Ethical Hacking
Security Assessment Findings Report

Information Technology

Date: May 8th, 202
Project: DC-001

Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Demo Corp 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 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

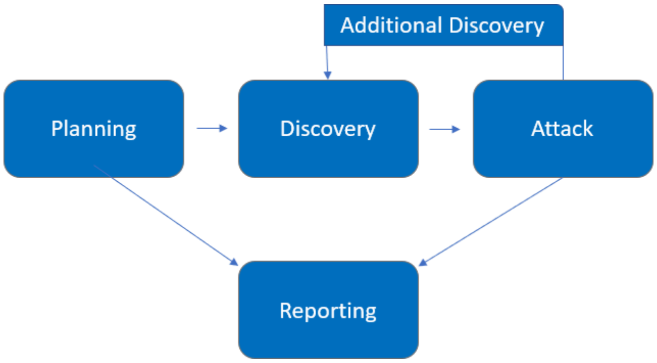
Name	Title	Contact Information
Demo Corp		
Subkhan Masudi	5027221044	Email: akutuban2@gmail.com

Assessment Overview

From May 07nd, 2024 to March 8th, 2024, All testing performed is based on the Information Security Testing and Assessment Technical Guide module, OWASP ZAP Testing Guide, 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	Definitio n
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.
Information al	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, TCMS 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 Demo Corp.

Client Allowances

Demo Corp provided TCMS the following allowances:

- Internal access to network via dropbox and port allowances

Executive Summary

TCMS evaluated Demo Corp's internal security posture through penetration testing from February 22nd, 2021 to March 5th, 2021. 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 ten (10) business days.

Testing Summary

The network assessment evaluated Demo Corp's internal network security posture. From an internal perspective, the TCMS team performed vulnerability scanning against all IPs provided by Demo Corp to evaluate the overall patching health of the network. The team also performed common Active Directory based attacks, such as Link-Local Multicast Name Resolution (LLMNR) Poisoning, SMB relaying, IPv6 man-in-the-middle relaying, and Kerberoasting. Beyond vulnerability scanning and Active Directory attacks, the TCMS evaluated other potential risks, such as open file shares, default credentials on servers/devices, and sensitive information disclosure to gain a complete picture of the network's security posture.

The TCMS team discovered that LLMNR was enabled in the network (Finding IPT-001), which permitted the interception of user hashes via LLMNR poisoning. These hashes were taken offline and cracked via dictionary attacks, which signals a weak password policy (Finding IPT-005). Utilizing the cracked passwords, the TCMS team gained access to several machines within the network, which indicates overly permissive user accounts.

With machine access, and the use of older operating systems in the network (Finding IPT-009), the team was able to leverage WDigest (Finding IPT-003) to recover cleartext credentials to accounts. The team was also able to dump local account hashes on each machine accessed. The TCMS team discovered that the local account hashes were being re-used across devices (Finding IPT-002), which lead to additional machine access through pass-the-hash attacks.

Ultimately, the TCMS team was able to leverage accounts captured through WDigest and hash dumps to move laterally throughout the network until landing on a machine that had a

Domain Administrator credential in cleartext via WDigest. The testing team was able to use this credential to log into the domain controller and compromise the entire domain. For a full walkthrough of the path to Domain Admin, please see Finding IPT-025.

In addition to the compromise listed above, the TCMS team found that users could be impersonated through delegation attacks (Finding IPT-004), SMB relay attacks were possible due to SMB signing being disabled (Finding IPT-007), and IPv6 traffic was not restricted, which could lead to LDAPS relaying and domain compromise (Finding IPT-006).

The remainder of critical findings relate to patch management as devices with critical out-of-date software (Finding IPT-008), operating systems (Finding IPT-009), and Microsoft RCE vulnerabilities (Findings IPT-010, IPT-011, IPT-012, IPT-013), were found to be present within the network.

The remainder of the findings were high, moderate, low, or informational. For further information on findings, please review the Technical Findings section.

Tester Notes and Recommendations

Testing results of the Demo Corp network are indicative of an organization undergoing its first penetration test, which is the case here. Many of the findings discovered are vulnerabilities within Active Directory that come enabled by default, such as LLMNR, IPv6, and Kerberoasting.

During testing, two constants stood out: a weak password policy and weak patching. The weak password policy led to the initial compromise of accounts and is usually one of the first footholds an attacker attempts to use in a network. The presence of a weak password policy is backed up by the evidence of our testing team cracking over 2,200 user account passwords, including a majority of the Domain Administrator accounts, through basic dictionary attacks.

We recommended that Demo Corp re-evaluates their current password policy and considers a policy of 15 characters or more for their regular user accounts and 30 characters or more for their Domain Administrator accounts. We also recommend that Demo Corp explore password blacklisting and will be supplying a list of cracked user passwords for the team to evaluate. Finally, a Privilege Access Management solution should be considered.

Weak patching and dated operating systems led to the compromise of dozens of machines within the network. We believe the number of compromised machines would have been significantly larger, however the TCMS and Demo Corp teams agreed it was not necessary to attempt to exploit any remote code execution (RCE) based vulnerabilities, such as MS17-010 (Finding IPT-012), as the domain controller had already been compromised and the teams did not want to risk any denial of service through failed attacks.

We recommend that the Demo Corp team review the patching recommendations made in the Technical Findings section of the report along with reviewing the provided Nessus scans for a full overview of items to be patched. We also recommend that Demo Corp improve their patch management policies and procedures to help prevent potential attacks within their network.

On a positive note, our testing team triggered several alerts during the engagement. The Demo Corp Security Operations team discovered our vulnerability scanning and was alerted when we attempted to use noisy attacks on a compromised machine. While not all attacks were discovered during testing, these alerts are a positive start. Additional guidance on alerting and detection has been provided for findings, when necessary, in the Technical Findings section.

Overall, the Demo Corp network performed as expected for a first-time penetration test. We recommend that the Demo Corp team thoroughly review the recommendations made in this report, patch the findings, and re-test annually to improve their overall internal security posture.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Observed some scanning of common enumeration tools (Nessus)
2. Mimikatz detected on some machines
3. Service accounts were not running as domain administrators
4. Demo Corp local administrator account password was unique to each device The following identifies the key weaknesses identified during the assessment:

1. Password policy found to be insufficient
2. Critically out-of-date operating systems and weak patching exist within the network
3. Passwords were observed in cleartext due to WDigest
4. LLMNR is enabled within the network
5. SMB signing is disabled on all non-server devices in the work
6. IPv6 is improperly managed within the network
7. User accounts can be impersonated through token delegation
8. Local admin accounts had password re-use and were overly permissive
9. Default credentials were discovered on critical infrastructure, such as iDRACs
10. Unauthenticated share access was permitted
11. User accounts were found to be running as service accounts
12. Service accounts utilized weak passwords
13. Domain administrator utilized weak passwords

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

0	0	4	7	4
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
Content Security Policy (CSP) Header Not Set	High	
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	High	
Absence of Anti-CSRF Tokens	Moderate	
Missing Anti-clickjacking Header	Moderate	
Vulnerable to Terrapin	Moderate	
Cookie No HttpOnly Flag	Low	
Cookie without SameSite Attribute	Low	
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	
X-Content-Type-Options Header Missing	Low	

there is port open on that 10.15.42.7 and 10.15.42.36	Low	
wp-user-enum:username open	Low	
Information Disclosure - Suspicious Comments	informational	
Modern Web Application	informational	
Session Management Response Identified	informational	
User Controllable HTML Element Attribute (Potential XSS)	informational	

