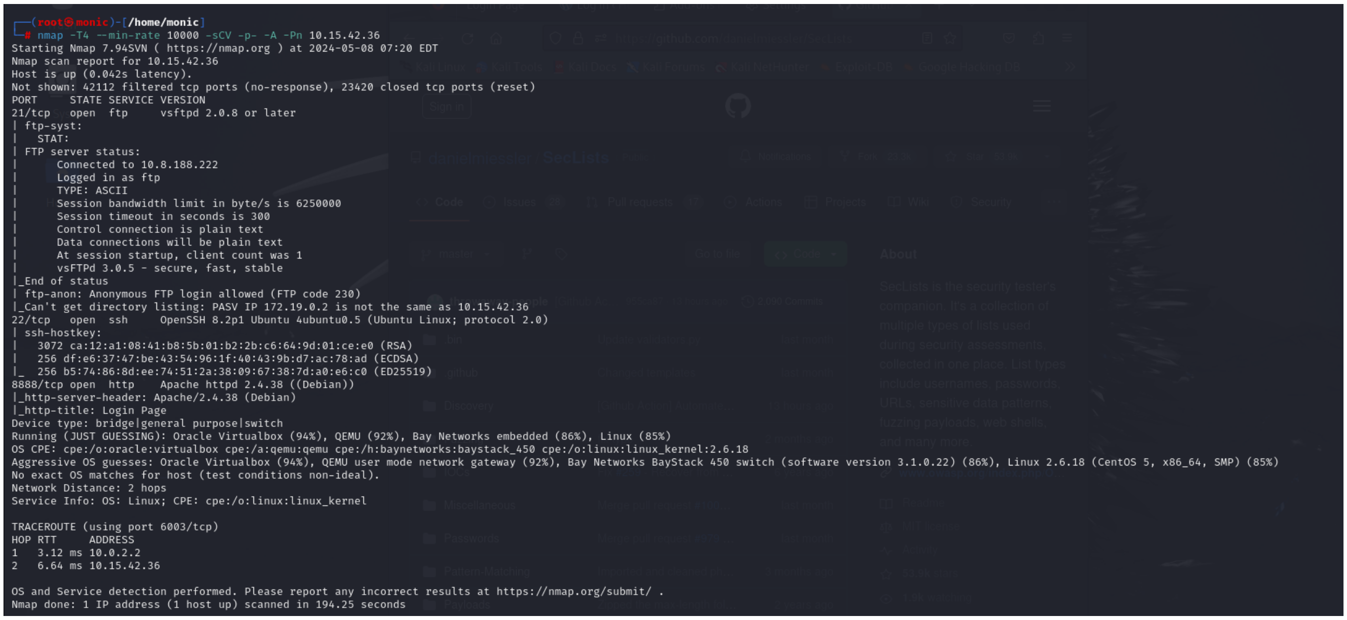
Technical Findings

Internal Penetration Test Findings

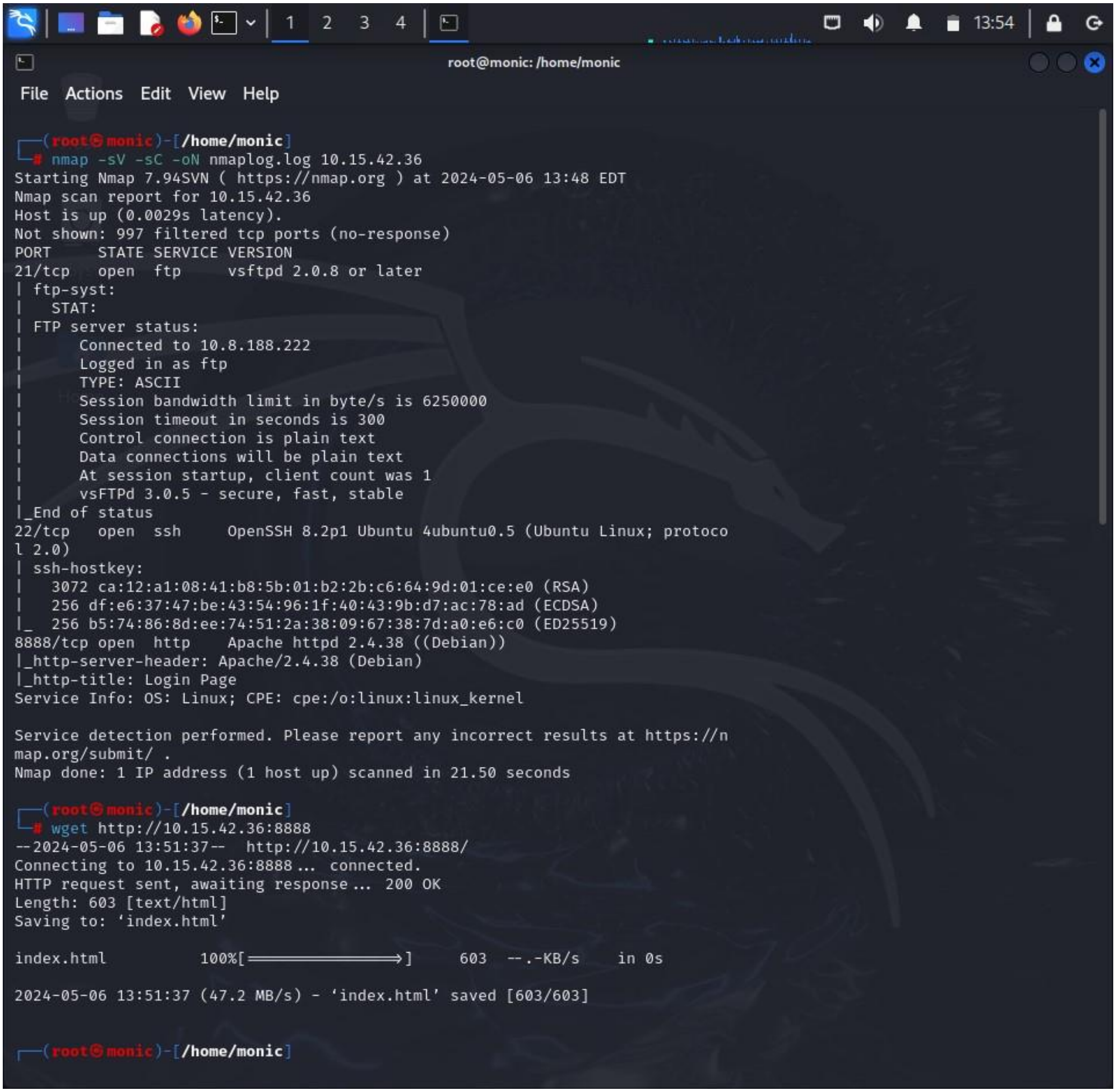
Finding IPT-001: Anonymous login via FTP on IP Address 10.15.42.36 (High)

Description:	The Nmap scan revealed that the FTP server (vsftpd 2.0.8 or later) running on port 21 of the host with IP 10.15.42.36 allows anonymous login. This configuration bypasses authentication mechanisms and grants unrestricted access to the FTP server, potentially exposing sensitive data and system files.
Risk:	Likelihood: Moderate – Allowing anonymous FTP access is a significant security risk, as it is a common attack vector that is easily exploitable by malicious actors but need higher skills to exploit attacks. Impact: High – Anonymous FTP access permits unauthorized access to the system, enabling attackers to explore and potentially compromise sensitive data, exfiltrate files, distribute malware, and gain a foothold for pivoting and lateral movement within the network..
System:	All
Tools Used:	Nmap on Kali Linux

