1. xor

```
# xor.py
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]

user_input = input("Enter the flag: ")

for i in range(len(enc_str)):

    if enc_str[i] != chr(((user_input[i] ^ i) + 3 * i)):
        print("Wrong flag")
        exit()

print("Correct flag")
```

Xor로 암호화된 flag를 푸는 간단한 문제이다.

Xor은 같은 값으로 한번 더 연산하면 원래의 값이 나오기에 이를 이용하여 복호화 해준다.

복호화 코드

```
# xor.py
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]


for i in range(len(enc_str)):
    enc_str[i] -= 3*i
    enc_str[i] = enc_str[i] ^ i
    print(chr(enc_str[i]), end='')
```

IxC{xor_is_very_useful_for_encryption}

2. Path Traversal

링크로 이동하면 다음 문자열이 뜬다.

./next

misc.isangxcaution.xyz:33164/next

해당 위치로 이동해보자.

./When were the first CSE students admitted?

다시 경로와 경로에 대한 힌트가 나온다.

CSE학생들이 처음 입학한 년도 -> 1972

http://misc.isangxcaution.xyz:33164/next/1972

../What is the student council room number of IS Department?

참고로 ../ 는 이전 디렉토리로 이동한다.

IS학과 학생회실 룸 넘버 -> 508 (IS는 산업보안학과이다.)

http://misc.isangxcaution.xyz:33164/next/508

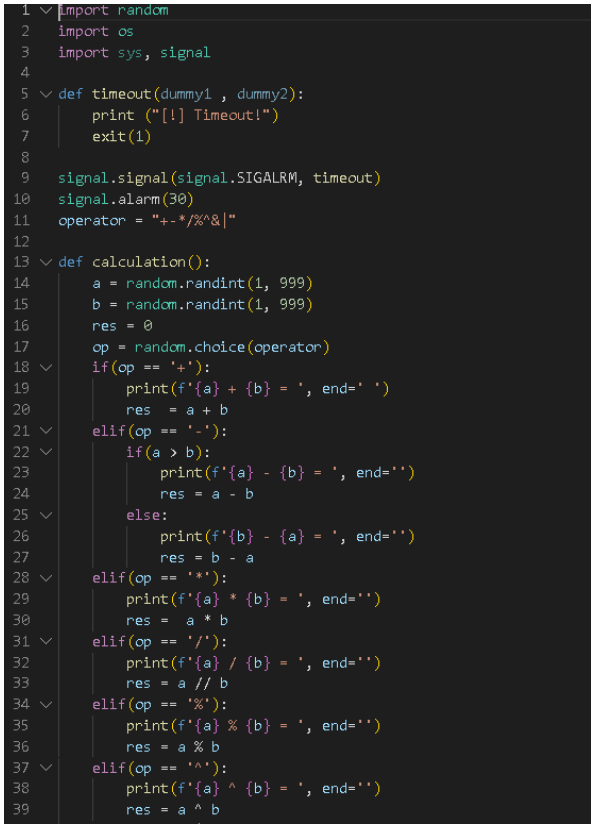
../../What is CAU's Pantone color?

Cau의 pantone color -> 2945C (blue)

Path Traversal (isangxcaution.xyz)

IxC{i_10ve_c4u}

3. homework



```python
import random
import os
import sys, signal

def timeout(dummy1 , dummy2):
    print ("[!] Timeout!")
    exit(1)

signal.signal(signal.SIGALRM, timeout)
signal.alarm(30)
operator = "+-*/%^&|"

def calculation():
    a = random.randint(1, 999)
    b = random.randint(1, 999)
    res = 0
    op = random.choice(operator)
    if(op == '+'):
        print(f'{a} + {b} = ', end=' ')
        res  = a + b
    elif(op == '-'):
        if(a > b):
            print(f'{a} - {b} = ', end='')
            res = a - b
        else:
            print(f'{b} - {a} = ', end='')
            res = b - a
    elif(op == '*'):
        print(f'{a} * {b} = ', end='')
        res =  a * b
    elif(op == '/'):
        print(f'{a} / {b} = ', end='')
        res = a // b
    elif(op == '%'):
        print(f'{a} % {b} = ', end='')
        res = a % b
    elif(op == '^'):
        print(f'{a} ^ {b} = ', end='')
        res = a ^ b
```

```
    elif(op == '%'):
        print(f'{a} % {b} = ', end='')
        res = a % b
    elif(op == '^'):
        print(f'{a} ^ {b} = ', end='')
        res = a ^ b
    elif(op == '|'):
        print(f'{a} | {b} = ', end='')
        res = a | b
    elif(op == '&'):
        print(f'{a} & {b} = ', end='')
        res = a & b
    return res

def main():
    cnt = 0
    for i in range(50):
        res = calculation()
        inp = int(input())
        if(res != inp):
            print("Nope!")
            exit(0)
        cnt+=1

    if(cnt == 50):
        print("Congraturations!")
        os.system("cat /flag")


if __name__ == '__main__':
    main()
```

