# 2024.11.28

## web

### [SWPUCTF 2021 新生赛]jicao

> 做题人:焦昱淇

> 题目url:https://www.nssctf.cn/problem/384

> 知识点:PHP 代码审计 RCE

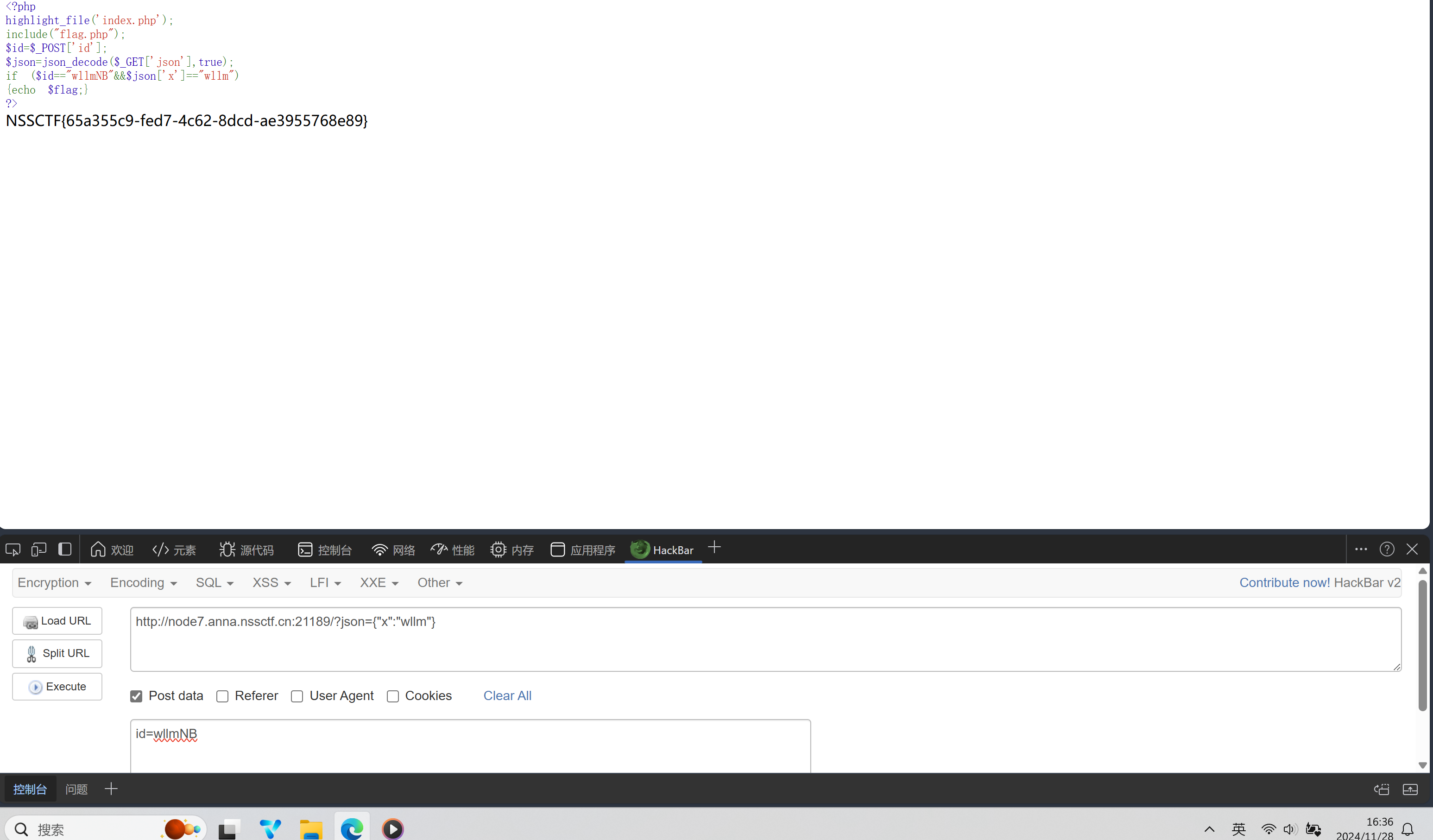
阅读源码了解到需要post值给id，get值给json，json\_decode()可以对一串JSON进行解码，故需要构造payload为 {"x":"wllm"}之后：

方法一：使用HackBar进行/?id=wllmNB,然后post json

方法二：使用burp直接修改请求头

方法三：python脚本

方法一：



Python

import requests

# 设置POST和GET参数

post\_data = {"id": "wllmNB"}

get\_data = {"json": '{"x":"wllm"}'}

# 发送请求到目标网址

response = requests.post("http://node1.anna.nssctf.cn:28678/", data=post\_data, params=get\_data)

# 打印响应内容

print(response.text)