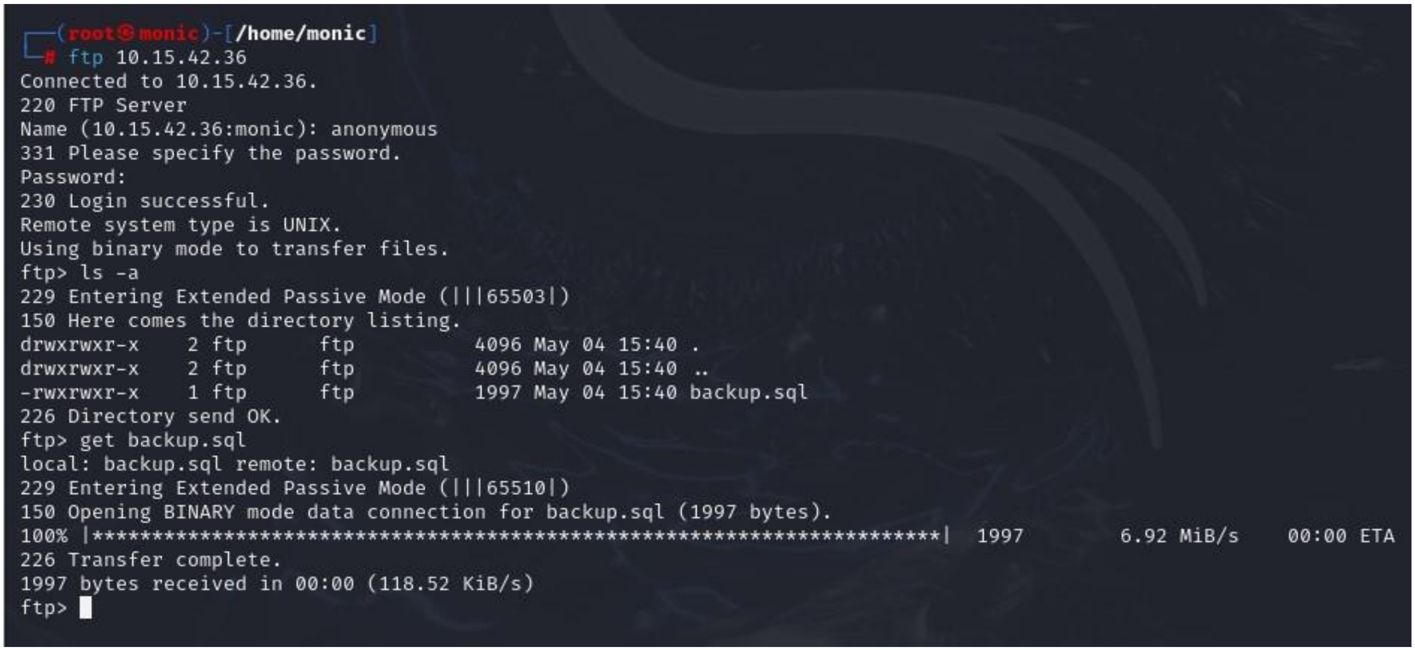
Evidence



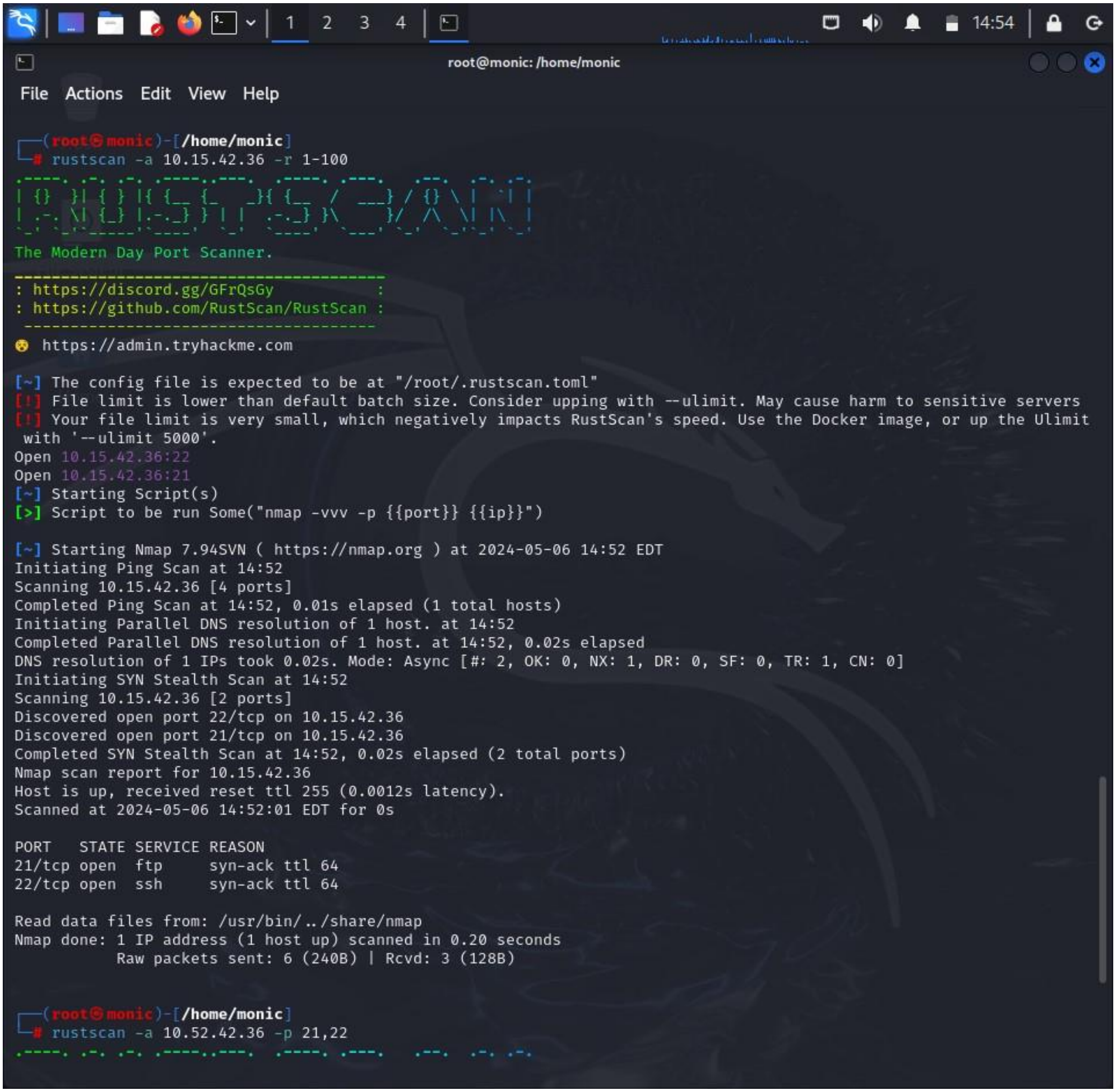
```
┌──(root㉿monic)-[/home/monic]
└─# nmap -T4 --min-rate 10000 -sCV -p- -A -Pn 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 07:20 EDT
Nmap scan report for 10.15.42.36
Host is up (0.042s latency).
Not shown: 42112 filtered tcp ports (no-response), 23420 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.8.188.222
|      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 1
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 172.19.0.2 is not the same as 10.15.42.36
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-server-header: Apache/2.4.38 (Debian)
|_http-title: Login Page
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (94%), QEMU (92%), Bay Networks embedded (86%), Linux (85%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450 cpe:/o:linux:linux_kernel:2.6.18
Aggressive OS guesses: Oracle Virtualbox (94%), QEMU user mode network gateway (92%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%), Linux 2.6.18 (CentOS 5, x86_64, SMP) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 6003/tcp)
HOP RTT     ADDRESS
1   3.12 ms 10.0.2.2
2   6.64 ms 10.15.42.36

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 194.25 seconds
```



