DIMI CTF
Write up

대덕소프트웨어마이스터고등학교 김성훈 (닉네임 :)

참가 부분 : 고등부

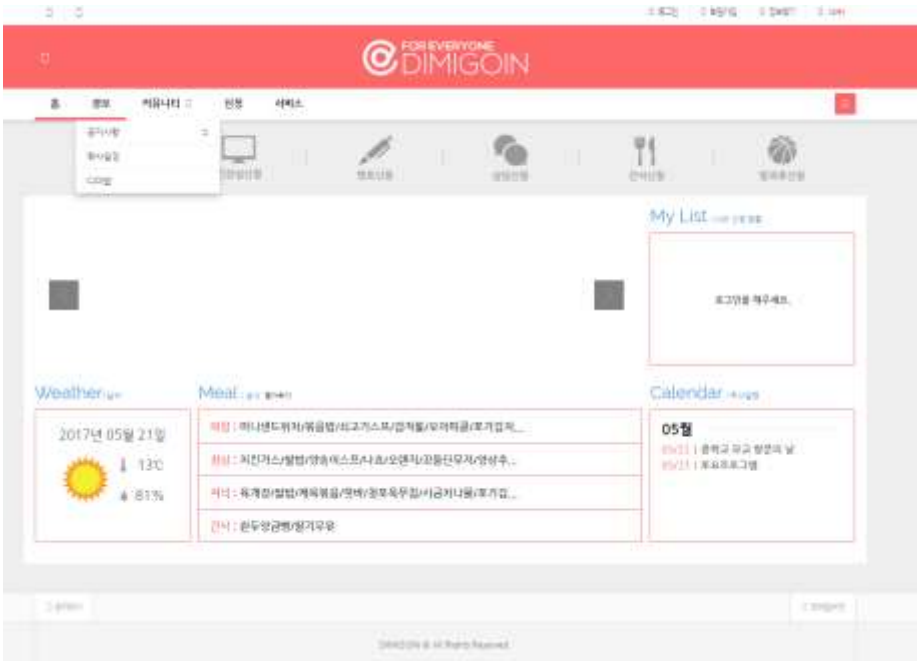
이메일 : sunghun7511@naver.com

1. Web
   A. 100

처음 사이트에 접속하면

이런 알림이 뜬다.

그리고 사이트에 들어가보니



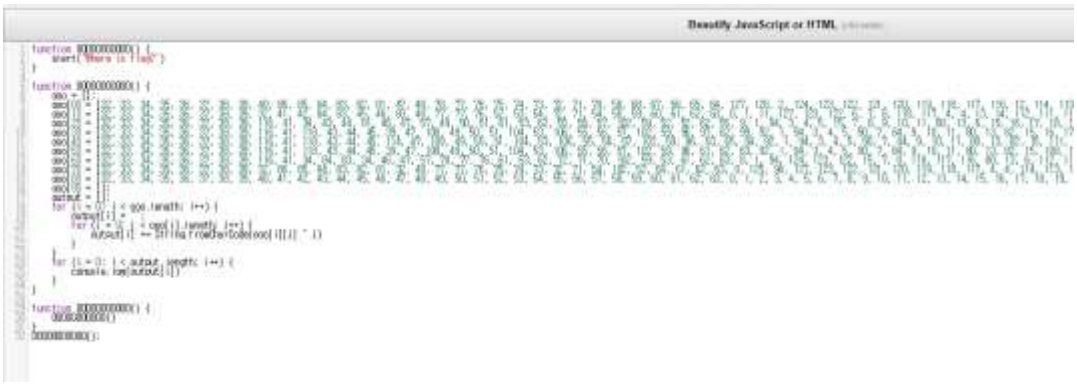
디미고인 사이트를 그대로 가져왔다.

(그래서 일부 링크들은 디미고인으로 연결되었다.)