Technical Findings

Internal Penetration Test Findings

Absence of Anti-CSRF Tokens (moderate)

Description:	This alert indicates that the website lacks Anti-CSRF tokens, leaving it vulnerable to Cross-Site Request Forgery attacks.
Risk:	CSRF attacks can lead to unauthorized actions being performed on behalf of the user, such as changing settings, making purchases, or transferring funds.
System:	Web applications that rely on session cookies for authentication.
Tools Used:	OWASP ZAP
References:	http://projects.webappsec.org/Cross-Site-Request-Forgery https://cwe.mitre.org/data/definitions/352.html

Evidence

https://drive.google.com/drive/folders/1saldHwObyppjaqi5ARf1HN64u3-WGJm3?usp=sharing

Remediation

Implement the use of Anti-CSRF tokens on web forms to prevent CSRF attacks. These tokens should be included with every action that affects server data

Content Security Policy (CSP) Header Not Set

Description:	This alert indicates that the website doesn't have a Content Security Policy (CSP) header configured, making it more susceptible to various web-based attacks.
Risk:	Without CSP, the site is more vulnerable to XSS, data injection, and other code injection attacks.
System:	All
Tools Used:	OWASP ZAP
References:	1. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy 2. https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html 3. http://www.w3.org/TR/CSP/ 4. http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html 5. http://www.html5rocks.com/en/tutorials/security/content-security-policy/ 6. http://caniuse.com/#feat=contentsecuritypolicy 7. http://content-security-policy.com/

Evidence

https://drive.google.com/drive/folders/1saldHwObyppjaqi5ARf1HN64u3-WGJm3?usp=sharing

Remediation

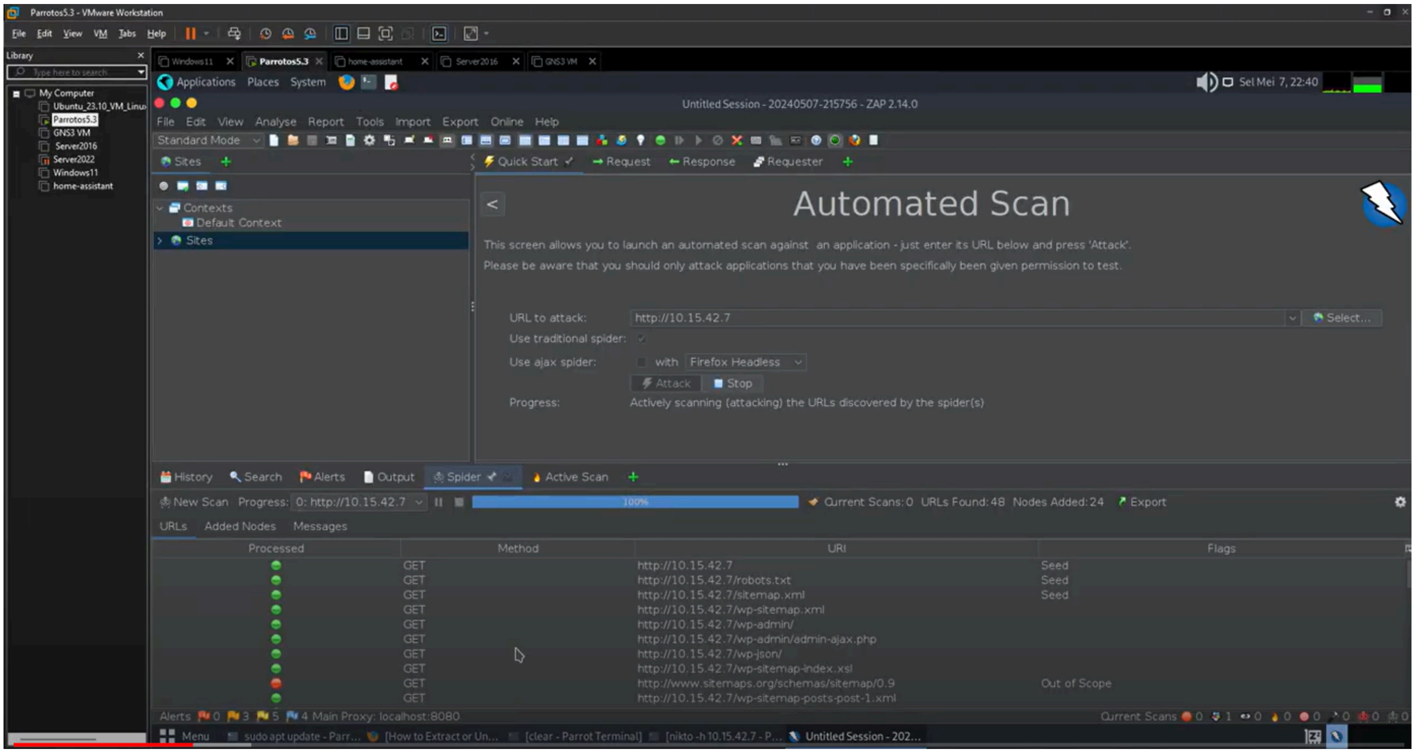
Configure the CSP header with a policy that restricts the resources allowed to be loaded by the web page. Ensure to set a policy that is appropriate for the application's needs.

Missing Anti-clickjacking Header

Description:	This alert indicates that the website is missing the X-Frame-Options header, making it vulnerable to clickjacking attacks.
Risk:	Clickjacking attacks can trick users into performing unintended actions by embedding the website in an invisible iframe.
System:	Web applications that load in iframes
Tools Used:	OWASP ZAP
References:	1. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Evidence

-



Untitled Session - 20240507-215756 - ZAP 2.14.0

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://10.15.42.7
Use traditional spider: ✓
Use ajax spider: □ with Firefox Headless
Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

New Scan Progress: 0: http://10.15.42.7 100% Current Scans: 0 URLs Found: 48 Nodes Added: 24

Processed	Method	URI	Flags
●	GET	http://10.15.42.7	Seed
●	GET	http://10.15.42.7/robots.txt	Seed
●	GET	http://10.15.42.7/sitemap.xml	Seed
●	GET	http://10.15.42.7/wp-sitemap.xml	
●	GET	http://10.15.42.7/wp-admin/	
●	GET	http://10.15.42.7/wp-admin/admin-ajax.php	
●	GET	http://10.15.42.7/wp-json/	
●	GET	http://10.15.42.7/wp-sitemap-index.xsl	
●	GET	http://www.sitemaps.org/schemas/sitemap/0.9	Out of Scope
●	GET	http://10.15.42.7/wp-sitemap-posts-post-1.xml	

Alerts 0 3 5 4 Main Proxy: localhost:8080

Remediation

Add the X-Frame-Options header with a value of "DENY" or "SAMEORIGIN" to protect the website from clickjacking attacks. This can be done by configuring the web server or using headers within the application.