연산자도 랜덤이고 피연산자도 랜덤인데 계산 결과 값을 맞춰야 한다.

하지만 실행 시에 계산해야할 식을 출력해 주므로 이를 읽고 eval로 계산하는 자동화 코드를 작성한다면 시간 안에 flag를 얻을 수 있다.

```
from pwn import *
p = remote("misc.isangxcaution.xyz", 33002)

for i in range(50):
    s = p.recvuntil(b'= ')
    s = s.decode('utf-8')
    s = s.replace('/', '//')
    print(s)
    s = s[0:s.find('=')]
    r = eval(s)
    sleep(0.2)
    p.sendline(str(r))

p.interactive()
```

```
574 | 216 =
715 * 558 =
102 ^ 832 =
733 | 853 =
891 + 276 =
 601 + 645 =
 187 & 317 =
835 | 672 =
818 + 808 =
 86 ^ 61 =
156 - 3 =
857 * 508 =
107 * 356 =
[*] Switching to interactive mode
Congraturations!
IxC{7h4nk_y0u_50_much!!}[*] Got EOF while reading in interactive
$
```

4. lucky number

```python
#!/usr/bin/env python 2.7

import os
import sys, signal
def timeout(dummy1 , dummy2):
    print "[!] Timeout!"
    exit(1)

signal.signal(signal.SIGALRM, timeout)
signal.alarm(30)
lucky_num = int(os.urandom(512).encode('hex'), 16)
print "Welcome And Happy New Year!!"
print "Select Your LUCKEY NUMBER!!: ",
select_number = input()

if(lucky_num == select_number):
    print "Congraturations!"
    os.system("cat /flag")

else:
    print "Hmm... Try again!!"


```

Random 함수로 나온 랜덤 값을 맞추면 되는 문제이고, 파이썬 2.7 버전이다.

random함수 자체에는 취약점이 없으나 python2에 한에서 input 함수는 eval(raw_input(prompt))로 실행된다는 취약점이 있다.

eval 함수는 문자열로 받은 것을 실행시켜 주기 때문에 입력에

__builtins__.__dict__['__import__']("os").system("cat flag")

을 주면 flag를 읽어오게 된다.

```
Welcome And Happy New Year!!
Select Your LUCKEY NUMBER!!:  __builtins__.__dict__['__import__']("os").system("cat flag")
IxC{py7h0n2_1npu7__15_vuln3r4bl3..}
Hmm... Try again!!
```

5. rockgame

```
    scanf("%d", &batMoney);
    if (batMoney > money | batMoney < 0)
    {
        printf("적절하지 않은 금액입니다.\n");
        continue;
    }
    do {
        if (playerValue) printf("올바른 값이 아닙니다\n");
        printf("가위바위보 게임을 시작합니다.\n");
        printf("가위 바위 보 중에 하나를 선택해주세요.(정수)\n");
        printf("[가위 : 0], [바위 : 1], [보 : 2]\n");
        scanf("%d", &playerValue);
    } while (playerValue != 0 && playerValue != 1 && playerValue != 2);
    comValue = batMoney % 3;
    if ((playerValue + 1) % 3 == comValue)
    {
        // comWin
        printf("저는 %s를 냈어요. 제가 이겼네요!!\n\n", valTran[comValue]);
        money -= batMoney;
        if (money <= 100)
        {
                        printf("당신! 돈 100원도 없다면서요!?\n");
            printf("다시 연습해와요~~~~~\n");
            return 0;
        }
    }
    else if ((comValue + 1) % 3 == playerValue)
    {
        // playerWin
        printf("저는 %s를 냈어요. 제가 졌네요...!!\n\n", valTran[comValue]);
        money += batMoney;
        if (money >= 10000)
        {
            printf("스승님! 저를 제자로 받아주세요ㅠㅠ\n");
            get_flag();

        }
    }
```