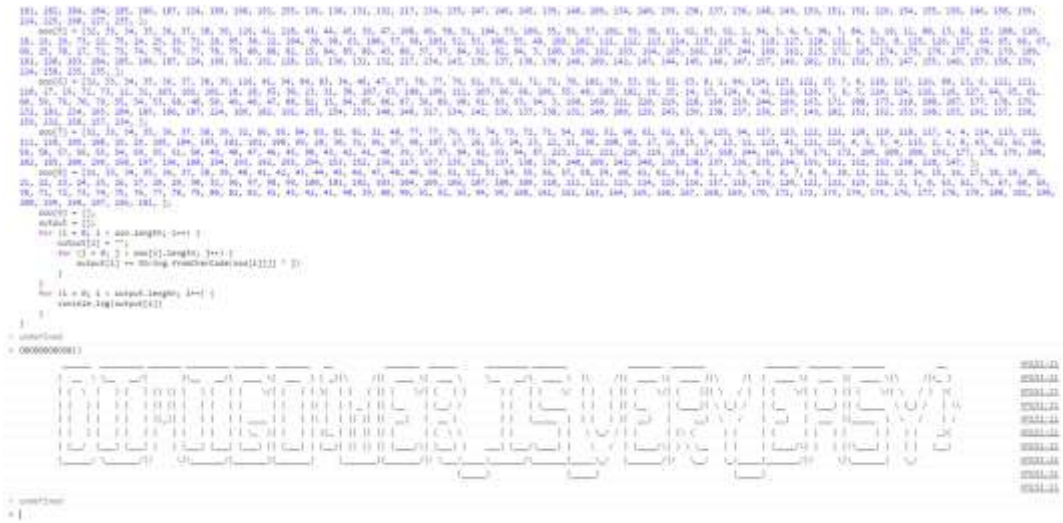
여기서 실제 디미고인 사이트와 차이점을 확인하면서 자바스크립트 파일중

index_files/script.js 이라는 파일을 보게 되었고, 열어보니

이런 스크립트가 나왔는데, 난독화 처리되었구나 라는걸 느끼고 일단은 어떤 기능인지 실험해보기 위해 http://jsbeautifier.org/ 에 접속하여 포매팅을 했더니



이런식으로 함수 3개가 나왔는데 그중 중간에 있는 함수를 자바스크립트 콘솔에 넣고 (크로니움 개발자도구) 실행시키니 플래그가 나왔다.



Flag : dimigo{web_is_very_easy}

B. 200

처음 접속하니

이런 로그인 창이 나왔고, 유저 이름을 치고 LOGIN 버튼을 누르니

이런식으로 2048 게임이 나왔다.

열심히 게임을 하다 게임이 끝나니

RANK

RANK USERNAME

1	jtjisgod_0.0.0.0
2	1%a1');/*_114.207.221.197
3	swccsproj_114.207.221.197
4	1_121.170.91.130
5	7020kjs_221.158.206.97
6	1_121.170.91.130
7	A_121.170.91.130
8	it'sme_121.170.91.130
9	it'sme_121.170.91.130
10	HIHIHIHIHIHIHHI_121.170.91.130
11	HIHIHIHIHIHIHHI_121.170.91.130
12	I_AM_GOD__121.170.91.130
13	jib_121.170.91.130

이렇게 랭크가 나왔다. 문제를 보니

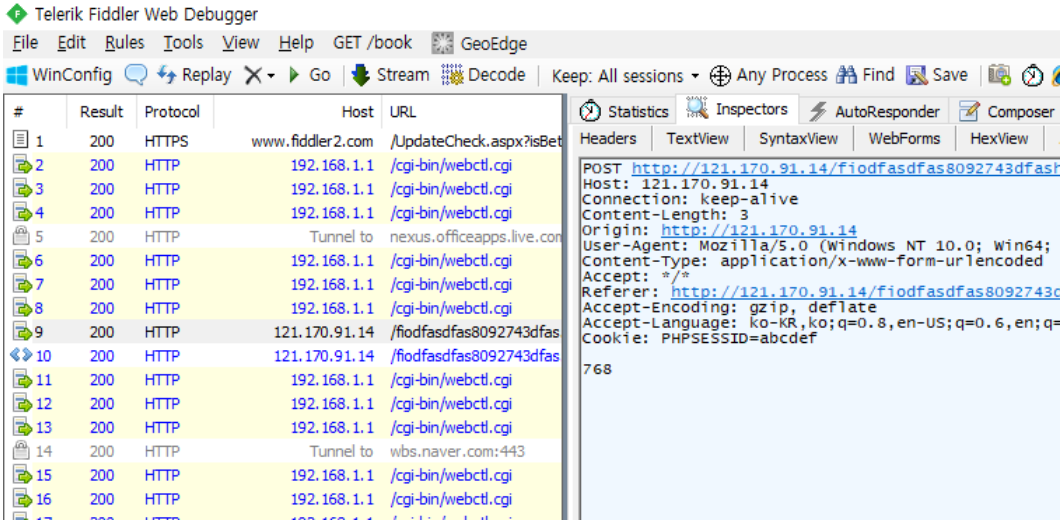
Be a GoD (200p)

아주 간단한 문제

Be a GoD 이다.