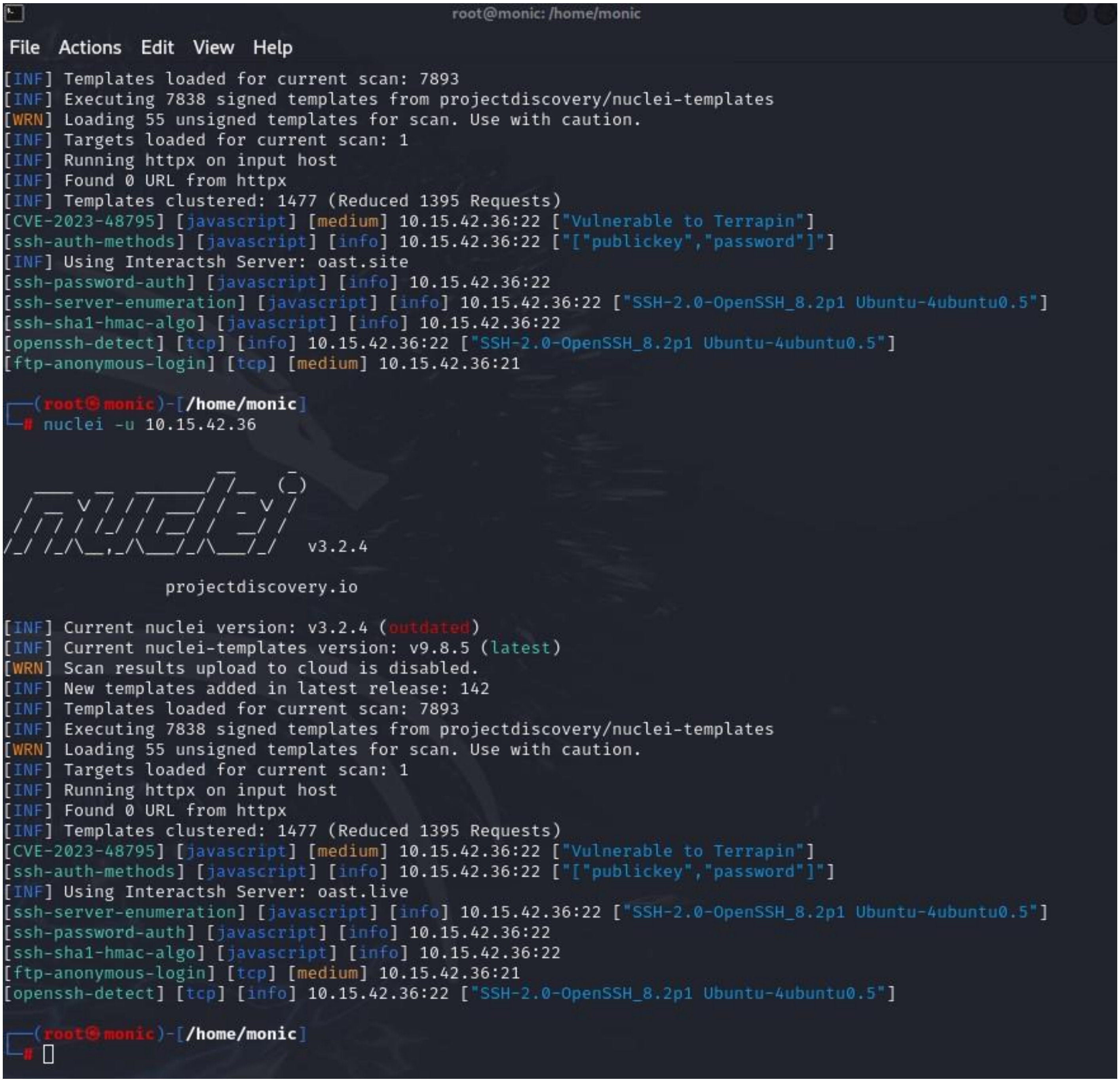
```
┌──(root㉿monic)-[/home/monic]
└─# nmap -sV -sC -oN nmaplog.log 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 13:48 EDT
Nmap scan report for 10.15.42.36
Host is up (0.0029s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.8.188.222
|      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 1
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protoco
l 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-server-header: Apache/2.4.38 (Debian)
|_http-title: Login Page
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.50 seconds

┌──(root㉿monic)-[/home/monic]
└─# wget http://10.15.42.36:8888
--2024-05-06 13:51:37--  http://10.15.42.36:8888/
Connecting to 10.15.42.36:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: 603 [text/html]
Saving to: 'index.html'

index.html          100%[===================>]     603  --.-KB/s    in 0s

2024-05-06 13:51:37 (47.2 MB/s) - 'index.html' saved [603/603]


┌──(root㉿monic)-[/home/monic]
```



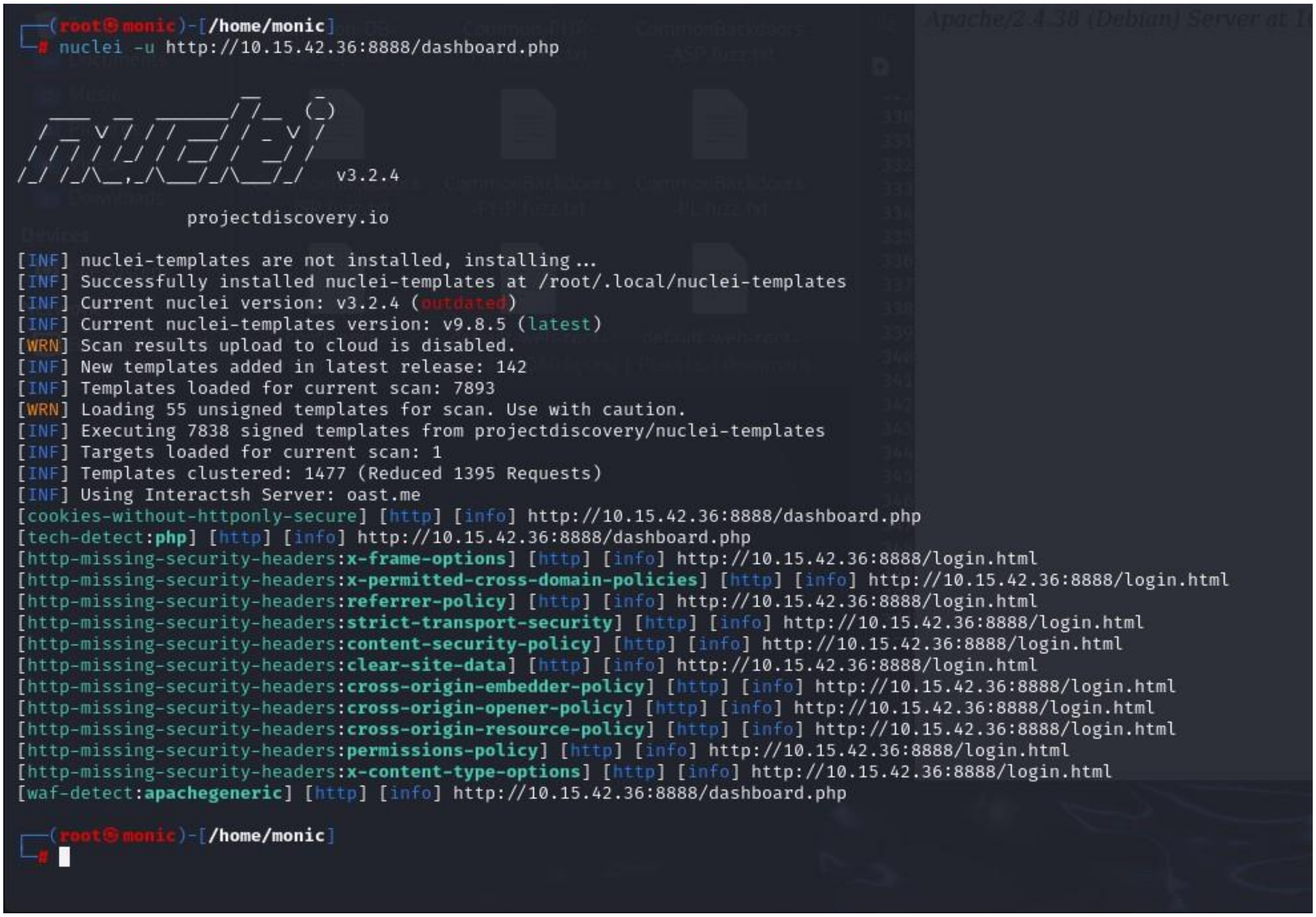
```
┌──(root㉿monic)-[/home/monic]
└─# ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:monic): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -a
229 Entering Extended Passive Mode (|||65503|)
150 Here comes the directory listing.
drwxrwxr-x    2 ftp      ftp          4096 May 04 15:40 .
drwxrwxr-x    2 ftp      ftp          4096 May 04 15:40 ..
-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 (|||65510|)
150 Opening BINARY mode data connection for backup.sql (1997 bytes).
100% |***********************************************************************|  1997        6.92 MiB/s    00:00 ETA
226 Transfer complete.
1997 bytes received in 00:00 (118.52 KiB/s)
ftp> █
```



