

ROOTCTF

- 참가 닉네임 : UI
- 12등...

MISC

Welcome - 50점

- FLAG : FLAG{Welcome_to_Seoul_Digitech_ROOT_CTF}

Calculate - 167점

- 어떤 python파일을 준다.
문자열을 입력받으면 4개의 함수를 거쳐서 숫자로 암호화되고 그 결과가 **result**리스트의 값과 같으면 “Correct” 를 띄우고 아니면 “Incorrect” 를 띄운다.
모든 문자들을 암호화시킨 다음에 **result**리스트와 순서대로 비교하여 플래그를 찾아내었다.

```
# 위에 있는 암호화함수 생략
if __name__ == "__main__":
    result = [5040, 4944, 5088, 4992, 7232, 4848, 7584, 7344, 4288, 7408, 7360, 7584, 4608, 4880, 4320, 7328, 7360,
              4608, 4896, 4320, 7472, 7328, 7360, 4608, 4752, 4368, 4848, 4608, 4848, 4368, 4944, 7200]

    string = "`1234567890-=qwertyuiop[]\';lkjhgfdsazxcvbnm,./~!@#$$%^&*()_+}{POIUYTREWQASDFGHJKL:\"\'?><MNBVCXZ"
    Number = []
    tmp = 0
    answer = ""

    for i in string:
        Number.append(ord(i))

    for i in Number:
        Number[tmp] = one(i, 100)
        tmp += 1
    tmp = 0
    for i in Number:
        Number[tmp] = two(i, 100)
        tmp += 1
    tmp = 0
    for i in Number:
        Number[tmp] = three(i, 100)
        tmp += 1
    tmp = 0
    for i in Number:
        Number[tmp] = four(i, 100)
        tmp += 1

    print(Number)
    for i in result:
        cnt=0
        for j in Number:
            if i == j:
                answer+=string[cnt]
                cnt=cnt+1
        print()
    print(answer)
```

- FLAG : FLAG{Rev3rse_P1us_M1nus_X0R_R0L}

Vocabulary - 460점

- PNG이미지 파일을 하나 준다.

처음에 많이 해했다. hint로 PNG height가 나온 것을 보고 금방 알 수 있었다.

바로 PNG hex format을 검색하여 높이를 담당하는 hex값을 변경했다.

	pleas_find_원본.png	pleas_find_답.png
Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....
00000010	00 00 02 BC 00 00 02 EE 08 06 00 00 00 9B A5 91 ...¼...i...	00 00 02 BC 00 00 10 EE 08 06 00 00 00 9B A5 91 ...¼...i...
00000020	32 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 2....sRGB.®	32 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 2....sRGB.
00000030	00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 ..gAMA..±..	00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 ..gAMA..±..
00000040	00 09 70 48 59 73 00 00 0E C2 00 00 0E C2 01 15 ..pHYs...Â.	00 09 70 48 59 73 00 00 0E C2 00 00 0E C2 01 15 ..pHYs...Â.
00000050	28 4A 80 00 00 93 A5 49 44 41 54 78 5E EC DD 4F (J€..."#IDAT	28 4A 80 00 00 93 A5 49 44 41 54 78 5E EC DD 4F (J€..."#IDAT
00000060	4C 5B 77 BE FF FF 57 7E 8B 96 2E A6 A2 D2 AD 4C L[w³ÿÿW~<-.	4C 5B 77 BE FF FF 57 7E 8B 96 2E A6 A2 D2 AD 4C L[w³ÿÿW~<-.
00000070	34 95 70 DB 45 48 37 90 CD E0 2C 6E 70 A5 9B 81 4•pÛEH7.Íà,	34 95 70 DB 45 48 37 90 CD E0 2C 6E 70 A5 9B 81 4•pÛEH7.Íà,
00000080	AA BD C2 BD AD 84 E9 2C 70 BE 1B 98 CD E0 2C A6 ºÂ¸.„é,p³.	AA BD C2 BD AD 84 E9 2C 70 BE 1B 98 CD E0 2C A6 ºÂ¸.„é,p³.
00000090	10 69 2A 45 EA 48 38 ED 02 E7 6E 42 36 17 67 31 .i*EêH8í.çn	10 69 2A 45 EA 48 38 ED 02 E7 6E 42 36 17 67 31 .i*EêH8í.çn
000000A0	B5 23 B5 DF 38 9A 8E E2 B4 57 C2 E4 2E 30 77 03 µ#µß8šŽâ'WÂ	B5 23 B5 DF 38 9A 8E E2 B4 57 C2 E4 2E 30 77 03 µ#µß8šŽâ'WÂ
000000B0	D9 14 66 D1 E2 4A 1D 61 D4 AF 04 EA 2C A0 DD 9C Û.fÑâJ.aÔ~.	D9 14 66 D1 E2 4A 1D 61 D4 AF 04 EA 2C A0 DD 9C Û.fÑâJ.aÔ~.
000000C0	DF 31 1C 12 1F 63 EC 63 63 08 7C 78 3E D4 B7 7A ß1...cìcc.	DF 31 1C 12 1F 63 EC 63 63 08 7C 78 3E D4 B7 7A ß1...cìcc.
000000D0	6C 7C 7C 8E FF E4 F8 E5 8F 3F E7 F3 39 23 C9 B2 l žÿäöâ.?ç	6C 7C 7C 8E FF E4 F8 E5 8F 3F E7 F3 39 23 C9 B2 l žÿäöâ.?ç

