

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

rot13.com

[About ROT13](#)

LP_MMDQJ_KDFN



ROT23 ▼



IM_JJANG_HACK

3. Mata Hari

제공되는 악보의 음표에 맞게 알파벳을 적어준다.

FMCJMXZ YQCRPYVI U SZ # HA ? YM



Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type scrabble

Results

↑↓	↑↓
↗+0	FLAGISTRITHEMIUFCIPHER
↘+2	HPGOSEHHANDCMKYLKSBVUJ
↗+11	QWLRTDECTESPXTFQNTASPC
↘+6	LTKSWILLERHGQOCPOWFZYN
↗+8	NTIOQABZQBPMUCNKQXPMZ
↗+14	TZOUWGHFWHVS AWITQWDVSF
↘+21	AIZHLXAATGWVFDREDLUONC
↘+4	JRIQUGJJCPFEOMANMUDXLW

TRITHEMIUS CIPHER

Cryptography > Trithemius Cipher

Sponsored ads

Trithemius Decoder

★ TRITHEMIUS CIPHERTEXT

FMCJMXZYQCRPY
VIUSZHAYM

★ ALPHABET

★ EVOLUTION OF THE SHIFT

☐ INITIAL SHIFT +

☒ TRY ALL SHIFTS (BRUTEFORCE)