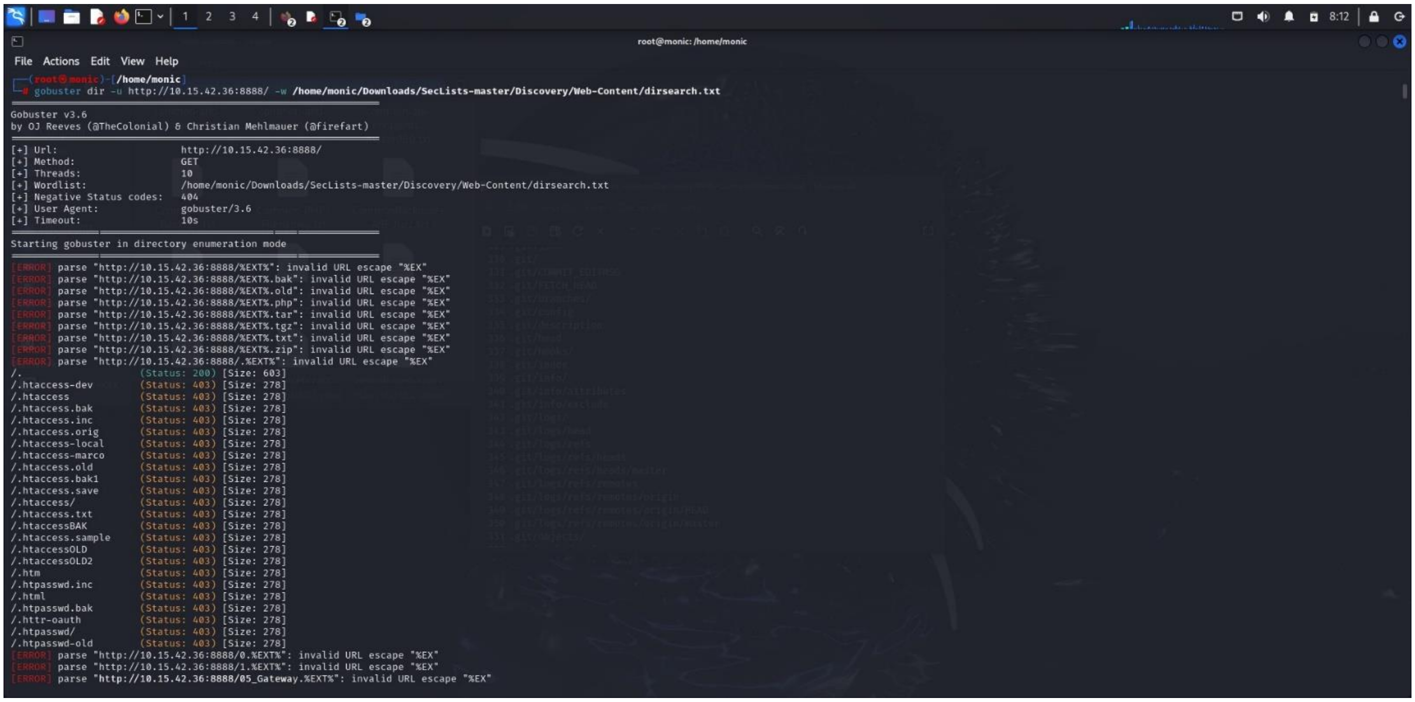
```
┌──(root㉿monic)-[/home/monic]
└─# rustscan -a 10.15.42.36 -r 1-100
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
😵 https://admin.tryhackme.com

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit
 with '--ulimit 5000'.
Open 10.15.42.36:22
Open 10.15.42.36:21
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")

[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 14:52 EDT
Initiating Ping Scan at 14:52
Scanning 10.15.42.36 [4 ports]
Completed Ping Scan at 14:52, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:52
Completed Parallel DNS resolution of 1 host. at 14:52, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 14:52
Scanning 10.15.42.36 [2 ports]
Discovered open port 22/tcp on 10.15.42.36
Discovered open port 21/tcp on 10.15.42.36
Completed SYN Stealth Scan at 14:52, 0.02s elapsed (2 total ports)
Nmap scan report for 10.15.42.36
Host is up, received reset ttl 255 (0.0012s latency).
Scanned at 2024-05-06 14:52:01 EDT for 0s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 64
22/tcp open  ssh     syn-ack ttl 64

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
           Raw packets sent: 6 (240B) | Rcvd: 3 (128B)


┌──(root㉿monic)-[/home/monic]
└─# rustscan -a 10.52.42.36 -p 21,22
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
```



```
[INF] Templates loaded for current scan: 7893
[INF] Executing 7838 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 55 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 0 URL from httpx
[INF] Templates clustered: 1477 (Reduced 1395 Requests)
[CVE-2023-48795] [javascript] [medium] 10.15.42.36:22 ["Vulnerable to Terrapin"]
[ssh-auth-methods] [javascript] [info] 10.15.42.36:22 ["["publickey","password"]"]
[INF] Using Interactsh Server: oast.site
[ssh-password-auth] [javascript] [info] 10.15.42.36:22
[ssh-server-enumeration] [javascript] [info] 10.15.42.36:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
[ssh-sha1-hmac-algo] [javascript] [info] 10.15.42.36:22
[openssh-detect] [tcp] [info] 10.15.42.36:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
[ftp-anonymous-login] [tcp] [medium] 10.15.42.36:21

┌──(root㉿monic)-[/home/monic]
└─# nuclei -u 10.15.42.36

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.2.4

                projectdiscovery.io

[INF] Current nuclei version: v3.2.4 (outdated)
[INF] Current nuclei-templates version: v9.8.5 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 142
[INF] Templates loaded for current scan: 7893
[INF] Executing 7838 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 55 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 0 URL from httpx
[INF] Templates clustered: 1477 (Reduced 1395 Requests)
[CVE-2023-48795] [javascript] [medium] 10.15.42.36:22 ["Vulnerable to Terrapin"]
[ssh-auth-methods] [javascript] [info] 10.15.42.36:22 ["["publickey","password"]"]
[INF] Using Interactsh Server: oast.live
[ssh-server-enumeration] [javascript] [info] 10.15.42.36:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
[ssh-password-auth] [javascript] [info] 10.15.42.36:22
[ssh-sha1-hmac-algo] [javascript] [info] 10.15.42.36:22
[ftp-anonymous-login] [tcp] [medium] 10.15.42.36:21
[openssh-detect] [tcp] [info] 10.15.42.36:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]

┌──(root㉿monic)-[/home/monic]
└─# 
```



```
┌──(root㉿monic)-[/home/monic]
└─# nuclei -u http://10.15.42.36:8888/dashboard.php

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.2.4

                projectdiscovery.io

[INF] nuclei-templates are not installed, installing...
[INF] Successfully installed nuclei-templates at /root/.local/nuclei-templates
[INF] Current nuclei version: v3.2.4 (outdated)
[INF] Current nuclei-templates version: v9.8.5 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 142
[INF] Templates loaded for current scan: 7893
[WRN] Loading 55 unsigned templates for scan. Use with caution.
[INF] Executing 7838 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1477 (Reduced 1395 Requests)
[INF] Using Interactsh Server: oast.me
[cookies-without-httponly-secure] [http] [info] http://10.15.42.36:8888/dashboard.php
[tech-detect:php] [http] [info] http://10.15.42.36:8888/dashboard.php
[http-missing-security-headers:x-frame-options] [http] [info] http://10.15.42.36:8888/login.html
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.15.42.36:8888/login.html
[http-missing-security-headers:referrer-policy] [http] [info] http://10.15.42.36:8888/login.html
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.15.42.36:8888/login.html
[http-missing-security-headers:content-security-policy] [http] [info] http://10.15.42.36:8888/login.html
[http-missing-security-headers:clear-site-data] [http] [info] http://10.15.42.36:8888/login.html
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://10.15.42.36:8888/login.html
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.15.42.36:8888/login.html
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://10.15.42.36:8888/login.html
[http-missing-security-headers:permissions-policy] [http] [info] http://10.15.42.36:8888/login.html
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.15.42.36:8888/login.html
[waf-detect:apachegeneric] [http] [info] http://10.15.42.36:8888/dashboard.php

┌──(root㉿monic)-[/home/monic]
└─# 
```



```
┌──(root㉿monic)-[/home/monic]
└─# gobuster dir -u http://10.15.42.36:8888/ -w /home/monic/Downloads/SecLists-master/Discovery/Web-Content/dirsearch.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.15.42.36:8888/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/monic/Downloads/SecLists-master/Discovery/Web-Content/dirsearch.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
[ERROR] parse "http://10.15.42.36:8888/%EXT%": invalid URL escape "%EX"
[ERROR] parse "http://10.15.42.36:8888/%EXT%.bak": invalid URL escape "%EX"
[ERROR] parse "http://10.15.42.36:8888/%EXT%.old": invalid URL escape "%EX"
[ERROR] parse "http://10.15.42.36:8888/%EXT%.php": invalid URL escape "%EX"
[ERROR] parse "http://10.15.42.36:8888/%EXT%.tar": invalid URL escape "%EX"
[ERROR] parse "http://10.15.42.36:8888/%EXT%.tgz": invalid URL escape "%EX"
[ERROR] parse "http://10.15.42.36:8888/%EXT%.txt": invalid URL escape "%EX"
[ERROR] parse "http://10.15.42.36:8888/%EXT%.zip": invalid URL escape "%EX"
[ERROR] parse "http://10.15.42.36:8888/.%EXT%": invalid URL escape "%EX"
/.                    (Status: 200) [Size: 603]
/.htaccess-dev        (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htaccess.bak        (Status: 403) [Size: 278]
/.htaccess.inc        (Status: 403) [Size: 278]
/.htaccess.orig       (Status: 403) [Size: 278]
/.htaccess-local      (Status: 403) [Size: 278]
/.htaccess-marco      (Status: 403) [Size: 278]
/.htaccess.old        (Status: 403) [Size: 278]
/.htaccess.bak1       (Status: 403) [Size: 278]
/.htaccess.save       (Status: 403) [Size: 278]
/.htaccess/           (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/.htaccessBAK         (Status: 403) [Size: 278]
/.htaccess.sample     (Status: 403) [Size: 278]
/.htaccessOLD         (Status: 403) [Size: 278]
/.htaccessOLD2        (Status: 403) [Size: 278]
/.htm                 (Status: 403) [Size: 278]
/.htpasswd.inc        (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/.htpasswd.bak        (Status: 403) [Size: 278]
/.httr-oauth          (Status: 403) [Size: 278]
/.htpasswd/           (Status: 403) [Size: 278]
/.htpasswd-old        (Status: 403) [Size: 278]
[ERROR] parse "http://10.15.42.36:8888/0.%EXT%": invalid URL escape "%EX"
[ERROR] parse "http://10.15.42.36:8888/1.%EXT%": invalid URL escape "%EX"
[ERROR] parse "http://10.15.42.36:8888/05_Gateway.%EXT%": invalid URL escape "%EX"
```