돈을 베팅하고 가위바위보를 해서 이기면 2배로 받는 게임이다.

comValue = batMoney % 3

컴퓨터가 내는 값은 베팅한 돈을 3으로 나눈 나머지이고,

(comValue + 1) % 3 == playerValue

컴퓨터 값에 1을 더한 후 3으로 나눈 값이 플레이어가 낸 값과 같으면 이긴다.

따라서 매 베팅마다 최대 값을 베팅하면서 플레이어가 낸 값이 저 조건을 만족하도록 하면 된다.

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

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

==========================
소유 금액 : 4000
배팅할 금액을 입력해주세요 : 4000
가위바위보 게임을 시작합니다.
가위 바위 보 중에 하나를 선택해주세요.(정수)
[가위 : 0], [바위 : 1], [보 : 2]
2
저는 바위를 냈어요. 제가 졌네요...!!

==========================
소유 금액 : 8000
배팅할 금액을 입력해주세요 : 8000
가위바위보 게임을 시작합니다.
가위 바위 보 중에 하나를 선택해주세요.(정수)
[가위 : 0], [바위 : 1], [보 : 2]
0
저는 보를 냈어요. 제가 졌네요...!!

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

6. rockgame2

코드도 없는 걸 보니 진짜 랜덤 값인 것 같다.

```
==========================
소유 금액 : 8000
배팅할 금액을 입력해주세요 : 8000
가위바위보 게임을 시작합니다.
가위 바위 보 중에 하나를 선택해주세요.(정수)
[가위 : 0], [바위 : 1], [보 : 2]
0
저는 보를 냈어요. 제가 졌네요...!!

스승님! 저를 제자로 받아주세요ㅠㅠ
IxC{Y0uaR_RandO0m_Mast2r}
```

7. rockgame3

```
int computerAI(int playerValue)
{
    switch (playerValue)
    {
    case 0:
        return 1;
        break;
    case 1:
        return 2;
        break;
    case 2:
        return 0;
        break;
    default:
        return 0;
        break;
    }
}
```

```
if ((playerValue + 1) % 3 == comValue)
{
    // comWin
    printf("저는 %s를 냈어요. 제가 이겼네요!!\n\n", valTran[comValue]);
    if (money <= 100)
    {
        printf("당신! 돈 100원도 없다면서요!?\n");
        printf("다시 연습해와요~~~~~\n");
        return 0;
    }
}
else if ((comValue + 1) % 3 == playerValue)
{
    // playerWin
    printf("저는 %s를 냈어요. 제가 졌네요...!!\n\n", valTran[comValue]);
    goto ddd;
    money += 2 * batMoney;
}
else
{
    printf("무승부에요!!! 기본 금액만 지급됩니다!\n");
    goto ddd;
}


while (NULL)
{
    if (0)
    {
        ddd:
        money += 100;
    }
}
```

0~2사이의 값을 쓰면 무조건 플레이어가 진다.

3이상의 값을 쓰면 컴퓨터는 무조건 0을 내고 만약 (playerValue + 1) % 3 == comValue,

(comValue + 1) % 3 == playerValue 이 두 조건 모두 피해가면 무승부로 기본 금액 100원이 지급된다.

```c
int inputMoney(void)
{
    printf("========================\n");
    printf("소유 금액 : %d\n", money);
    printf("배팅할 금액을 입력해주세요 : ");
    scanf("%d", &batMoney);
    if (batMoney > money)
    {
        printf("가지고 있는 금액보다 큰 금액입니다.\n");
        return inputMoney();
    }
    else if(batMoney >= 99 == 0)
    {
        printf("100원 이상을 배팅해야합니다.\n");
        return inputMoney();
    }
    return batMoney;


}
```

최소 배팅 금액이 있는데, 100원 이상이 아니라 99원 이상이기 때문에 99원을 배팅하고 무승부로 만들 때마다 1원씩 이득 볼 수 있다.

comValue는 0이기 때문에 하나의 예시로 플레이어가 4를 내면 두 조건을 피하고 무승부로 이득을 본다.