Cookie No HttpOnly Flag

Description:	This alert indicates that the HttpOnly flag is not set on cookies, allowing them to be accessed by client-side scripts.
Risk:	Without the HttpOnly flag, cookies are vulnerable to theft via XSS attacks, potentially leading to session hijacking or other unauthorized actions.
System:	Web applications that utilize cookies for session management
Tools Used:	OWASP ZAP, Cheat Sheet
References:	1. https://owasp.org/www-community/HttpOnly

Evidence

https://drive.google.com/drive/folders/1saldHwObyppjaqi5ARf1HN64u3-WGJm3?usp=sharing

Remediation

Ensure all cookies used by the application have the HttpOnly flag set. This can be done through server configuration or adjustments to the application code that sets cookies.

Cookie without SameSite Attribute

Description:	This alert indicates that cookies are missing the SameSite attribute, which can help mitigate CSRF and XSSI attacks.
Risk:	Without the SameSite attribute, cookies are vulnerable to CSRF attacks, allowing unauthorized actions to be performed on behalf of the user.
System:	Web applications that rely on cookies for session management.
Tools Used:	OWASP ZAP
References:	1. https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Evidence

https://drive.google.com/drive/folders/1saldHwObyppjaqi5ARf1HN64u3-WGJm3?usp=sharing

Remediation

Add the SameSite attribute to all cookies used by the application. You can set the SameSite value as "Strict" or "Lax" depending on the application's needs.

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description:	This alert indicates that the server is disclosing information via the "X-Powered-By" HTTP response header, potentially revealing sensitive details about server technologies.
Risk:	Disclosure of server technologies can aid attackers in crafting targeted attacks against known vulnerabilities.
System:	Web servers and applications.
Tools Used:	OWASP ZAP
References:	1. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx 2. http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Evidence

https://drive.google.com/drive/folders/1saldHwObyppjaqi5ARf1HN64u3-WGJm3?usp=sharing

Remediation

Configure the web server to remove or hide the "X-Powered-By" response header. This can be done through web server configuration such as Apache or Nginx.

X-Content-Type-Options Header Missing

Description:	This alert indicates that the X-Content-Type-Options header is missing, leaving the website vulnerable to MIME-sniffing attacks.
Risk:	Without the X-Content-Type-Options header, browsers may attempt to guess the content type, leading to potential security risks like XSS attacks.
System:	Any web application.
Tools Used:	OWASP ZAP,http response headers

References:	1. http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx 2. https://owasp.org/www-community/Security_Headers

Evidence

https://drive.google.com/drive/folders/1saldHwObyppjaqi5ARf1HN64u3-WGJm3?usp=sharing

Remediation

Add the X-Content-Type-Options header with a value of "nosniff" to every HTTP response to prevent MIME-sniffing. This can be done through server configuration or adjustments to the application.

Information Disclosure - Suspicious Comment

Description:	This alert indicates the presence of suspicious comments in the website's source code, potentially leaking sensitive information.
Risk:	Suspicious comments may inadvertently reveal implementation details or sensitive information, aiding attackers in identifying vulnerabilities.
System:	Web applications.
Tools Used:	OWASP ZAP
References:	(Information Disclosure - Suspicious Comments)CWE ID200WASC ID13

Evidence

https://drive.google.com/drive/folders/1saldHwObyppjaqi5ARf1HN64u3-WGJm3?usp=sharing

Remediation

Check and remove all suspicious comments from the application's source code. Ensure not to leave comments that may provide sensitive information.

Modern Web Application

Description:	This alert signifies that the website is built using modern web application technologies.
Risk:	Depending on implementation, modern web applications may introduce new attack vectors or vulnerabilities.
System:	Any modern web application.
Tools Used:	OWASP ZAP
References:	raised by a passive scanner (Modern Web Application)

Evidence

https://drive.google.com/drive/folders/1saldHwObyppjaqi5ARf1HN64u3-WGJm3?usp=sharing

Remediation

Ensure all technologies and frameworks used in the application development are updated to the latest secure versions. Conduct regular security scans to detect and fix existing vulnerabilities.

Session Management Response Identifie

Description:	This alert indicates the identification of a response related to session management.
Risk:	Session management issues can lead to unauthorized access, session hijacking, or other security compromises.
System:	Web applications with session management functionality.
Tools Used:	OWASP ZAP
References:	1. https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id

Evidence

https://drive.google.com/drive/folders/1saldHwObyppjaqi5ARf1HN64u3-WGJm3?usp=sharing

Remediation

Check and ensure session management is implemented correctly and securely. Use strong authentication and authorization methods, and ensure sessions are handled properly and not vulnerable to attacks like session fixation or session hijacking.

User Controllable HTML Element Attribute (Potential XSS)

Description:	This alert indicates user-controllable HTML element attributes, which may pose potential XSS vulnerabilities.
Risk:	XSS vulnerabilities can allow attackers to execute malicious scripts in the context of other users' sessions.
System:	Web applications that render user-generated content.
Tools Used:	OWASP ZAP, inspection of HTML source code
References:	1. http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute

Evidence

https://drive.google.com/drive/folders/1saldHwObyppjaqi5ARf1HN64u3-WGJm3?usp=sharing

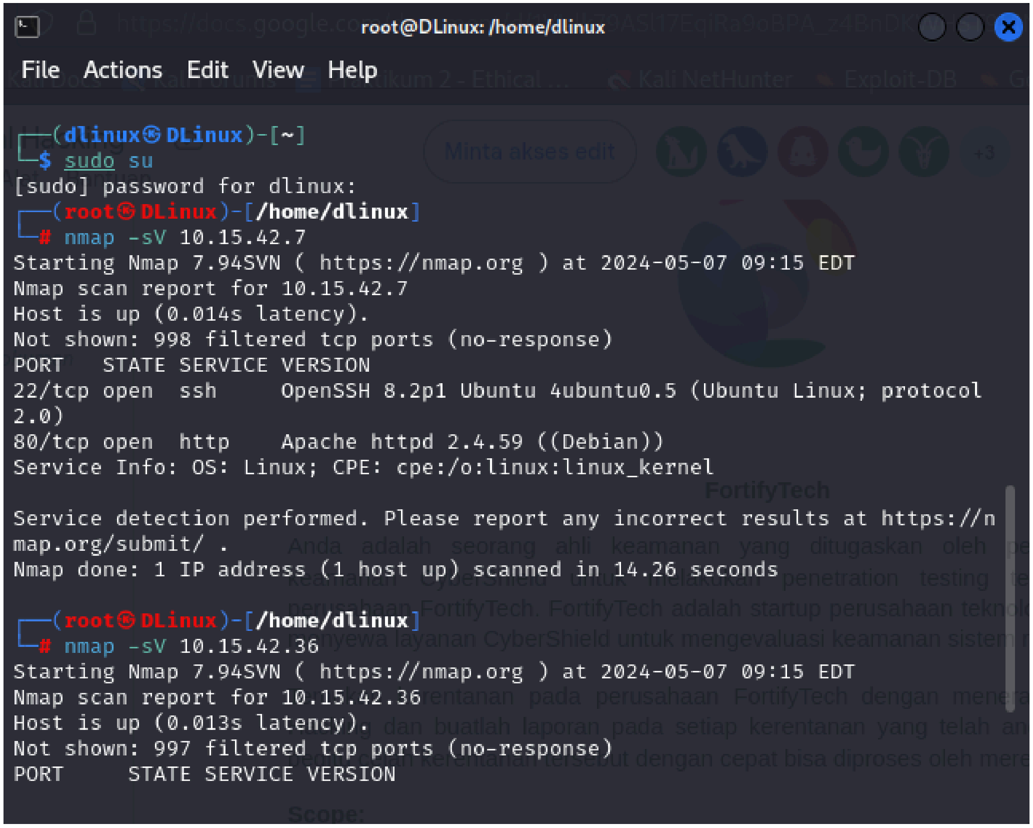
Remediation

Sanitize all user input included in HTML element attributes. This can be done by removing or disallowing unwanted special characters, or by using sanitization libraries or functions available in the framework or programming language used.