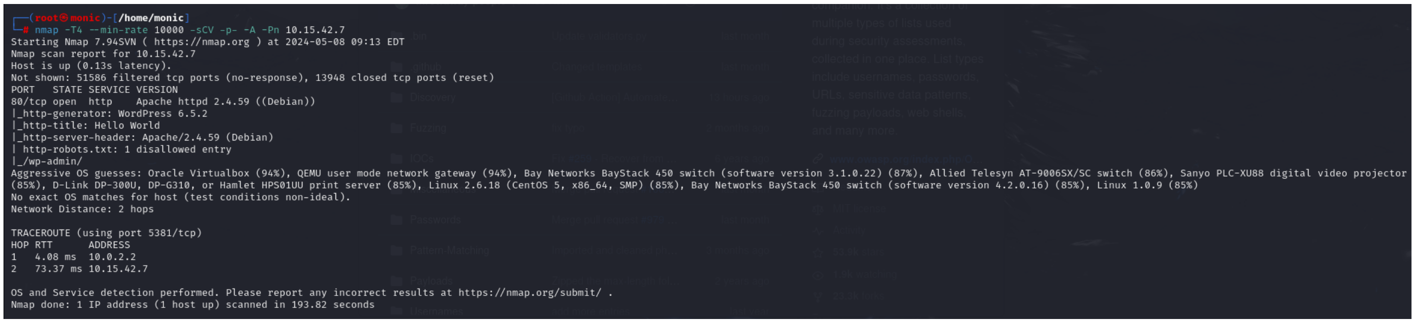
Remediation

To remediate the anonymous FTP login vulnerability on 10.15.42.36, FortifyTech must promptly disable anonymous access, enforce strong authentication, restrict FTP access, harden the server configuration, enable secure protocols, regularly patch and update, implement logging and monitoring, enforce least privilege access controls, and conduct routine security audits..

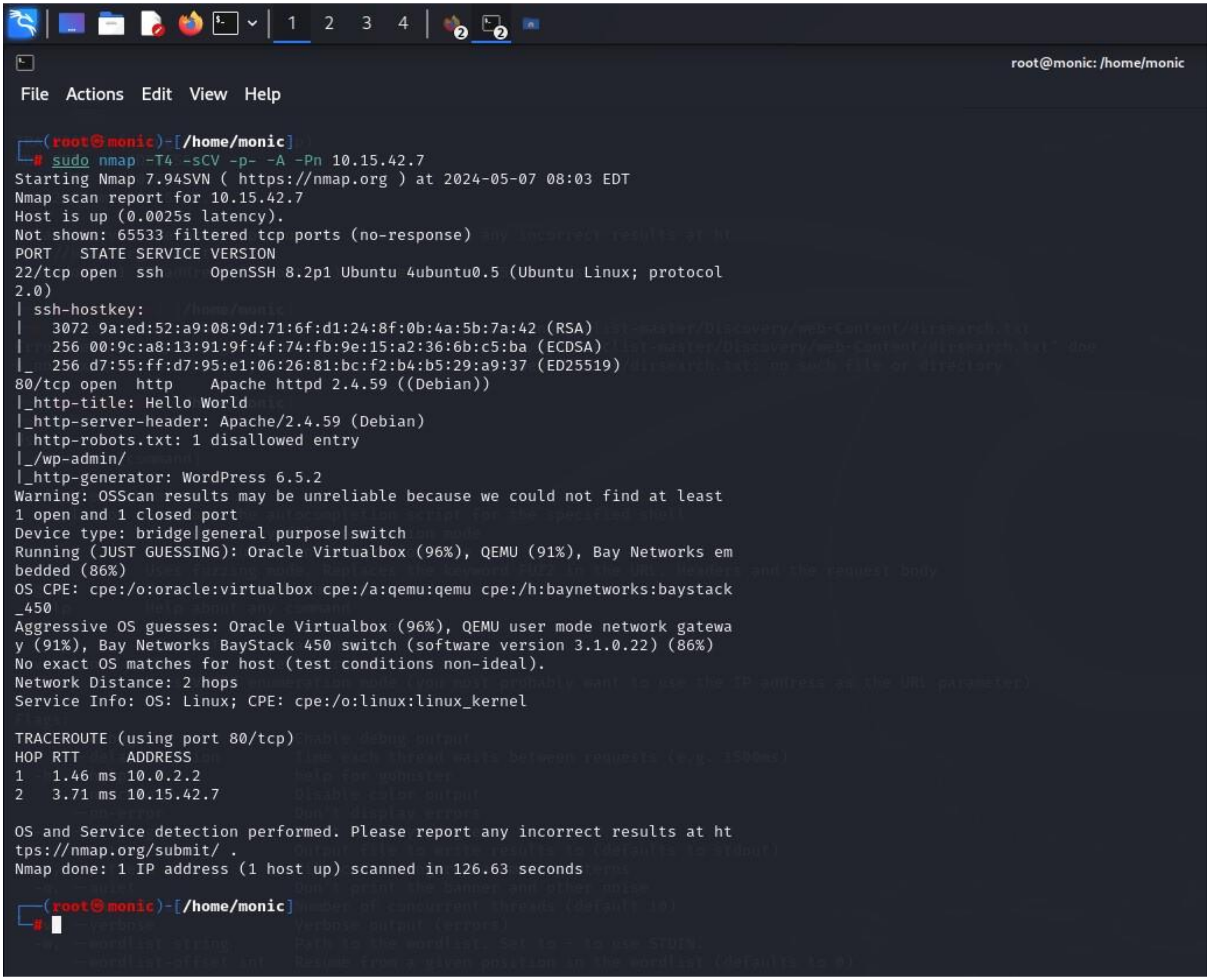
Finding IPT-002: XSS vulnerability in 10.15.42.7 running WordPress 6.5.2(Moderate)

Description:	The Nmap scan revealed an HTTP service running on port 80, identified as Apache httpd 2.4.59 (Debian). The server is hosting a WordPress installation, version 6.5.2, as indicated by the "http-generator" header. The scan also detected that the "/wp-admin/" directory is disallowed in the robots.txt file, suggesting that the WordPress administration area may be accessible.
Risk:	Likelihood: Moderate – WordPress installations are commonly targeted by attackers due to their widespread use and the availability of various exploit techniques and tools. Impact: Moderate – If the WordPress installation is not properly secured and updated, it could be vulnerable to various attacks such as data loss or takeover of control by other system.
System:	All
Tools Used:	Nmap on Kali Linux