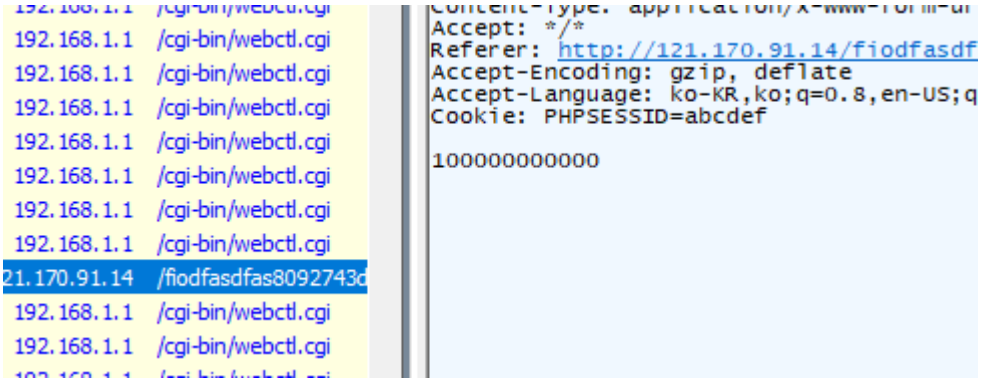
GoD 가 되라는 문제인데, 랭크 페이지 맨 오른쪽을 보니 가장 점수가 높으면 GoD 라고 표시가 된다.

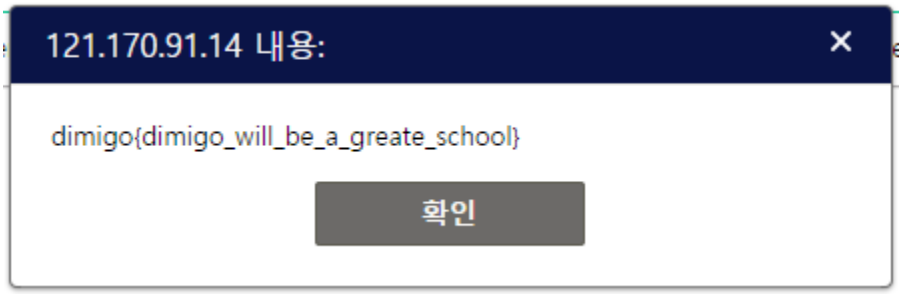
그래서 Fiddler 이라는 프로그램을 이용하여 패킷을 캡쳐해봤는데



이런식으로 문자 형식으로 점수를 전달한다.

그래서 저 문자를 현재 GoD의 점수보다 1 높은 100000000000 를 입력하고 재전송 한 뒤, 랭킹 화면에 들어갔더니 플래그가 나왔다.