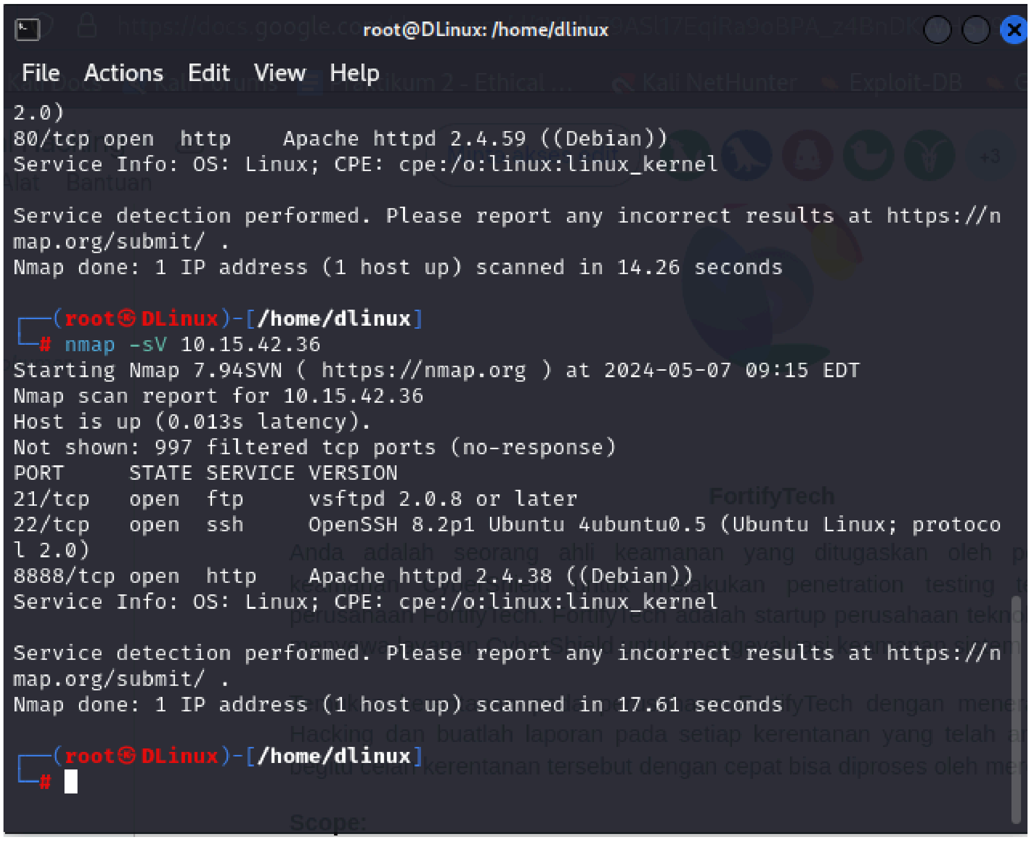
Port Open on 10.15.42.7 and 10.15.42.36

Description:	This alert indicates that there is a port open on both IP addresses, 10.15.42.7 and 10.15.42.36. Specifically, port `wp-user-enum:username` is open.
Risk:	Open ports can provide entry points for attackers to gain unauthorized access to the system. Depending on the service running on the open port, there could be various risks, including unauthorized data access, service disruption, or even complete system compromise.
System:	Systems with the open port, specifically IP addresses 10.15.42.7 and 10.15.42.36.
Tools Used:	Nmap
References:	nmap apllication

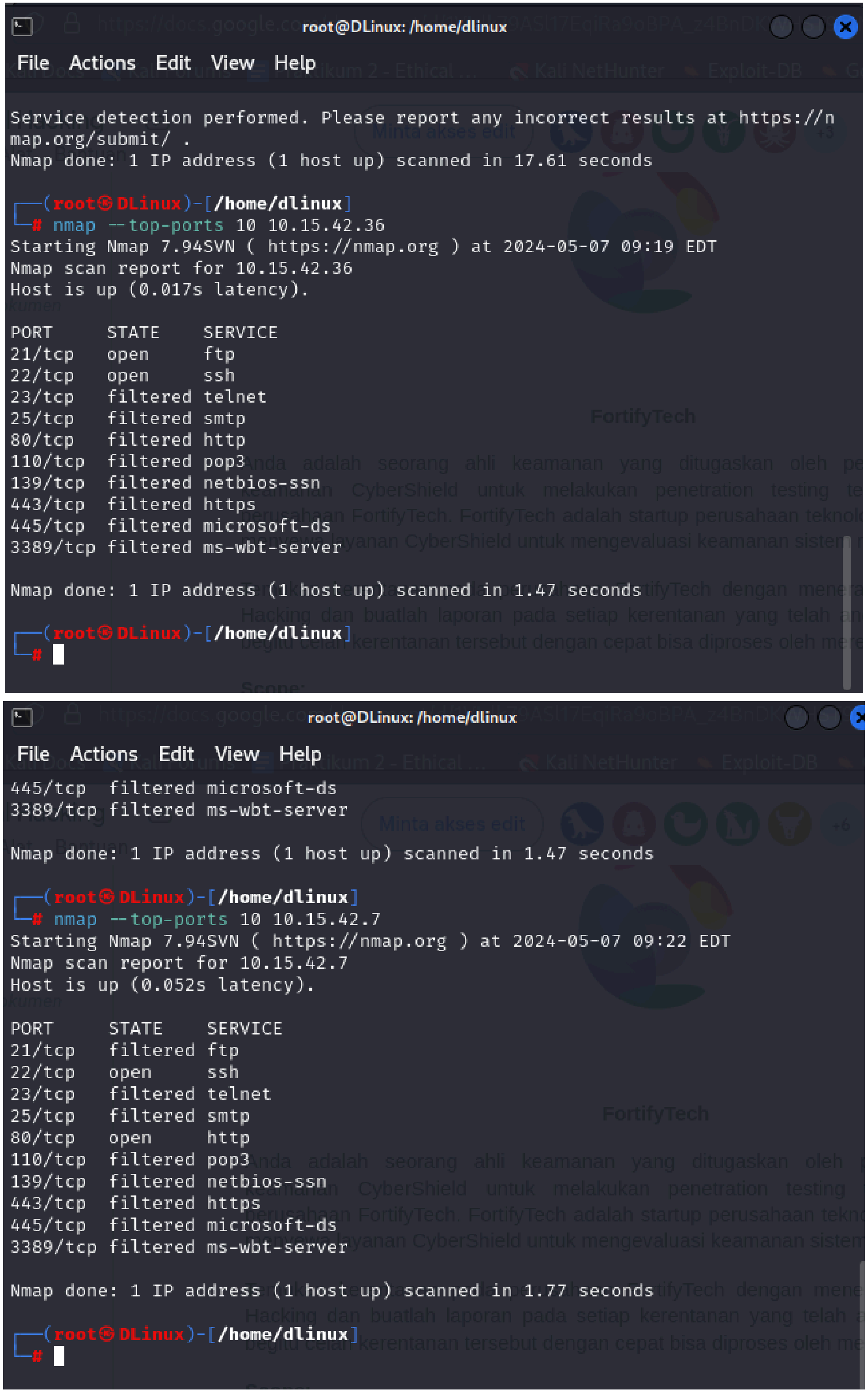
Evidence



```
┌──(dlinux㉿DLinux)-[~]
└─$ sudo su
[sudo] password for dlinux:
┌──(root㉿DLinux)-[/home/dlinux]
└─# nmap -sV 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 09:15 EDT
Nmap scan report for 10.15.42.7
Host is up (0.014s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol
2.0)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
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 14.26 seconds

┌──(root㉿DLinux)-[/home/dlinux]
└─# nmap -sV 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 09:15 EDT
Nmap scan report for 10.15.42.36
Host is up (0.013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
```



```
2.0)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
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 14.26 seconds

┌──(root㉿DLinux)-[/home/dlinux]
└─# nmap -sV 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 09:15 EDT
Nmap scan report for 10.15.42.36
Host is up (0.013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protoco
l 2.0)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
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 17.61 seconds

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