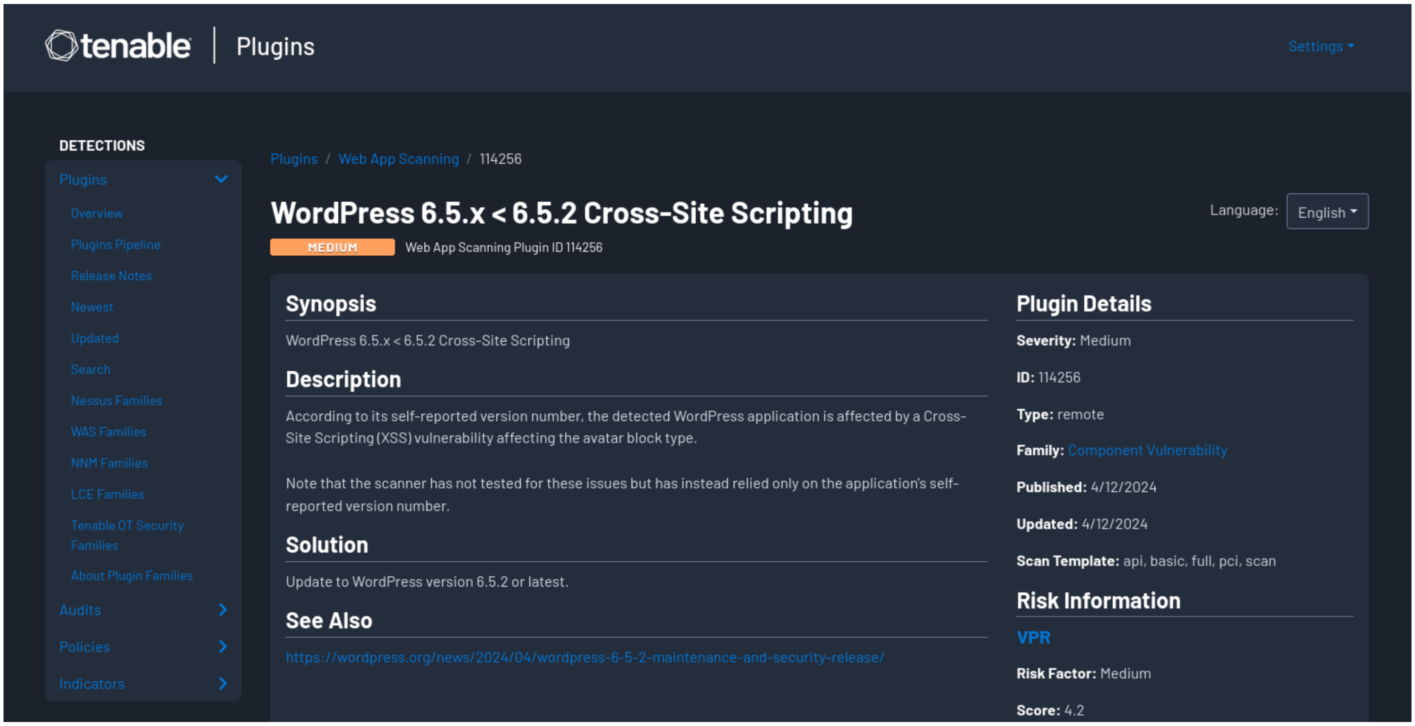
Evidence



```
┌──(root㉿monic)-[/home/monic]
└─# nmap -T4 --min-rate 10000 -sCV -p- -A -Pn 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 09:13 EDT
Nmap scan report for 10.15.42.7
Host is up (0.13s latency).
Not shown: 51586 filtered tcp ports (no-response), 13948 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
|_http-generator: WordPress 6.5.2
|_http-title: Hello World
|_http-server-header: Apache/2.4.59 (Debian)
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
Aggressive OS guesses: Oracle Virtualbox (94%), QEMU user mode network gateway (94%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (87%), Allied Telesyn AT-9006SX/SC switch (86%), Sanyo PLC-XU88 digital video projector
(85%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU print server (85%), Linux 2.6.18 (CentOS 5, x86_64, SMP) (85%), Bay Networks BayStack 450 switch (software version 4.2.0.16) (85%), Linux 1.0.9 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 5381/tcp)
HOP RTT      ADDRESS
1   4.08 ms  10.0.2.2
2   73.37 ms 10.15.42.7

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 193.82 seconds
```



```
┌──(root㉿monic)-[/home/monic]
└─# sudo nmap -T4 -sCV -p- -A -Pn 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 08:03 EDT
Nmap scan report for 10.15.42.7
Host is up (0.0025s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 9a:ed:52:a9:08:9d:71:6f:d1:24:8f:0b:4a:5b:7a:42 (RSA)
|   256 00:9c:a8:13:91:9f:4f:74:fb:9e:15:a2:36:6b:c5:ba (ECDSA)
|_  256 d7:55:ff:d7:95:e1:06:26:81:bc:f2:b4:b5:29:a9:37 (ED25519)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: Hello World
|_http-server-header: Apache/2.4.59 (Debian)
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-generator: WordPress 6.5.2
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks em
bedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack
_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gatewa
y (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   1.46 ms 10.0.2.2
2   3.71 ms 10.15.42.7

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.63 seconds

┌──(root㉿monic)-[/home/monic]
└─# 
```



Plugins / Web App Scanning / 114256

WordPress 6.5.x < 6.5.2 Cross-Site Scripting

MEDIUM Web App Scanning Plugin ID 114256

Synopsis

WordPress 6.5.x < 6.5.2 Cross-Site Scripting

Description

According to its self-reported version number, the detected WordPress application is affected by a Cross-Site Scripting (XSS) vulnerability affecting the avatar block type.

Note that the scanner has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Update to WordPress version 6.5.2 or latest.

See Also

https://wordpress.org/news/2024/04/wordpress-6-5-2-maintenance-and-security-release/

Plugin Details

Severity: Medium

ID: 114256

Type: remote

Family: Component Vulnerability

Published: 4/12/2024

Updated: 4/12/2024

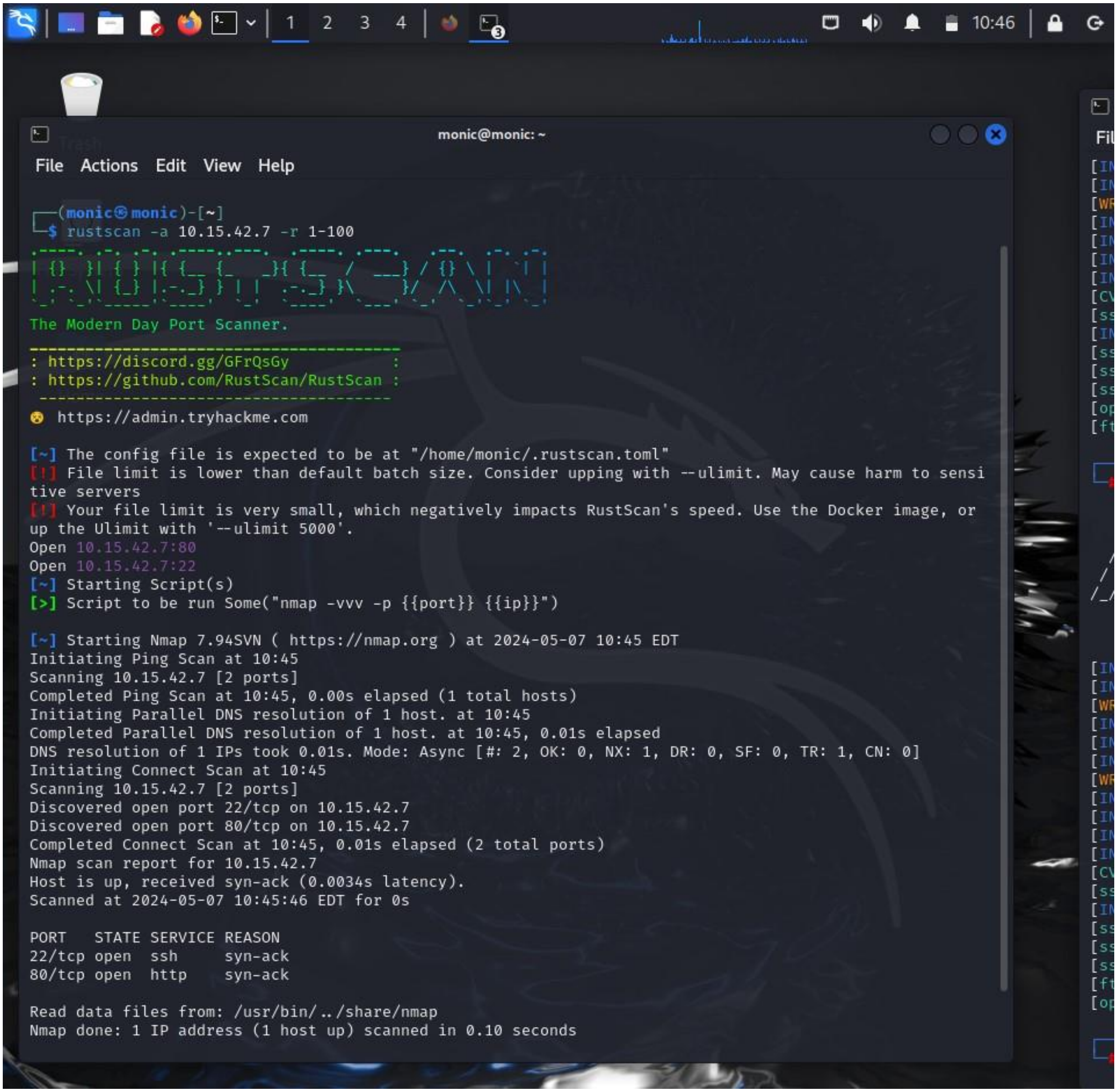
Scan Template: api, basic, full, pci, scan