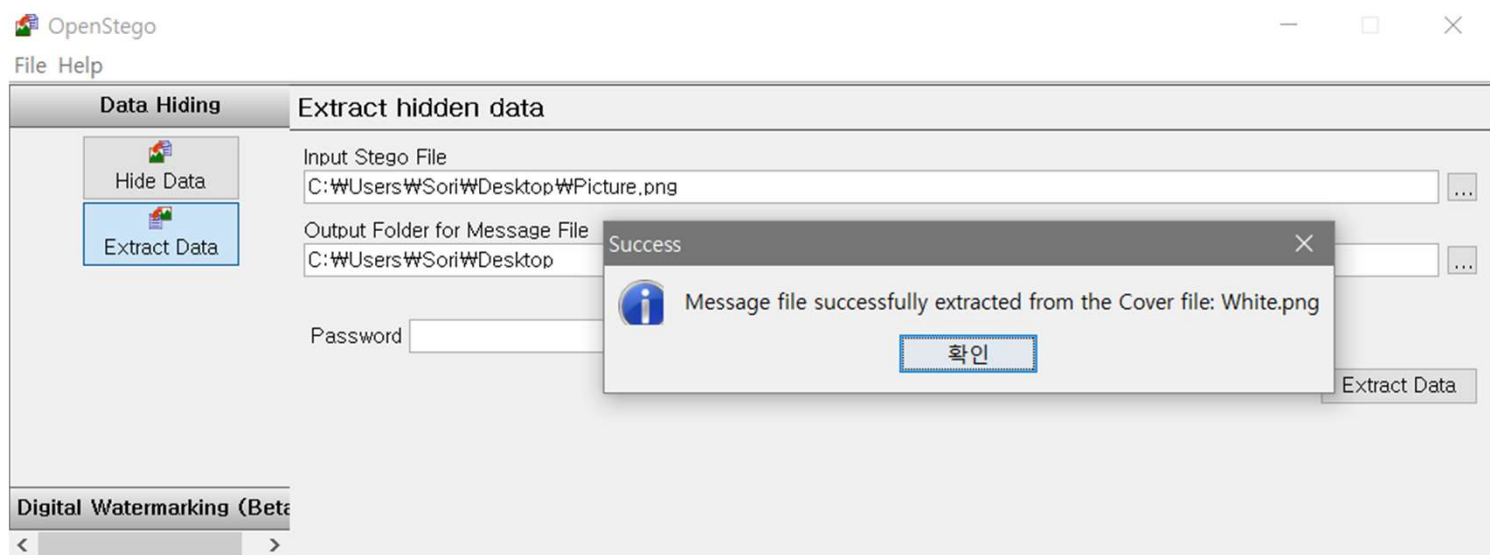
Caesar Cipher — Shift Cipher

FLAG_IS_TRITHEMIUS_CIPHER

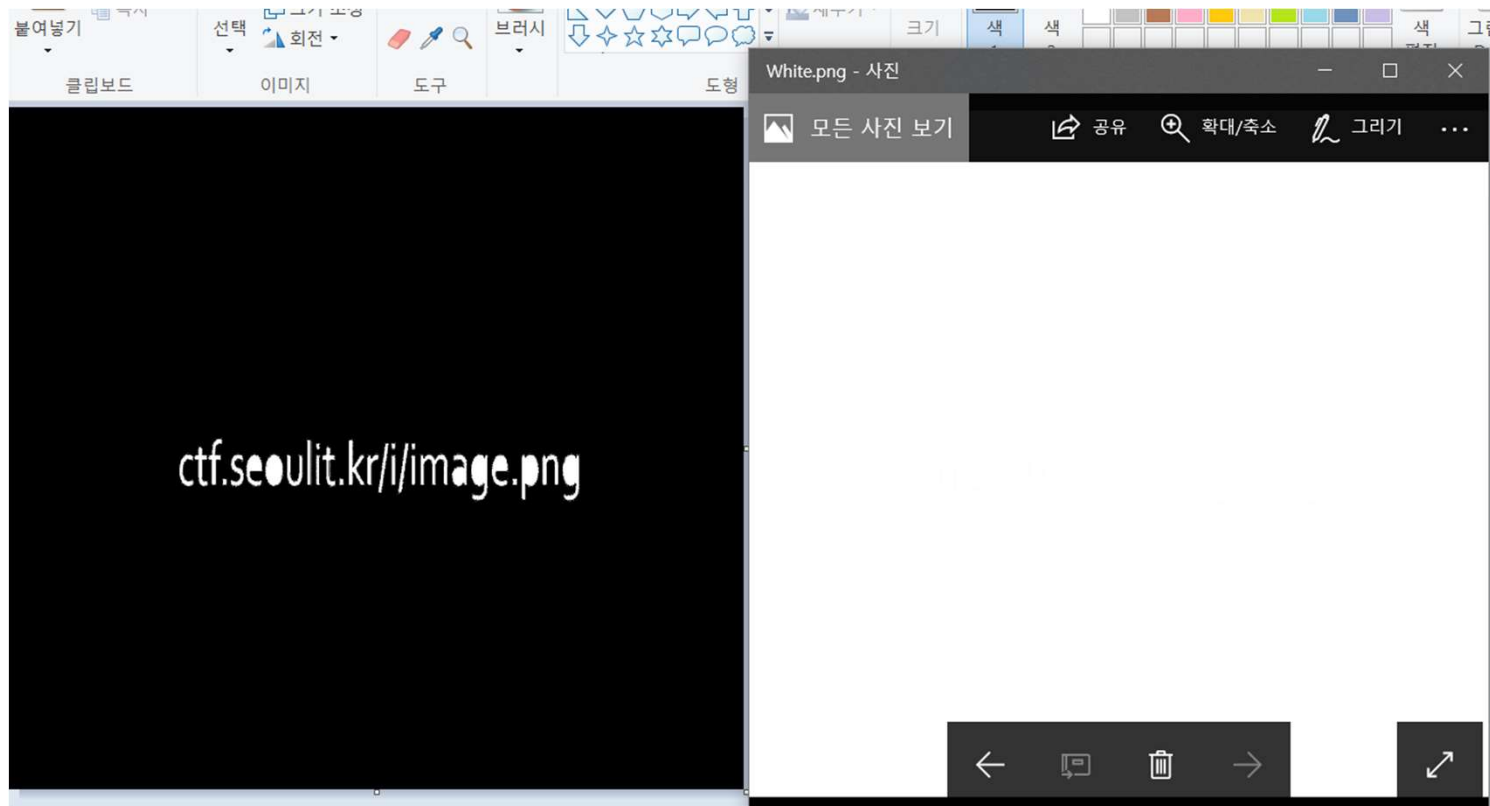
4. Bonobono



제공된 파일을 open stego 7.0 버전으로 extract



4. Bonobono



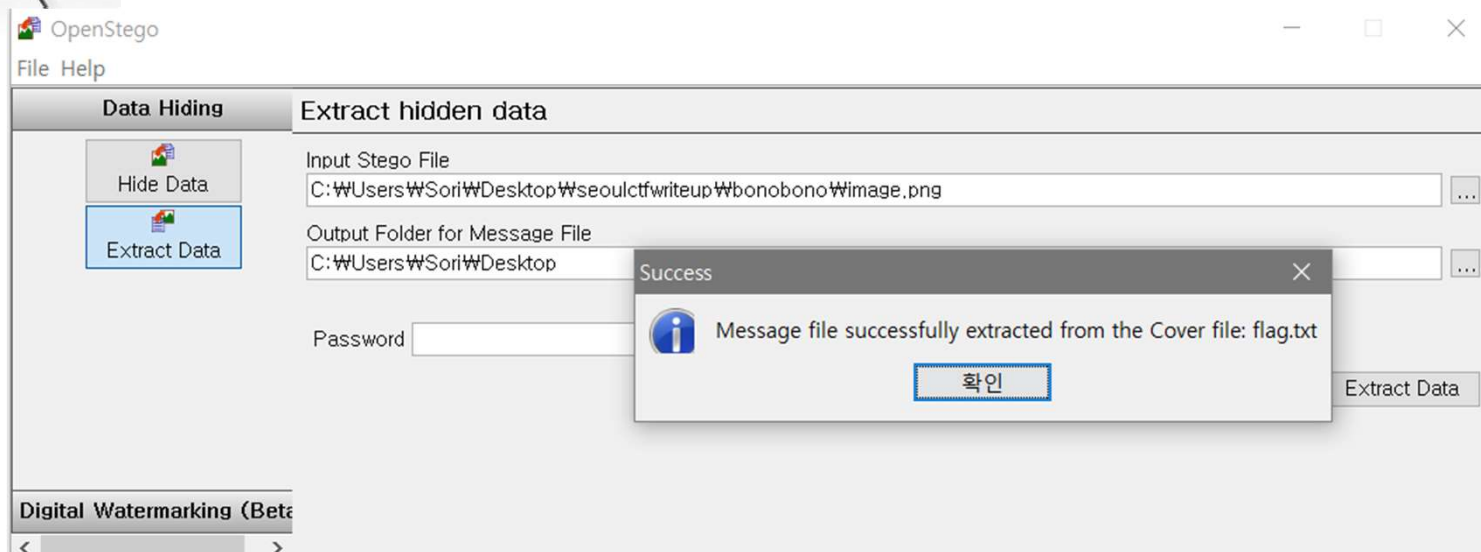
그림판으로 칠해주면 url이 나온다

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

$A \oplus B = C$, $C \oplus B = A$ 와 같은 xor규칙을 이용하여 역연산하면 플래그가 나온다

6. permission

▼ problem.seoulit.kr | permission

값
false

도메인
problem.seoulit.kr

경로
/web/5sdudf6f5214fnj214

기한
23/09/2017 11:51 PM

Host only ☒ 세션 ☐ Secure ☐ HTTP 전용 ☐

✓ 도움말

▼ problem.seoulit.kr | permission

값
true

도메인

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

쿠키 변조

7. spongebob

```
<!--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.

SCTF(SPONG2B0B_1S_P1NGP1NG)

8. wizard