```
Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.61 seconds

┌──(root㉿DLinux)-[/home/dlinux]
└─# nmap --top-ports 10 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 09:19 EDT
Nmap scan report for 10.15.42.36
Host is up (0.017s latency).

PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   filtered http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  filtered https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds

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

```
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds

┌──(root㉿DLinux)-[/home/dlinux]
└─# nmap --top-ports 10 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 09:22 EDT
Nmap scan report for 10.15.42.7
Host is up (0.052s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   open     ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   open     http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  filtered https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.77 seconds

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

port open

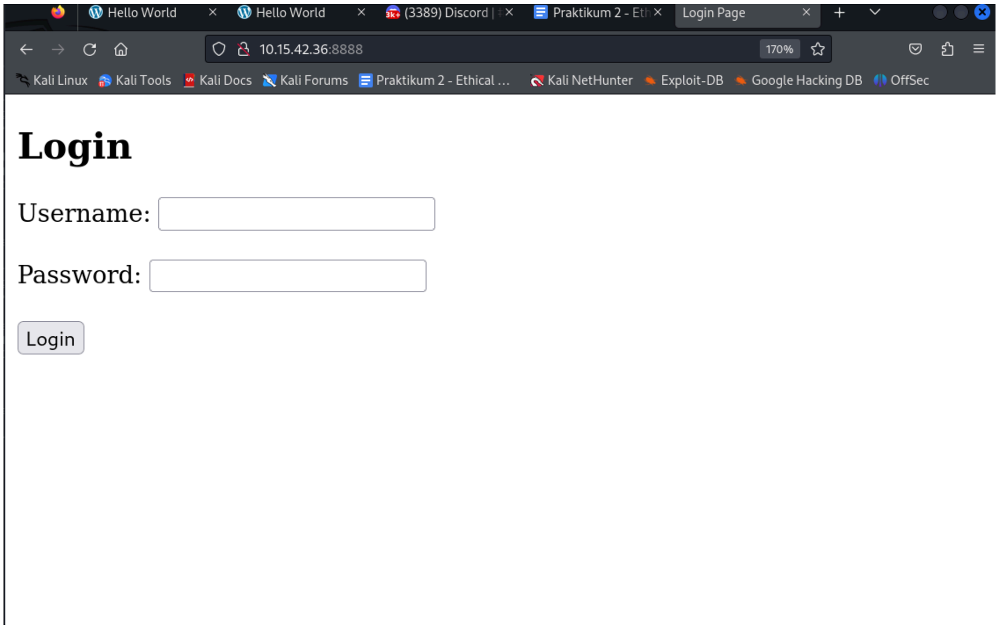
Remediation