	pleas_find_원본.png	pleas_find_답.png
Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....
00000010	00 00 02 BC 00 00 02 EE 08 06 00 00 00 9B A5 91 ...¼...i...	00 00 02 BC 00 00 10 EE 08 06 00 00 00 9B A5 91 ...¼...i...
00000020	32 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 2....sRGB.	32 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 2....sRGB.
00000030	00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 ..gAMA..±..	00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 ..gAMA..±..
00000040	00 09 70 48 59 73 00 00 0E C2 00 00 0E C2 01 15 ..pHYs...Â.	00 09 70 48 59 73 00 00 0E C2 00 00 0E C2 01 15 ..pHYs...Â.
00000050	28 4A 80 00 00 93 A5 49 44 41 54 78 5E EC DD 4F (J€..."#IDA	28 4A 80 00 00 93 A5 49 44 41 54 78 5E EC DD 4F (J€..."#IDA
00000060	4C 5B 77 BE FF FF 57 7E 8B 96 2E A6 A2 D2 AD 4C L[w³ÿÿW~<-.	4C 5B 77 BE FF FF 57 7E 8B 96 2E A6 A2 D2 AD 4C L[w³ÿÿW~<-.
00000070	34 95 70 DB 45 48 37 90 CD E0 2C 6E 70 A5 9B 81 4•pÛEH7.Íà	34 95 70 DB 45 48 37 90 CD E0 2C 6E 70 A5 9B 81 4•pÛEH7.Íà
00000080	AA BD C2 BD AD 84 E9 2C 70 BE 1B 98 CD E0 2C A6 ºÂ¸.„é,p³.	AA BD C2 BD AD 84 E9 2C 70 BE 1B 98 CD E0 2C A6 ºÂ¸.„é,p³.
00000090	10 69 2A 45 EA 48 38 ED 02 E7 6E 42 36 17 67 31 .i*EêH8í.ç	10 69 2A 45 EA 48 38 ED 02 E7 6E 42 36 17 67 31 .i*EêH8í.ç
000000A0	B5 23 B5 DF 38 9A 8E E2 B4 57 C2 E4 2E 30 77 03 µ#µß8šŽâ'W	B5 23 B5 DF 38 9A 8E E2 B4 57 C2 E4 2E 30 77 03 µ#µß8šŽâ'W

- 답
- FLAG : FLAG{_1vErticAl_2rEADiNg_3TAStISb}
- 도움받은 링크 : [Link](#)

Do you know □ □ □ ? - 706점

Find the Flag!

[0 = 4dog] [2 = 1dog] [4 = 4dog] [5 = 4dog]

[6 = 1dog] [7 = 1dog] [8 = 2dog] [9 = 3dog]

[a = 4dog] [b = 3dog] [c = 3dog] [d = 2dog]

- 처음 나왔을 때 hint가 cat=고양이라 했으니까 설마 dog는 개, 갓수를 뜻하는 거겠어 하며 의아해 하면서 해석했다.