```
<p>unknown</p>
```

```
<input type="radio" value="Fitzgerald"> == $0
```

```
</form>
```

```
</div>
```

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

input 태그에 name값이 안 맞아서 선택이 안 되기때문에 character로 맞춰준다

8. wizard



SCTF{W1ZZARD_POWER_IS_19999}

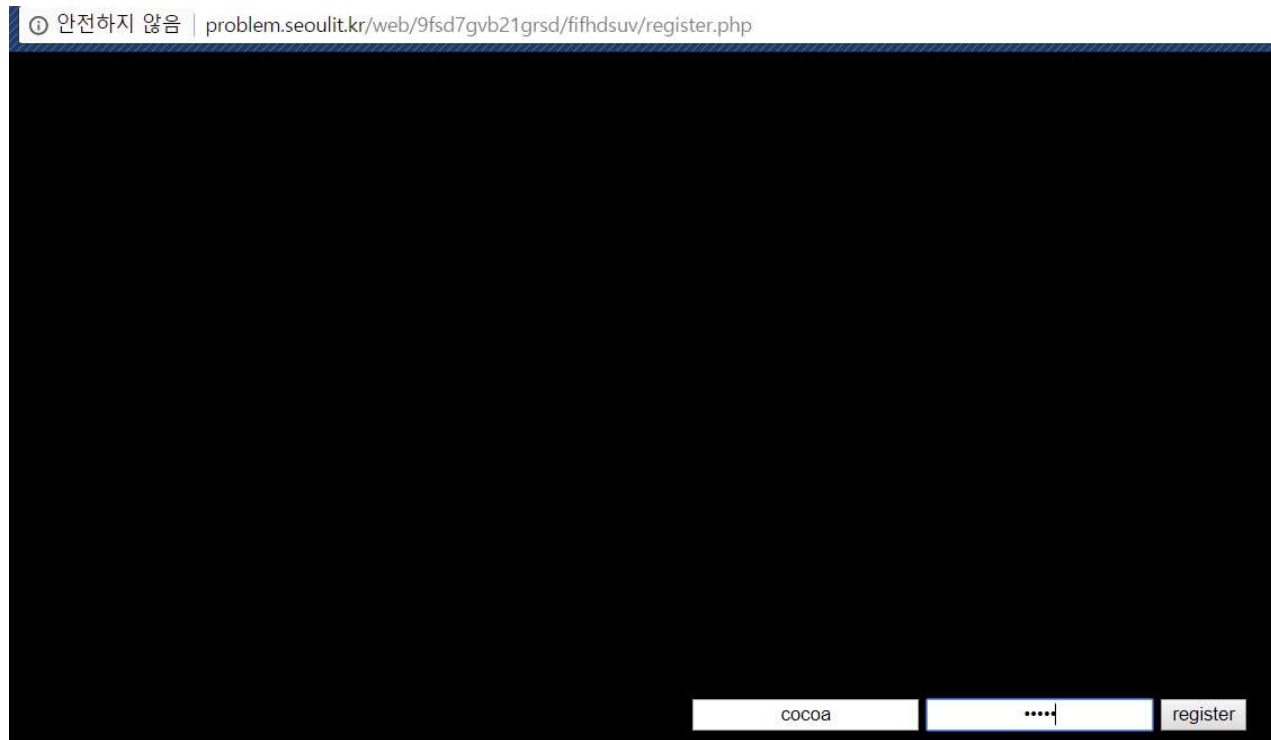
change wizard

change weapon

shop

왜 인지는 모르겠으나 앞에 한글자를 소문자로 해줘야 플래그가 나온다

9. login



소스보고 register.php로 들어가서 회원가입.

9. login

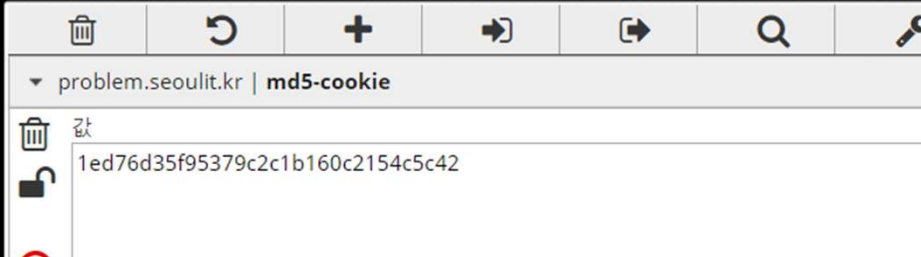
← → ↻ ⓘ problem.seoulit.kr/web/9fsd7gvb21grsd/fifhdsuv/robots.txt

Disallow: /admin

① problem.seoulit.kr/web/9fsd7gvb21grsd/fifhdsuv/admin/

admin only

Found : cocoa
(hash = 1ed76d35f95379c2c1b160c2154c5c42)



SCTF{C00K1E_1S_B2S7_S2CUR1TY}

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  
-->
```

```
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}  
7781
```