- Identify the service running on the open port by conducting service enumeration.
- If the service is unnecessary or not in use, consider closing the port or disabling the service.
- Ensure that the service is properly configured with strong authentication mechanisms and access controls to prevent unauthorized access.
- Regularly monitor network traffic and conduct vulnerability assessments to detect and address any new open ports or services.

wp-user-enum:username Open Port

Description:	This alert specifically identifies an open port with the service name `wp-user-enum:username`. This likely indicates a WordPress user enumeration tool is running on the specified port.
Risk:	User enumeration tools can aid attackers in gathering information about valid usernames on a WordPress site, potentially facilitating brute-force attacks or targeted phishing campaigns.
System:	Systems with the open port and the WordPress user enumeration tool running.
Tools Used:	Nmap
References:	nmap application

Evidence

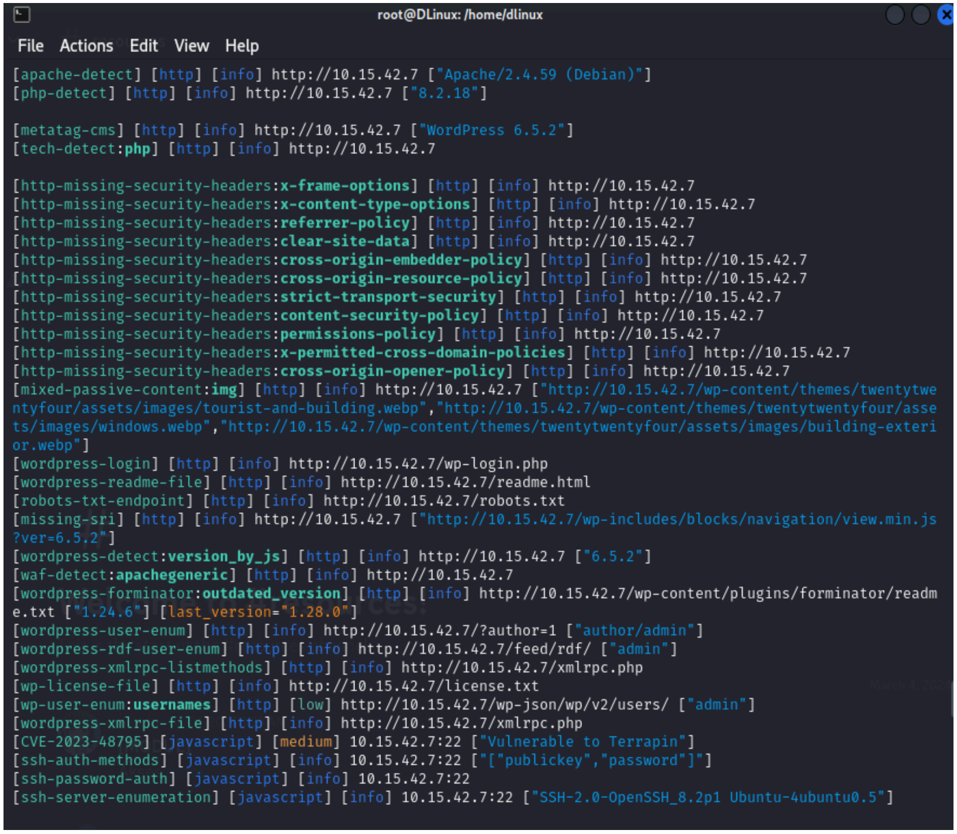


Login

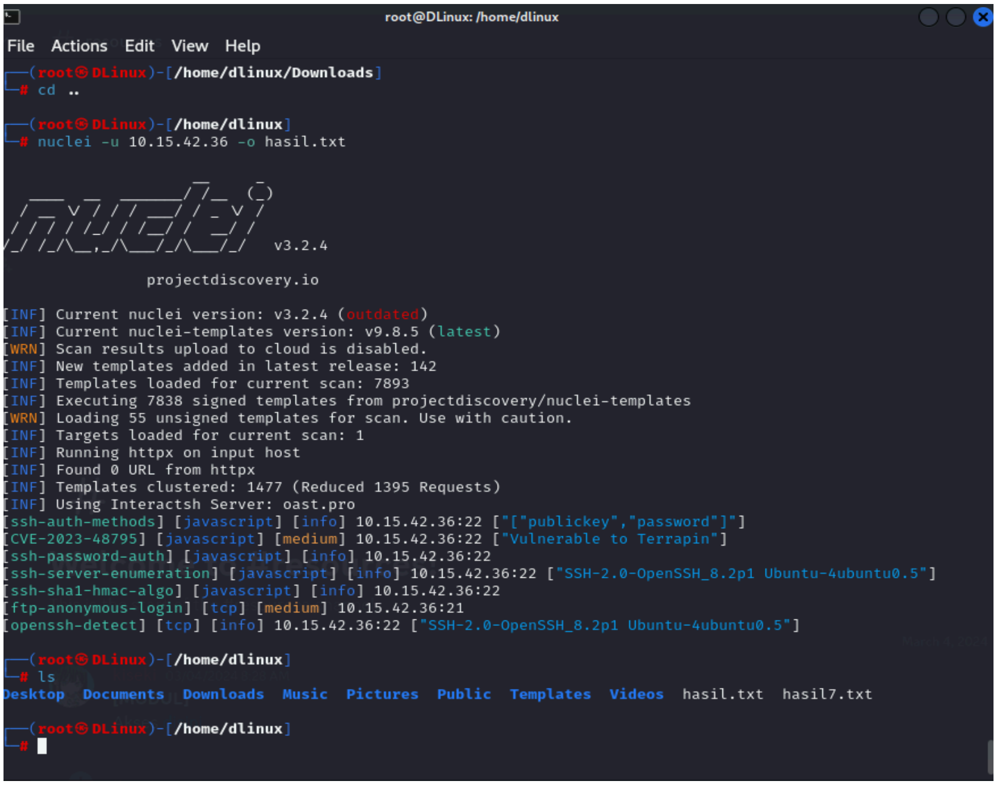
Username:

Password:

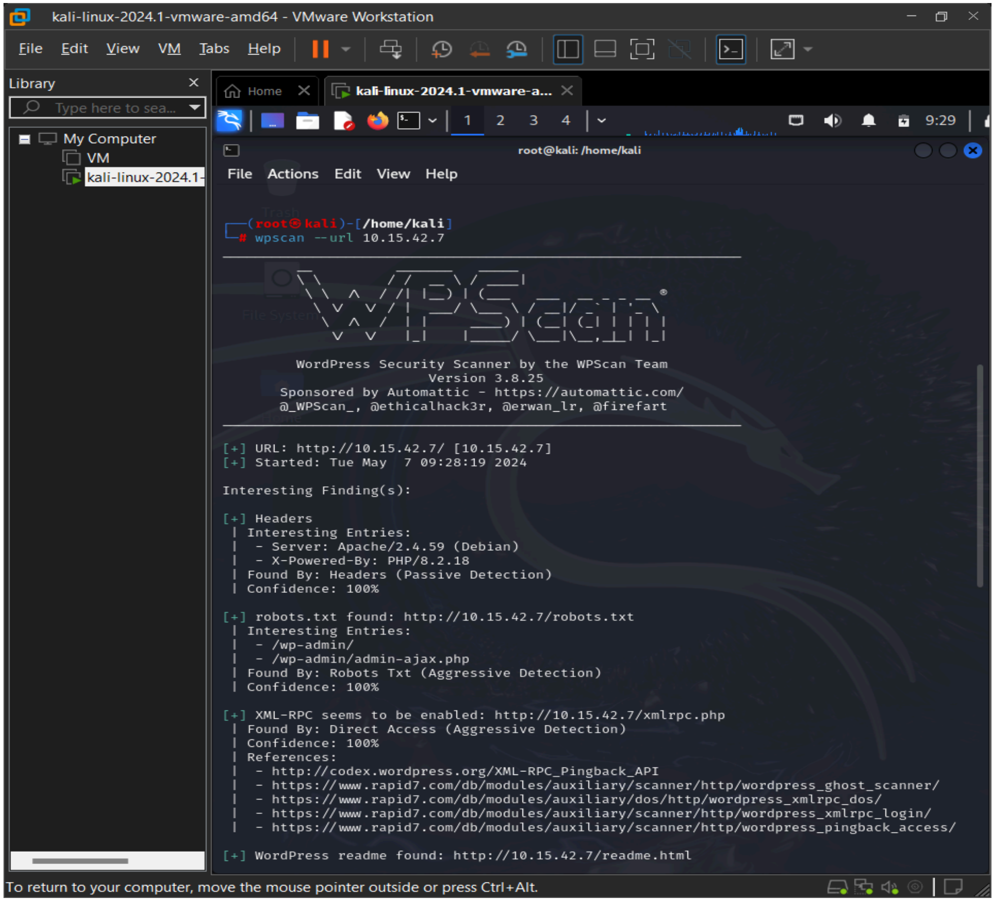
Login