[0 = 4개] [2 = 1개] [4 = 4개] [5 = 4개] [6 = 1개] [7 = 1개] [8 = 2개] [9 = 3개] [a = 4개] [b = 3개] [c = 3개] [d = 2개]

- 위의 문자들의 갓수를 맞춘 것은

b 0 2 5 5 4 4 c

c 0 7 9 8 5 4 4

0 d a c 0 b a a

9 d b 8 a 5 9 6

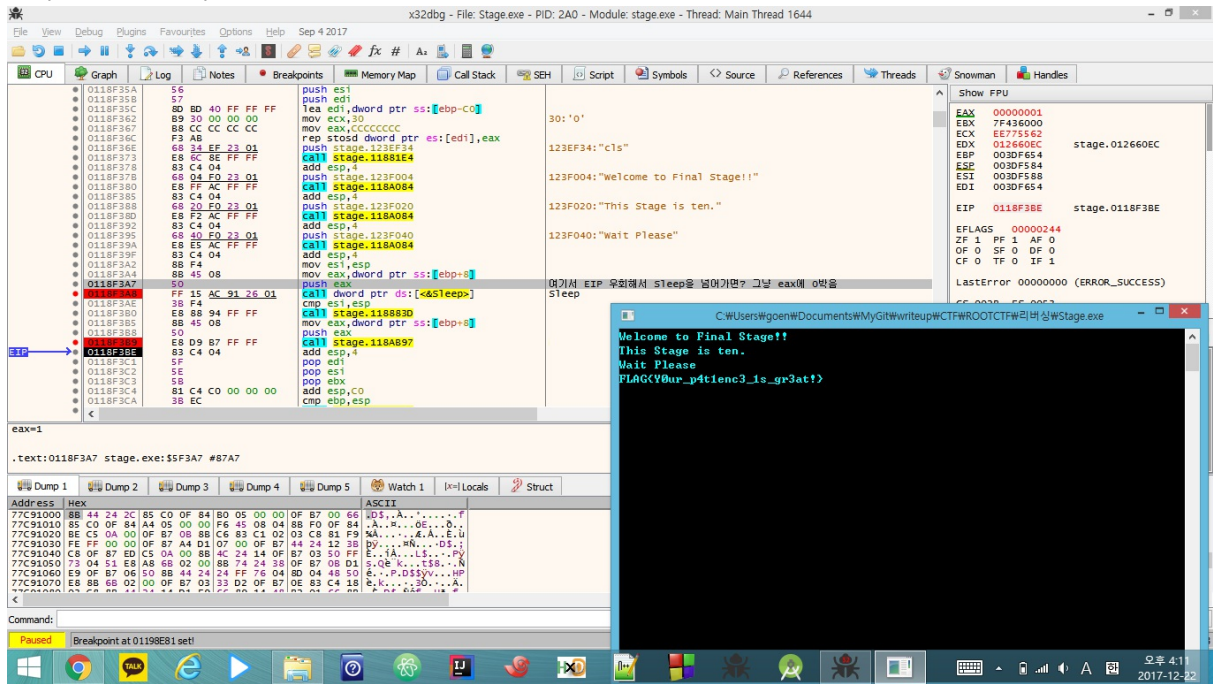
- 공백들을 없애고 <http://md5decryption.com/>에서 MD5 Decryption 돌리면 플래그가 나온다.
- FLAG : FLAG{MD5_3nCryPt_Ye@h}

REVERSING

리버스공학부한자 조금밖에 안 돼서 풀었다고 좋아했는데 누구나 다푸는 문제였어,

Stage Game - 229점

- 바이너리를 실행하면 입력창이 나오고 1을 입력하면 게임이 시작된다.
- sleep함수에 인자를 push eax로 전달하는 것 같은데 eax값을 0로 전달하고 실행시키다보면 플래그를 출력한다.



WEBHACKING

Login - 50점

```
<?php
include("dbcon.php");
$pw=$_GET['pw'];
$fwp=$_GET['pw'][1];
if(strlen($fwp)>5){
    echo "<script>alert('no hack~');location.href='login.html'</script>";
}
$query="select * from Login where pw='$fwp'";
$info=mysqli_query($con,$query);
$result=mysqli_fetch_array($info);
if($result['id']){
    setcookie("flag", "VmxeE1FNudSbk5UV0hCcIUwVmFmWxzVm1GTlZtUnhVbFJXYVZKdGVGcFdSM0JYWwxaV1ZVMUVhejA9");
    echo "<script>location.href='flag.html'</script>";
}
highlight_file("login.php");
?>
```