Risk Information

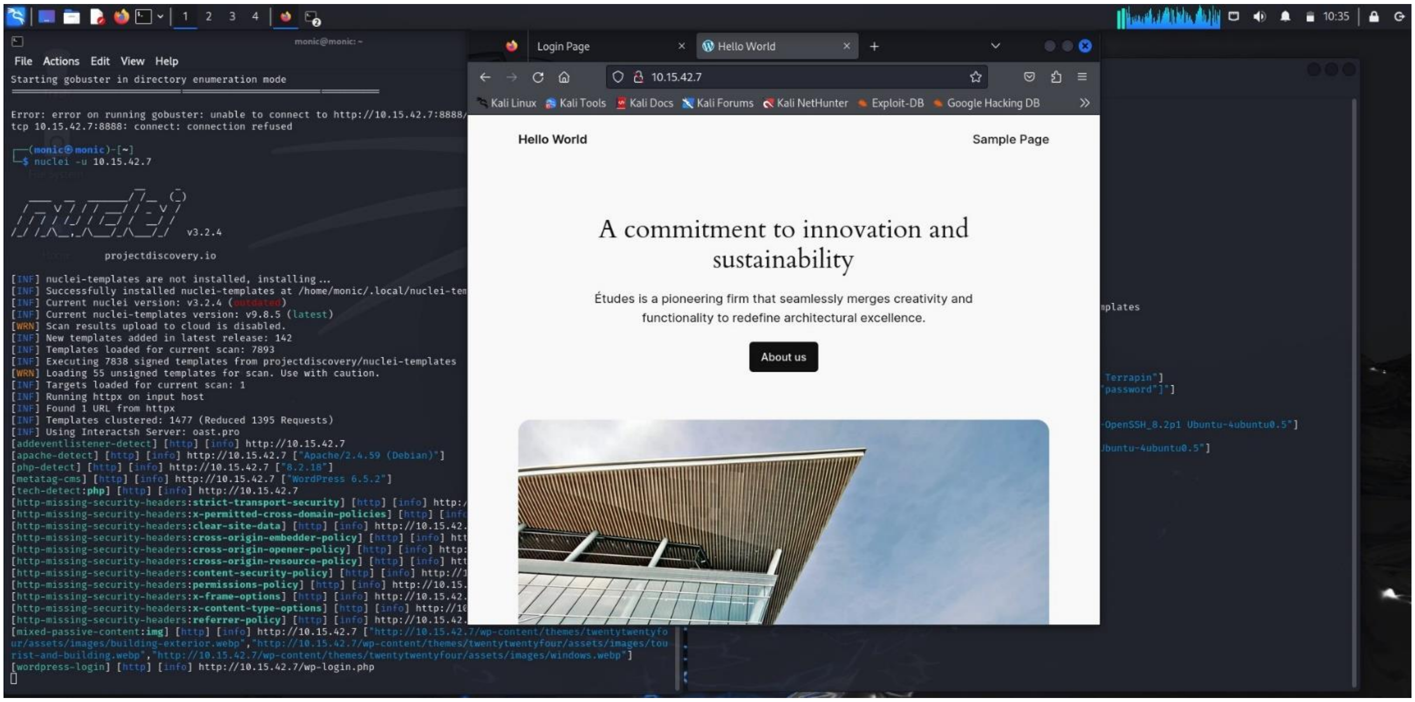
VPR

Risk Factor: Medium

Score: 4.2



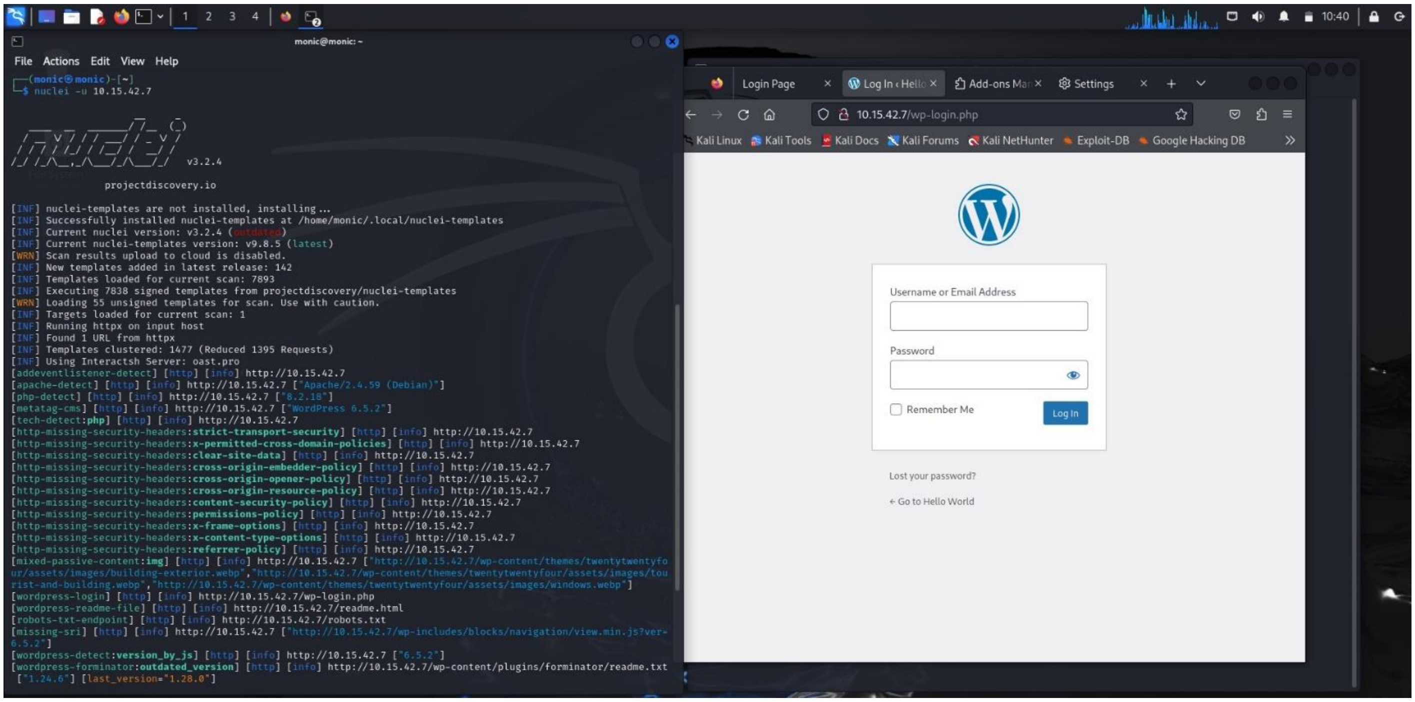
```
┌──(monic㉿monic)-[~]
└─$ rustscan -a 10.15.42.7 -r 1-100
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
😵 https://admin.tryhackme.com

[~] The config file is expected to be at "/home/monic/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensi
tive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or
up the Ulimit with '--ulimit 5000'.
Open 10.15.42.7:80
Open 10.15.42.7:22
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")

[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:45 EDT
Initiating Ping Scan at 10:45
Scanning 10.15.42.7 [2 ports]
Completed Ping Scan at 10:45, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:45
Completed Parallel DNS resolution of 1 host. at 10:45, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 10:45
Scanning 10.15.42.7 [2 ports]
Discovered open port 22/tcp on 10.15.42.7
Discovered open port 80/tcp on 10.15.42.7
Completed Connect Scan at 10:45, 0.01s elapsed (2 total ports)
Nmap scan report for 10.15.42.7
Host is up, received syn-ack (0.0034s latency).
Scanned at 2024-05-07 10:45:46 EDT for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```



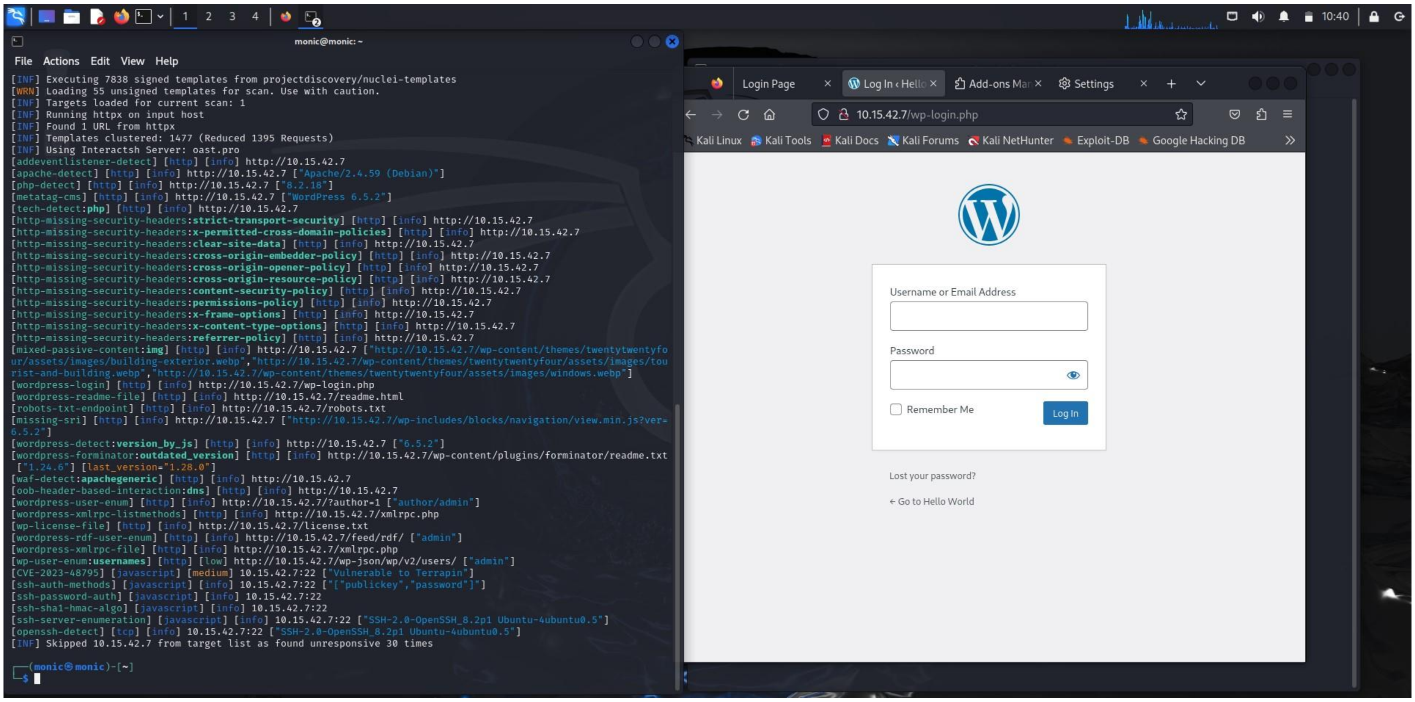
```
Starting gobuster in directory enumeration mode
===============================================================