```
[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: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
[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-resource-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
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-opener-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/twentytwe
ntyfour/assets/images/tourist-and-building.webp","http://10.15.42.7/wp-content/themes/twentytwentyfour/asse
ts/images/windows.webp","http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/building-exteri
or.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"]
[waf-detect:apachegeneric] [http] [info] http://10.15.42.7
[wordpress-forminator:outdated_version] [http] [info] http://10.15.42.7/wp-content/plugins/forminator/readm
e.txt ["1.24.6"] [last_version="1.28.0"]
[wordpress-user-enum] [http] [info] http://10.15.42.7/?author=1 ["author/admin"]
[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-license-file] [http] [info] http://10.15.42.7/license.txt
[wp-user-enum:usernames] [http] [low] http://10.15.42.7/wp-json/wp/v2/users/ ["admin"]
[wordpress-xmlrpc-file] [http] [info] http://10.15.42.7/xmlrpc.php
[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-server-enumeration] [javascript] [info] 10.15.42.7:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
```

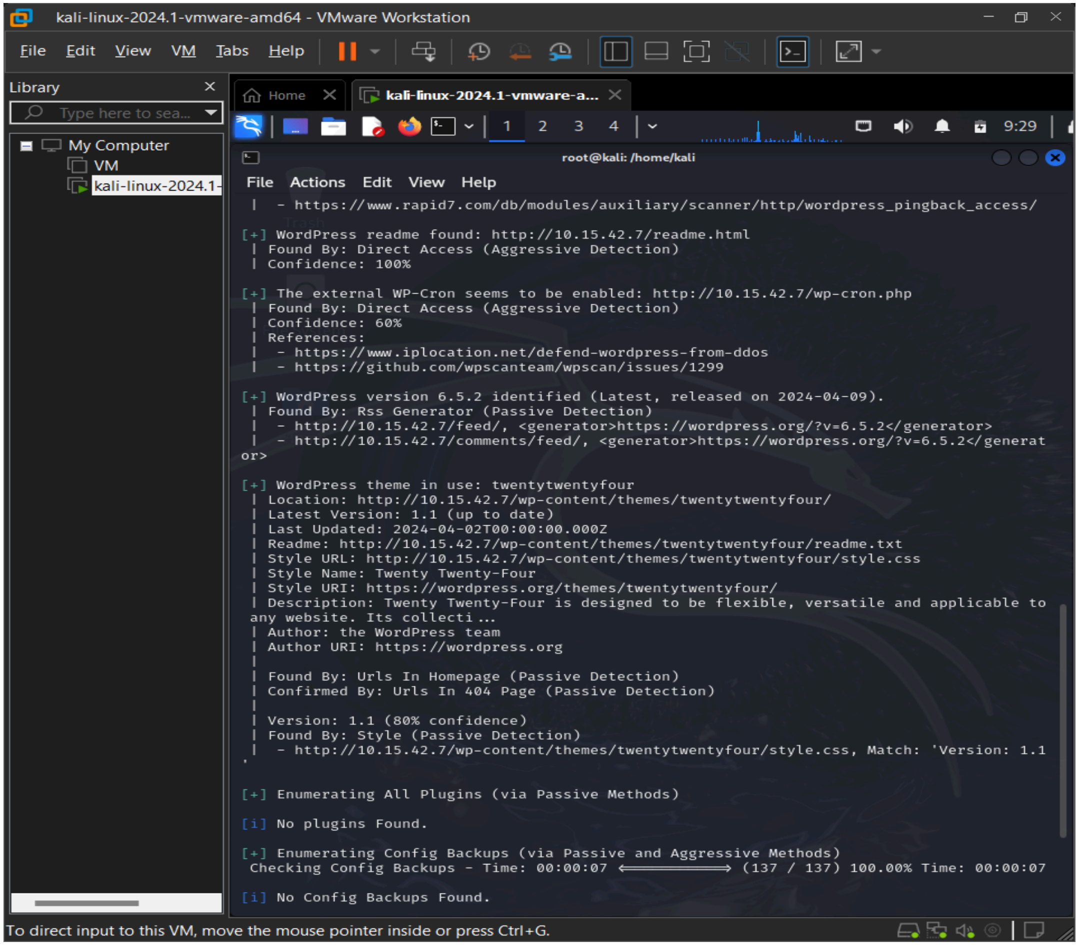


```
┌──(root㉿DLinux)-[/home/dlinux/Downloads]
└─# cd ..

┌──(root㉿DLinux)-[/home/dlinux]
└─# nuclei -u 10.15.42.36 -o hasil.txt

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   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)
[INF] Using Interactsh Server: oast.pro
[ssh-auth-methods] [javascript] [info] 10.15.42.36:22 ["["publickey","password"]"]
[CVE-2023-48795] [javascript] [medium] 10.15.42.36:22 ["Vulnerable to Terrapin"]
[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
[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㉿DLinux)-[/home/dlinux]
└─# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  hasil.txt  hasil7.txt

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


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
VM
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-a...
1 2 3 4
9:29
root@kali: /home/kali
File Actions Edit View Help

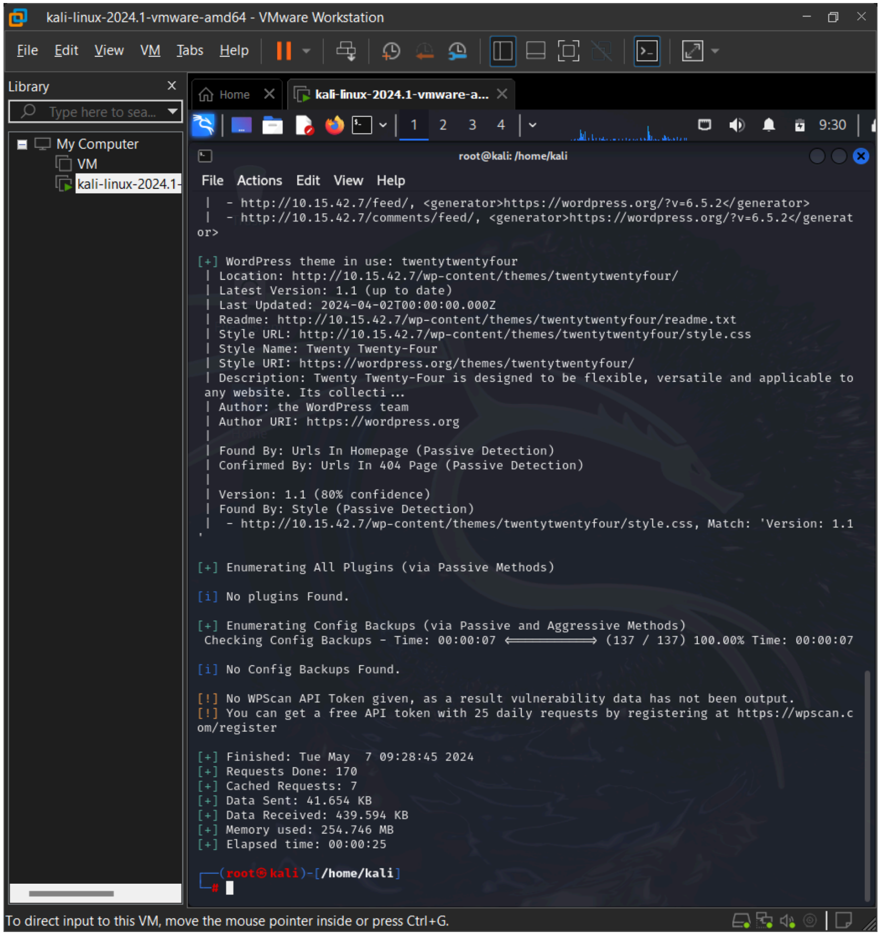
```
┌──(root㉿kali)-[/home/kali]
└─# wpscan --url 10.15.42.7
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.15.42.7/ [10.15.42.7]
[+] Started: Tue May  7 09:28:19 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.59 (Debian)
 |  - X-Powered-By: PHP/8.2.18
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.15.42.7/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.15.42.7/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://10.15.42.7/readme.html
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
VM
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-a...
1 2 3 4
9:29
root@kali: /home/kali
File Actions Edit View Help

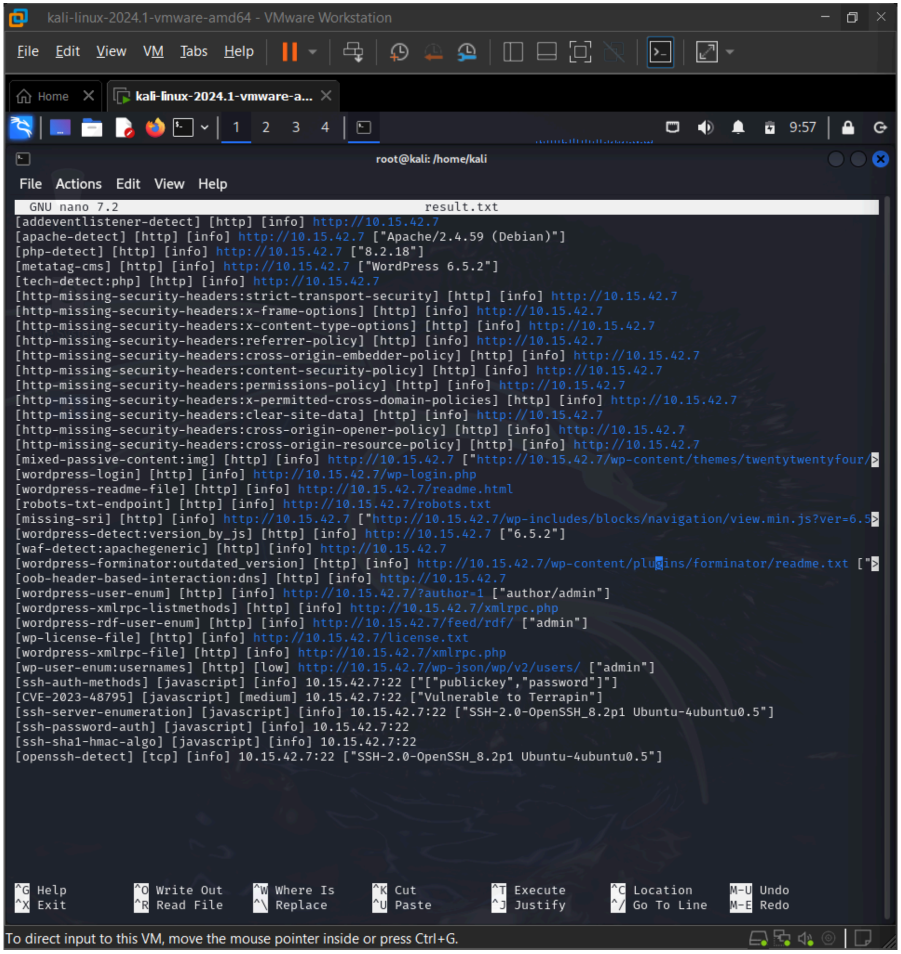
```
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://10.15.42.7/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.15.42.7/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.5.2 identified (Latest, released on 2024-04-09).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.15.42.7/feed/, <generator>https://wordpress.org/?v=6.5.2</generator>
 |  - http://10.15.42.7/comments/feed/, <generator>https://wordpress.org/?v=6.5.2</generat
or>