- \$_GET['pw'][1]의 길이가 5 이하가 되어야 하므로 false sql injection을 이용해서 길이를 줄여서 풀면 된다.
- 배열로 값을 전달하는 방법은 파라미터 바로 뒤에 대괄호를 붙여주면 된다.
- SQL에서 원하는 데이터가 있으면 'flag'쿠키의 값을 "VmxeE1FNudSbk5UV0hCcIUwVmFmWxzVm1GTlZtUnhVbFJXYVZKdGVGcFdSM0JYWwxaV1ZVMUVhejA9"로 설정해준다. 이 문자열을 base64로 디코딩하다보면 플래그가 나온다.
- payload : [http://sdhsroot.kro.kr/Login/login.php?pw\[1\]=1%27^1%23](http://sdhsroot.kro.kr/Login/login.php?pw[1]=1%27^1%23)
- FLAG : FLAG{jjang_easy}

SQL로 풀 필요 없이 그냥 지나온 문자열 base64로 디코딩

보물찾기 - 149점

- 홈페이지내부에서 플래그를 찾아오라했다.
- <http://sdhsroot.kro.kr/vendor/bootstrap/css/bootstrap.min.css>
위에가면 있다.
- FLAG : FLAG{bootstrap_1s_jj4ng}

SPACE PROSPECTION - 529점

- 2023년... SPACE PROSPECTION라는 회사가 화성에 진출했다. 회사의 사이트에 들어가 핵심 기술을 가져오자!! 라고 문제설명이 되었다.
- <http://sdhsroot.kro.kr/BlackOut/about.html>
여기에 들어가면 온통 영어로 써져있다.
- 이곳저곳 탐방하다 보면 <http://sdhsroot.kro.kr/BlackOut/singlepost.html>
이곳에 들어가면 수상하게도 한글로

지금은 2023년... 우리의 핵심기술을 잃어버렸다.

아주아주 오래전... 이 파일 안에는 우리의 핵심기술이 담겨있었습니다.

하지만 페이지 디자인 작업중 정전이 나버렸고, 이곳에 담겨있던 핵심기술은 날아가 버렸습니다.

지금도 이 서버 어딘가에 핵심기술이 담겨있는 파일이 돌아다닐 수 있습니다.

써져있다. vi로 작업하면 swp형식으로 백업파일이 생성된다.

- <http://sdhsroot.kro.kr/BlackOut/.singlepost.html.swp> 로 들어가면 FLAG가 있다.
숨김파일은 파일명에 .이 붙는다.
- FLAG : FLAG{FROM_2017_FLAG}

Phishing - 600점

- 접속하면 페이지에 주석으로 asd.php 가 써있고 접속하면 flag는 코드속에 있다고 한다.
- <http://jsbeautifier.org>에서 Detect packers and obfuscators? 옵션을 키고 돌리면 복호화된 코드가 나온다.

```
var b = 200;
for (a = 0; a <= 20; a++) {
  b = b + ((a * b) - (a / b));
  if (a == 0) b = 70;
  else if (a == 1) b = 76;
  else if (a == 3) b = 71;
  else if (a == 2) b = 65;
  else if (a == 4) b = 123;
  else if (a == 20) b = 125;
  else if (a == 5) {
    continue
  } else if (a == 6) {
    alert("코");
    continue
  } else if (a == 7) {
    alert("드");
    continue
  } else if (a == 8) {
    alert("속");
    continue
  } else if (a == 9) {
    alert("에");
    continue
  } else if (a == 10) {
    alert(".");
    continue
  } else if (a == 11) {
```





```
    alert(".");
    continue
} else if (a == 12) {
    alert(".");
    continue
} else if (a >= 4 && a <= 20) {
    continue
}
alert(String.fromCharCode(b))
}
```

여기서 코드를 조금 수정하면 웹페이지에 플래그를 출력하게 할 수 있다.

```
var b=200;
for(a=0;a<=20;a++){
    b=b*((a*b)-(a/b));
    if(a==0)b=70;
    else if(a==1)b=76;
    else if(a==2)b=65;
    else if(a==3)b=71;
    else if(a==4)b=123;
    else if(a==20)b=125;

    document.write(String.fromCharCode(b));

}
```

- FLAG : FLAG{갯벨넉넉눗복}
- FLAG{갯벨넉넉눗복}
- 옵션을 키더라도 <script>태그가 들어가있으면 제대로 작동하지 않는다.