Error: error on running gobuster: unable to connect to http://10.15.42.7:8888/
tcp 10.15.42.7:8888: connect: connection refused

┌──(monic㉿monic)-[~]
└─$ nuclei -u 10.15.42.7

                                        v3.2.4

                projectdiscovery.io

[INF] nuclei-templates are not installed, installing...
[INF] Successfully installed nuclei-templates at /home/monic/.local/nuclei-tem
[INF] Current nuclei version: v3.2.4 (outdated)
[INF] Current nuclei-templates version: v9.8.5 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 142
[INF] Templates loaded for current scan: 7893
[INF] Executing 7838 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 55 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1477 (Reduced 1395 Requests)
[INF] Using Interactsh Server: oast.pro
[addeventlistener-detect] [http] [info] http://10.15.42.7
[apache-detect] [http] [info] http://10.15.42.7 ["Apache/2.4.59 (Debian)"]
[php-detect] [http] [info] http://10.15.42.7 ["8.2.18"]
[metatag-cms] [http] [info] http://10.15.42.7 ["WordPress 6.5.2"]
[tech-detect:php] [http] [info] http://10.15.42.7
[http-missing-security-headers:strict-transport-security] [http] [info] http:/
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info
[http-missing-security-headers:clear-site-data] [http] [info] http://10.15.42.
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] htt
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http:
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] htt
[http-missing-security-headers:content-security-policy] [http] [info] http://1
[http-missing-security-headers:permissions-policy] [http] [info] http://10.15.
[http-missing-security-headers:x-frame-options] [http] [info] http://10.15.42.
[http-missing-security-headers:x-content-type-options] [http] [info] http://10
[http-missing-security-headers:referrer-policy] [http] [info] http://10.15.42.
[mixed-passive-content:img] [http] [info] http://10.15.42.7 ["http://10.15.42.7/wp-content/themes/twentytwentyfo
ur/assets/images/building-exterior.webp","http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/tou
rist-and-building.webp","http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/windows.webp"]
[wordpress-login] [http] [info] http://10.15.42.7/wp-login.php
```

```
mplates

 Terrapin"]
"password"]"]

-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]

Ubuntu-4ubuntu0.5"]
```

Login Page
Hello World
10.15.42.7
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Hello World
Sample Page
A commitment to innovation and sustainability
Études is a pioneering firm that seamlessly merges creativity and functionality to redefine architectural excellence.
About us



```
┌──(monic㉿monic)-[~]
└─$ nuclei -u 10.15.42.7

                                        v3.2.4

                projectdiscovery.io

[INF] nuclei-templates are not installed, installing...
[INF] Successfully installed nuclei-templates at /home/monic/.local/nuclei-templates
[INF] Current nuclei version: v3.2.4 (outdated)
[INF] Current nuclei-templates version: v9.8.5 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 142
[INF] Templates loaded for current scan: 7893
[INF] Executing 7838 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 55 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1477 (Reduced 1395 Requests)
[INF] Using Interactsh Server: oast.pro
[addeventlistener-detect] [http] [info] http://10.15.42.7
[apache-detect] [http] [info] http://10.15.42.7 ["Apache/2.4.59 (Debian)"]
[php-detect] [http] [info] http://10.15.42.7 ["8.2.18"]
[metatag-cms] [http] [info] http://10.15.42.7 ["WordPress 6.5.2"]
[tech-detect:php] [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:x-permitted-cross-domain-policies] [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:cross-origin-embedder-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:cross-origin-resource-policy] [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
[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:referrer-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/twentytwentyfo
ur/assets/images/building-exterior.webp","http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/tou
rist-and-building.webp","http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/windows.webp"]
[wordpress-login] [http] [info] http://10.15.42.7/wp-login.php
[wordpress-readme-file] [http] [info] http://10.15.42.7/readme.html
[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"]
[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"]
```



```
[INF] Executing 7838 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 55 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1477 (Reduced 1395 Requests)
[INF] Using Interactsh Server: oast.pro
[addeventlistener-detect] [http] [info] http://10.15.42.7
[apache-detect] [http] [info] http://10.15.42.7 ["Apache/2.4.59 (Debian)"]
[php-detect] [http] [info] http://10.15.42.7 ["8.2.18"]
[metatag-cms] [http] [info] http://10.15.42.7 ["WordPress 6.5.2"]
[tech-detect:php] [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:x-permitted-cross-domain-policies] [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:cross-origin-embedder-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:cross-origin-resource-policy] [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
[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:referrer-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/twentytwentyfo
ur/assets/images/building-exterior.webp","http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/tou
rist-and-building.webp","http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/windows.webp"]
[wordpress-login] [http] [info] http://10.15.42.7/wp-login.php
[wordpress-readme-file] [http] [info] http://10.15.42.7/readme.html
[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"]
[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"]
[waf-detect:apachegeneric] [http] [info] http://10.15.42.7
[oob-header-based-interaction:dns] [http] [info] http://10.15.42.7
[wordpress-user-enum] [http] [info] http://10.15.42.7/?author=1 ["author/admin"]
[wordpress-xmlrpc-listmethods] [http] [info] http://10.15.42.7/xmlrpc.php
[wp-license-file] [http] [info] http://10.15.42.7/license.txt
[wordpress-rdf-user-enum] [http] [info] http://10.15.42.7/feed/rdf/ ["admin"]
[wordpress-xmlrpc-file] [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"]
[CVE-2023-48795] [javascript] [medium] 10.15.42.7:22 ["Vulnerable to Terrapin"]
[ssh-auth-methods] [javascript] [info] 10.15.42.7:22 ["["publickey","password"]"]
[ssh-password-auth] [javascript] [info] 10.15.42.7:22
[ssh-sha1-hmac-algo] [javascript] [info] 10.15.42.7:22
[ssh-server-enumeration] [javascript] [info] 10.15.42.7:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
[openssh-detect] [tcp] [info] 10.15.42.7:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
[INF] Skipped 10.15.42.7 from target list as found unresponsive 30 times

┌──(monic㉿monic)-[~]
└─$ 
```

Username or Email Address

Password

□ Remember Me

Log In

Lost your password?

← Go to Hello World

Remediation

To remediate the risks associated with the WordPress installation on the host with IP 10.15.42.7, FortifyTech should promptly implement the following measures: ensure the WordPress core, plugins, and themes are up-to-date with the latest security patches; enforce strong authentication mechanisms and access controls; configure a web application firewall to protect against common attacks; regularly review and update WordPress security configurations; and conduct routine security audits and vulnerability assessments to identify and address any emerging threats.

Last Page