## pwn

### [CISCN 2019华北]PWN1

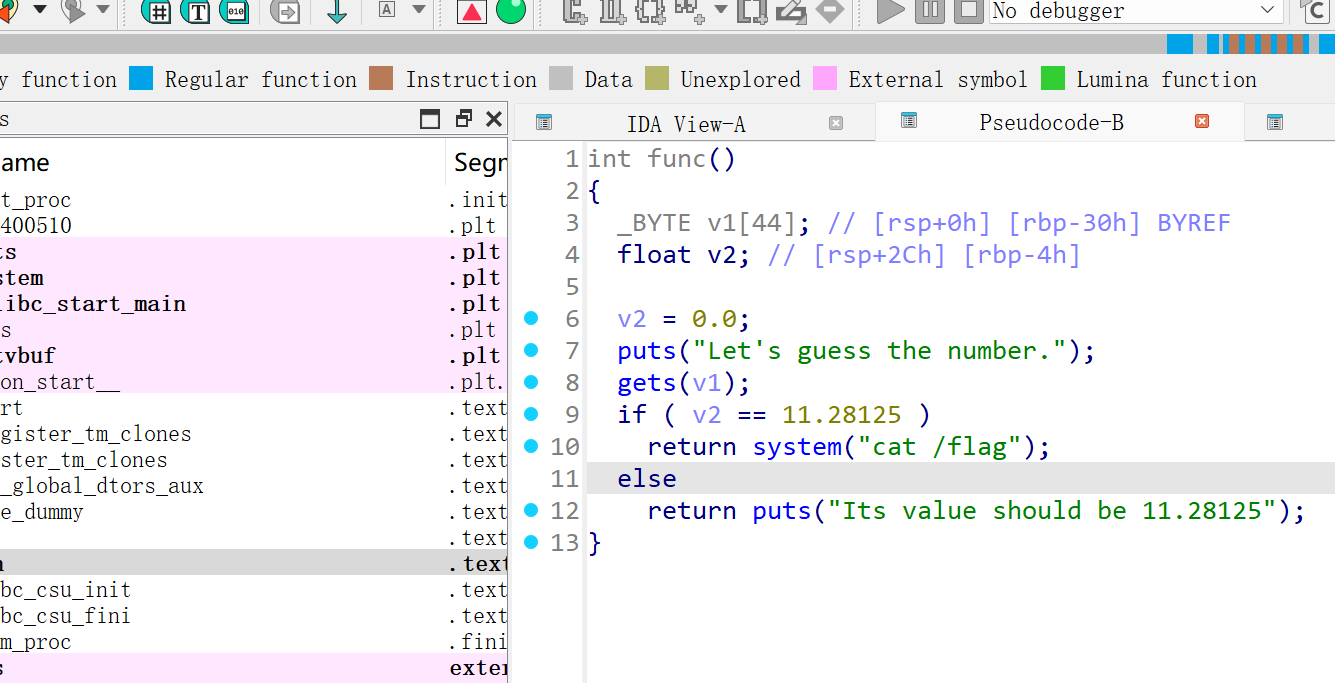
> 做题人:焦昱淇

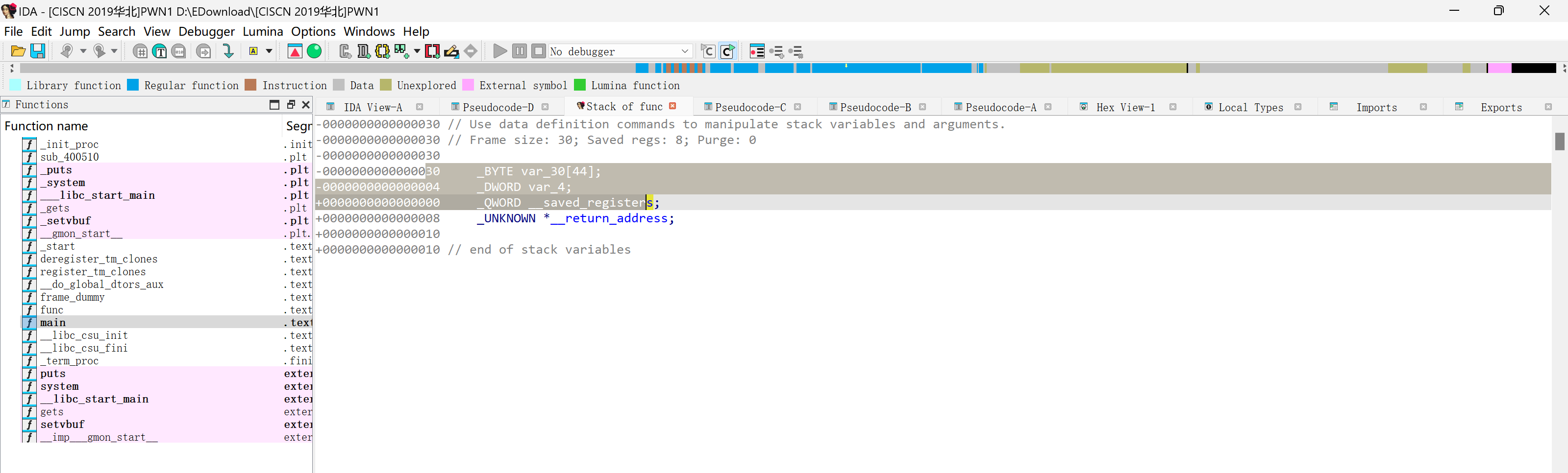
> 题目url:https://www.nssctf.cn/problem/100

> 知识点:整数溢出 覆盖 溢出

这边分析了一下程序，想要得到flag的话就要使v2=11.28125，只要使v2=11.28125那么程序就能cat flag。

但是这是pwn，你有cat flag，我想要就要了





V1 地址0x30

覆盖到cat flag就行

0x0000000004006BE