자동화 코드로 공격을 해주자.

```python
import sys

sys.stdin.encoding # 'UTF-8'

from pwn import *
p = remote("misc.isangxcaution.xyz", 33171)
#context.log_level = "debug"


for i in range(49):
    a = p.recvuntil("배팅할 금액을 입력해주세요 : ")
    #print(str(a))
    p.sendline(b"99")
    b = p.recvuntil(b"]\n")
    #print(str(b))
    p.sendline(b"4")


p.interactive()
```

```
소유 금액 : 1049
배팅할 금액을 입력 99
가위바위보 게임
가위 바위 보 중에 하나를 선택해주세요.(정수)
[가위 : 0], [바위 : 1], [보 : 2]
$ 4
무승부에요!!! 기본 금
스승님! 저를 제자로 받아주세요ㅠㅠ
IxC{Y0uaR_R0c2G1me_Mast2r}
```

8. 무대를 뒤집어 놓으셨다.

Mp4 파일이 제공된다.

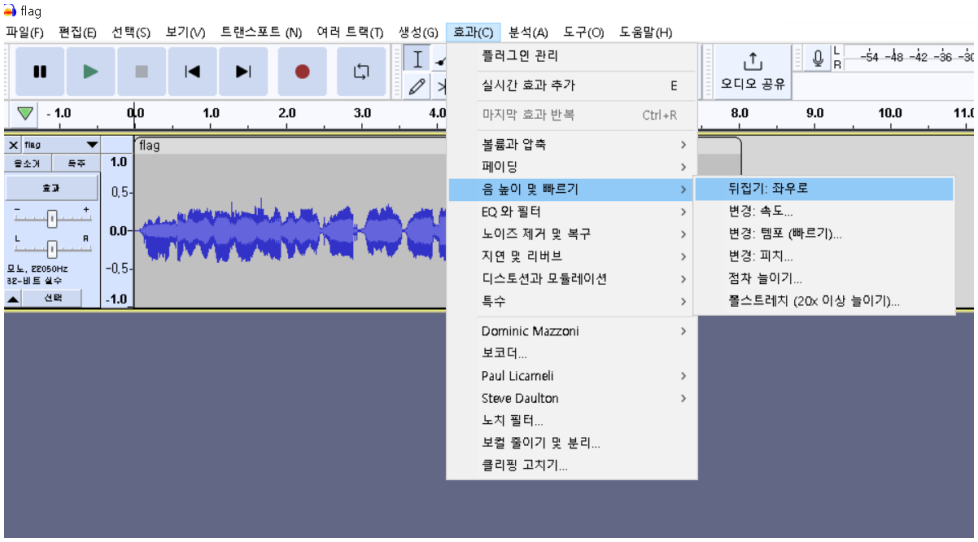
```
001B84B0  2A 0D C1 3B 99 A5 02 F6 F3 68 E9 67 48 90 3A 21  *.Á;™¥.öóhégH.:!
001B84C0  58 17 34 C9 7E 97 FF EA 20 FB 7C 35 60 F1 7C 3C  X.4É~—ÿê û|5`ñ|<
001B84D0  8E 6C 00 00 00 01 90 00 50 B8 C9 84 0E 52 49 46  Žl......P¸É„.RIF
001B84E0  46 10 6B 05 00 57 41 56 45 66 6D 74 20 10 00 00  F.k..WAVEfmt ...
001B84F0  00 01 00 01 00 22 56 00 00 44 AC 00 00 02 00 10  .....″V..D¬.....
001B8500  00 64 61 74 61 EC 6A 05 00 00 00 00 00 00 00 00  .dataìj.........
001B8510  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

HxD로 분석하면 wav파일의 시그니처가 보인다.

추출해서 다운 받아보자.

이상한 음성이 들린다.

원본을 역재생한 것 같으니 Audacity를 써서 역재생 해주면 flag를 읽어준다.



IxC{rev3rse__r3ver5e_zzz_}