[+] WordPress theme in use: twentytwentyfour
 | Location: http://10.15.42.7/wp-content/themes/twentytwentyfour/
 | Latest Version: 1.1 (up to date)
 | Last Updated: 2024-04-02T00:00:00.000Z
 | Readme: http://10.15.42.7/wp-content/themes/twentytwentyfour/readme.txt
 | Style URL: http://10.15.42.7/wp-content/themes/twentytwentyfour/style.css
 | Style Name: Twenty Twenty-Four
 | Style URI: https://wordpress.org/themes/twentytwentyfour/
 | Description: Twenty Twenty-Four is designed to be flexible, versatile and applicable to
 any website. Its collecti ...
 | Author: the WordPress team
 | Author URI: https://wordpress.org
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.15.42.7/wp-content/themes/twentytwentyfour/style.css, Match: 'Version: 1.1
'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:07 <==========> (137 / 137) 100.00% Time: 00:00:07

[i] No Config Backups Found.
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
VM
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-a...
1 2 3 4
9:30
root@kali: /home/kali
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
 |  - http://10.15.42.7/feed/, <generator>https://wordpress.org/?v=6.5.2</generator>
 |  - http://10.15.42.7/comments/feed/, <generator>https://wordpress.org/?v=6.5.2</generat
or>

[+] WordPress theme in use: twentytwentyfour
 | Location: http://10.15.42.7/wp-content/themes/twentytwentyfour/
 | Latest Version: 1.1 (up to date)
 | Last Updated: 2024-04-02T00:00:00.000Z
 | Readme: http://10.15.42.7/wp-content/themes/twentytwentyfour/readme.txt
 | Style URL: http://10.15.42.7/wp-content/themes/twentytwentyfour/style.css
 | Style Name: Twenty Twenty-Four
 | Style URI: https://wordpress.org/themes/twentytwentyfour/
 | Description: Twenty Twenty-Four is designed to be flexible, versatile and applicable to
 any website. Its collecti ...
 | Author: the WordPress team
 | Author URI: https://wordpress.org
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.15.42.7/wp-content/themes/twentytwentyfour/style.css, Match: 'Version: 1.1
'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:07 <==========> (137 / 137) 100.00% Time: 00:00:07

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.c
om/register

[+] Finished: Tue May  7 09:28:45 2024
[+] Requests Done: 170
[+] Cached Requests: 7
[+] Data Sent: 41.654 KB
[+] Data Received: 439.594 KB
[+] Memory used: 254.746 MB
[+] Elapsed time: 00:00:25

┌──(root㉿kali)-[/home/kali]
└─# 
```



kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
1 2 3 4
9:57
root@kali: /home/kali
File Actions Edit View Help

```
  GNU nano 7.2                                     result.txt
[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-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
[http-missing-security-headers:cross-origin-embedder-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-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-opener-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-resource-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/>
[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>
[wordpress-detect:version_by_js] [http] [info] http://10.15.42.7 ["6.5.2"]
[waf-detect:apachegeneric] [http] [info] http://10.15.42.7
[wordpress-forminator:outdated_version] [http] [info] http://10.15.42.7/wp-content/plugins/forminator/readme.txt [">
[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
[wordpress-rdf-user-enum] [http] [info] http://10.15.42.7/feed/rdf/ ["admin"]
[wp-license-file] [http] [info] http://10.15.42.7/license.txt
[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"]
[ssh-auth-methods] [javascript] [info] 10.15.42.7:22 ["["publickey","password"]"]
[CVE-2023-48795] [javascript] [medium] 10.15.42.7:22 ["Vulnerable to Terrapin"]
[ssh-server-enumeration] [javascript] [info] 10.15.42.7:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
[ssh-password-auth] [javascript] [info] 10.15.42.7:22
[ssh-sha1-hmac-algo] [javascript] [info] 10.15.42.7:22
[openssh-detect] [tcp] [info] 10.15.42.7:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]




^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

login page username password

Remediation

- Identify the source of the WordPress user enumeration tool and determine if it is necessary for legitimate purposes.
- If the tool is unnecessary or poses a security risk, disable or remove it from the system.
- Implement security measures such as CAPTCHA, account lockout policies, or rate limiting to mitigate the risk of brute-force attacks.

- Regularly update and patch WordPress installations and plugins to address known vulnerabilities that could be exploited by attackers.

Additional Scans and Reports

TCMS provides all clients with all report information gathered during testing. This includes Nessus files and full vulnerability scans in detailed formats. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by TCM Security.

The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depth opportunities. For more information, please see the documents in your shared drive folder labeled “Additional Scans and Reports”.

TCM
SECURITY

Last Page