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

11. noob test

0042CF4F	00	db 00	
0042CF50	\$ 60	pushad	
0042CF51	BE 00604200	mov esi, Noob_tes.00426000	
0042CF56	8DBE 00B0FDF	lea edi, dword ptr ds:[esi+FFFD8000]	

0042D0D6	^ 75 FA	jnz short Noob_tes.0042D0D2	
0042D0D8	83EC 80	sub esp, -80	
0042D0DB	- E9 5042FDF	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	75 1C	jnz short Noob_tes.004010A0	
00401084	68 40404200	push Noob_tes.00424040	ASCII "Seoulit_is_best"

00401087	5B4D 8C	cmp ecx, dword ptr ss:[ebp-74]	
00401082	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

0040B7CF	68 402A4200	push CrackMe.00422A40		
0040B7D4	E8 47A8FFFF	call CrackMe.00406020		
0040B7D9	83C4 04	add esp, 4		
0040B7DC	8D45 E8	lea eax, dword ptr ss:[ebp-18]		
0040B7DF	50	push eax		
0040B7E0	8D4D F4	lea ecx, dword ptr ss:[ebp-C]		
0040B7E3	51	push ecx		
0040B7E4	E8 27080000	call CrackMe.0040C010		
0040B7E9	83C4 08	add esp, 8		
0040B7EC	85C0	test eax, eax		
0040B7EE	75 0F	jnz short CrackMe.0040B7FF		
0040B7F0	68 900F4200	push CrackMe.00420F90	ASCII "Good Job!!"	
0040B7F5	E8 6658FFFF	call CrackMe.00401060		
0040B7FA	83C4 04	add esp, 4		
0040B7FD	EB 0F	jmp short CrackMe.0040B80E		
0040B7FF	68 740F4200	push CrackMe.00420F74	ASCII "Wrong password! Try again"	
0040B804	E8 5758FFFF	call CrackMe.00401060		
0040B809	83C4 04	add esp, 4		
0040B80C	EB 98	jmp short CrackMe.0040B7A6		
0040B80E	33C0	xor eax, eax		
0040B810	5F	pop edi		
0040B811		

Registers (FPU)	
EAX	0019FF28 ASCII "s68h90i50n"
ECX	00422A40 CrackMe.00422A40
EDX	00000000
EBX	002FC000
ESP	0019FEDC ASCII "?B"
EBP	0019FF40
ESI	004288D0 CrackMe.<ModuleEntryP
EDI	0019FF40
EIP 0040B7DF CrackMe.0040B7DF	
C 0	ES 002B 32bit 0(FFFFFFFF)
P 0	CS 0023 32bit 0(FFFFFFFF)
A 0	SS 002B 32bit 0(FFFFFFFF)
Z 0	DS 002B 32bit 0(FFFFFFFF)
S 0	FS 0053 32bit 2FF000(FFF)
T 0	GS 002B 32bit 0(FFFFFFFF)
D 0	
O 0	LastErr ERROR_SUCCESS (00000000)
EFL	00000202 (NO,NB,NE,A,NS,PO,GE,I
ST0	empty 0,0

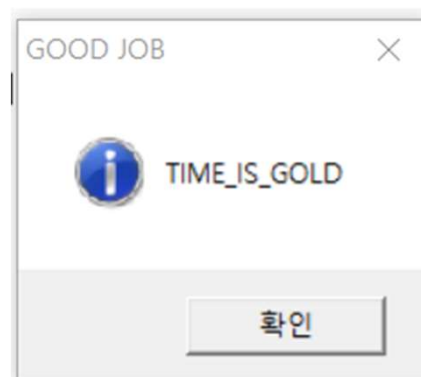
upx 언팩 후 디버거 돌리다보면 위처럼 eax에 플래그가 얹어져 있다.

13. timer

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

```
004011D3 , C2 1000 ret 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,113`부분을 변조하거나 분기를 수정하면 플래그가 나오게 된다.

14. description

004010F6	5E	pop esi	
004010F7	75 4C	jnz short Descript.00401145	
004010F9	33C9	xor ecx, ecx	
004010FB	6A 0C	push 0C	
004010FD	894C24 11	mov dword ptr ss:[esp+11], ecx	
00401101	8D5424 10	lea edx, dword ptr ss:[esp+10]	
00401105	894C24 15	mov dword ptr ss:[esp+15], ecx	
00401109	68 C4504000	push Descript.004050C4	
0040110E	52	push edx	
0040110F	885C24 18	mov byte ptr ss:[esp+18], bl	
00401113	894C24 21	mov dword ptr ss:[esp+21], ecx	
00401117	E8 44000000	call Descript.00401160	
0040111C	83C4 0C	add esp, 0C	
0040111F	85C0	test eax, eax	
00401121	7E 31	jle short Descript.00401154	
00401123	6A 40	push 40	
00401125	8D4424 10	lea eax, dword ptr ss:[esp+10]	
00401129	68 38604000	push Descript.00406038	
0040112E	50	push eax	
0040112F	55	push ebp	
00401130	FF15 A4504000	call near dword ptr ds:[<&USER32.MessageBoxA>]	
00401136	5F	pop edi	
00401137	5D	pop ebp	

Style = MB_OK|MB_ICONASTERISK|MB_APPLMOD

Title = "Answer"

Text

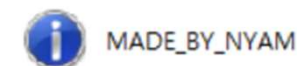
hOwner

MessageBoxA

EAX	00000000
ECX	00000012
EDX	000000EC
EBX	00000000
ESP	0019F9B8
EBP	000A0D70
ESI	000A0D70
EDI	0019F9D6 ASCII "CURITY_IN_SEOUL_ITSorisor i"
EIP	004010F7 Descript.004010F7
C 0	ES 002B 32bit 0(FFFFFFFF)
P 0	CS 0023 32bit 0(FFFFFFFF)
A 0	SS 002B 32bit 0(FFFFFFFF)
Z 0	DS 002B 32bit 0(FFFFFFFF)
S 0	FS 0053 32bit 3C4000(FFF)
T 0	GS 002B 32bit 0(FFFFFFFF)
D 0	
O 0	LastErr ERROR_SUCCESS (00000000)
EFL	00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0	empty 0,0
ST1	empty 0,0
ST2	empty 0,0
ST3	empty 0,0

004010F6	5E	pop esi
004010F7	74 4C	je short Descript.00401145
004010F9	33C9	xor ecx, ecx

Answer



확인

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

004010F7	5E	pop esi	EAX 00000000
004010F9	75 4C	jnz short Descript,00401145	ECX 00000000
004010FB	33C9	xor ecx, ecx	EDX 000000EC
004010FD	6A 0C	push 0C	EBX 00000000
00401101	894C24 11	mov dword ptr ss:[esp+11], ecx	ESP 0019F728
00401105	8D5424 10	lea edx, dword ptr ss:[esp+10]	EBP 001C0038
00401109	894C24 15	mov dword ptr ss:[esp+15], ecx	ESI 001C0038
0040110E	68 C4504000	push Descript,004050C4	EDI 0019F758 ASCII "SECURITY_IN_SEOUL_IT"
00401113	52	push edx	EIP 004010F7 Descript,004010F7
00401117	885C24 18	mov byte ptr ss:[esp+18], bl	C 0 ES 002B 32bit 0(FFFFFFFF)
0040111C	894C24 21	mov dword ptr ss:[esp+21], ecx	P 1 CS 0023 32bit 0(FFFFFFFF)
0040111F	E8 44000000	call Descript,00401160	A 0 SS 002B 32bit 0(FFFFFFFF)
00401121	83C4 0C	add esp, 0C	Z 1 DS 002B 32bit 0(FFFFFFFF)
00401125	85C0	test eax, eax	S 0 FS 0053 32bit 3E8000(FFF)
00401129	7E 31	jle short Descript,00401154	T 0 GS 002B 32bit 0(FFFFFFFF)
0040112E	6A 40	push 40	D 0
00401130	8D4424 10	lea eax, dword ptr ss:[esp+10]	O 0 LastErr ERROR_SUCCESS (00000000)
00401137	68 38604000	push Descript,00406038	EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
0040113D	50	push eax	ST0 empty 0,0
00401140	55	push ebp	ST1 empty 0,0
00401145	FF15 A4504000	call near dword ptr ds:[<&USER32.MessageBoxA>]	ST2 empty 0,0
0040114B	5F	pop edi	ST3 empty 0,0
00401150	5D	pop ebp	ST4 empty 152,99999848008155820
			ST5 empty 1,00000000000000000000

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

Packet list							Narrow & Wide
No.	Time	Source	Destination	Protocol	Length	Info	
429	72.319043	10.1.1.254	10.1.1.1	TELNET	60	Telnet Data ...	
430	72.354487	10.1.1.1	10.1.1.254	TELNET	55	Telnet Data ...	
431	72.359494	10.1.1.254	10.1.1.1	TELNET	60	Telnet Data ...	
432	72.548679	10.1.1.1	10.1.1.254	TCP	54	1040→23 [ACK] Seq=248 Ack=...	
433	76.220726	c4:01:12:f8:f1:01	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/0/c4:0...	
434	80.151196	c4:01:12:f8:f1:01	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/0/c4:0...	
435	84.084260	c4:01:12:f8:f1:01	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/0/c4:0...	
436	87.747797	10.1.1.1	10.1.1.254	TELNET	55	Telnet Data ...	
437	87.755809	10.1.1.254	10.1.1.1	TELNET	60	Telnet Data ...	
438	87.755809	10.1.1.1	10.1.1.254	TELNET	68	Telnet Data ...	
439	87.776816	10.1.1.254	10.1.1.1	TELNET	60	Telnet Data ...	
440	87.786822	10.1.1.254	10.1.1.1	TELNET	60	Telnet Data ...	
Frame 438: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0							
Ethernet II, Src: Vmware_39:5f:d4 (00:0c:29:39:5f:d4), Dst: c4:02:15:3c:00:00 (c4:02:15:3c:00:00)							
Internet Protocol Version 4, Src: 10.1.1.1, Dst: 10.1.1.254							
Transmission Control Protocol, Src Port: 1040, Dst Port: 23, Seq: 249, Ack: 508, Len: 14							
Telnet							
0000	c4 02 15 3c 00 00 00 0c	29 39 5f d4 08 00 45 00	...<....)9_...E.				
0010	00 36 03 9a 40 00 80 06	e0 27 0a 01 01 01 0a 01	.6..@...'......				
0020	01 fe 04 10 00 17 4b 6d	85 f4 31 ac 84 4e 50 18Km ..1..NP.				
0030	f8 f5 39 72 00 00 65 74	77 6f 72 6b 5f 49 73 5f	..9r..et work_Is_				
0040	45 61 73 79		Easy				

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)

← → ↻ ⓘ 52.78.182.122/fsadfhui21421uifbsdf8sa722148hvsvnasd.php

SCTF{fsdag412ydfs8xv5249vhdt7fudsg2fbvmvb21}

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=""_11111111111111111111'+'_11111111'+'_11111111'+'_11111111111111111111'+'_11111111'+'_11111111111111111111'+'_1'+'_1111'+'_111111111111'+'_11111111'+'_111111111111'+'_111111111111'+'_111111111111'+'_111111111111'+'_1'+'_11111111'+'_111111'+'.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"_1111111111111="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+s+a+d+m+i+n+p+a+g+e+.php"  
        thisisadminpage.php  
    }  
  
    else{  
        alert("Page Error\n[Permission Denied]")  
    }  
}
```

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

수고하셨습니다.