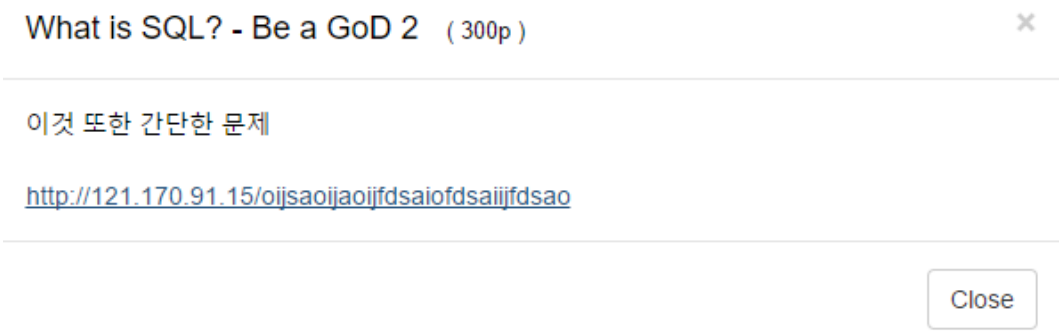




Flag : dimigo{dimigo_will_be_a_greate_school}

C. 300

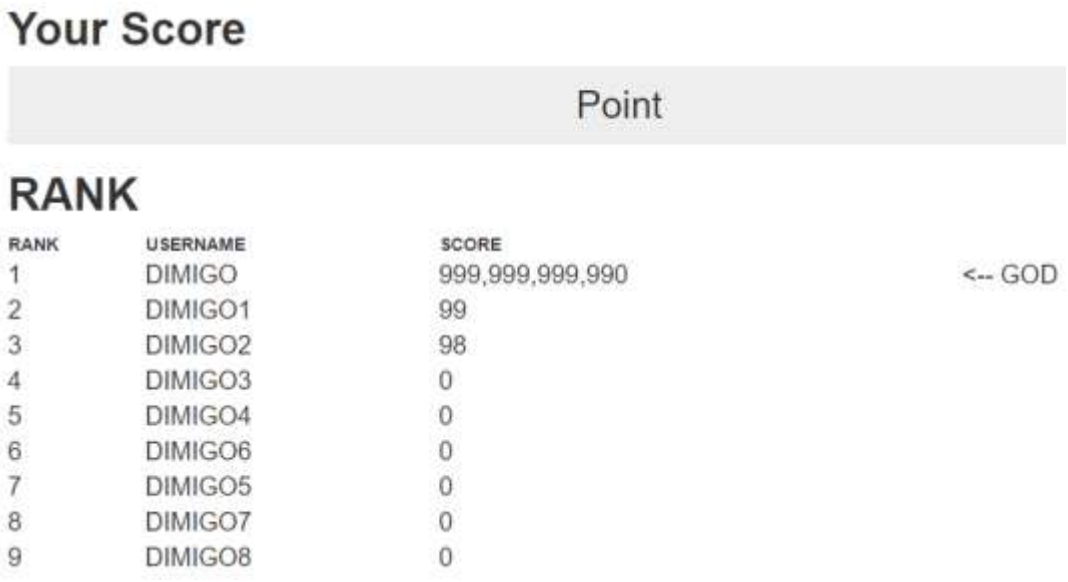
이 문제도 GoD 이 되라는 문제였다.



근데 SQL 에 대해 언급한 것 보니 SQL 인젝션을 이용해야 하는 것 같다.

들어가보니 똑같이 로그인 페이지가 나온다.

똑같이 2048이 나왔고, 2048에서 게임이 끝나고 나니



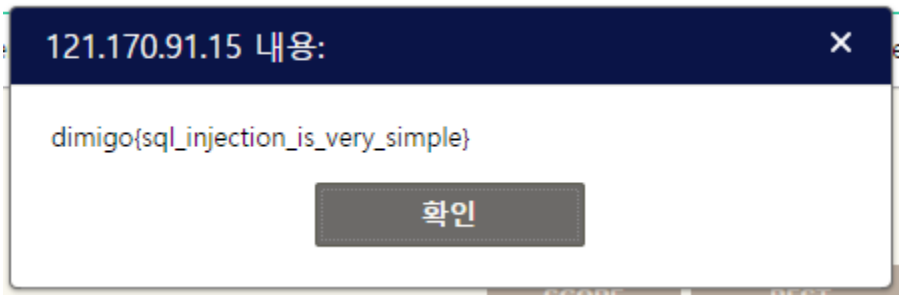
다음과 같은 랭킹 페이지가 나왔다. 현재 GOD는 DIMIGO이다.

이 문제를 풀려고 세션을 위조해서 보내고 혹시나 하는 마음에 포인트를 위조하기도 하는 등 여러 방법을 시도했지만 풀리지 않았다.

그런데 진짜 이렇게 쉽게 풀릴 줄은 몰랐는데,.....하.....

(솔직히 짜증났다.. 수준을 너무 높게 봤나.. 이 문제 때문에 시간 너무 뺐겼다..)

GOD 유저인 DIMIGO 를 쓰고 SQL을 끝내는 구문인 ‘ 을 쓰고 SQL 주석인 #를 써서 DIMIGO#’를 쓰고 로그인 한 뒤, 2048 을 풀게 되면

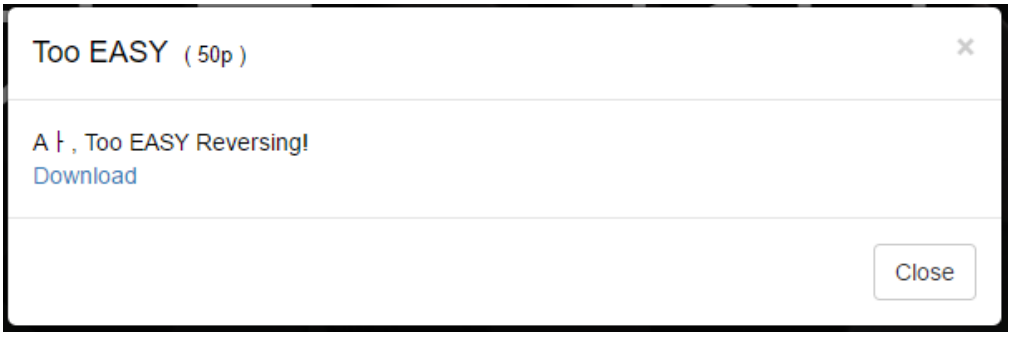


플래그가 나온다.

Flag: dimigo{sql_injection_is_very_simple}

2. Reversing
   A. 50

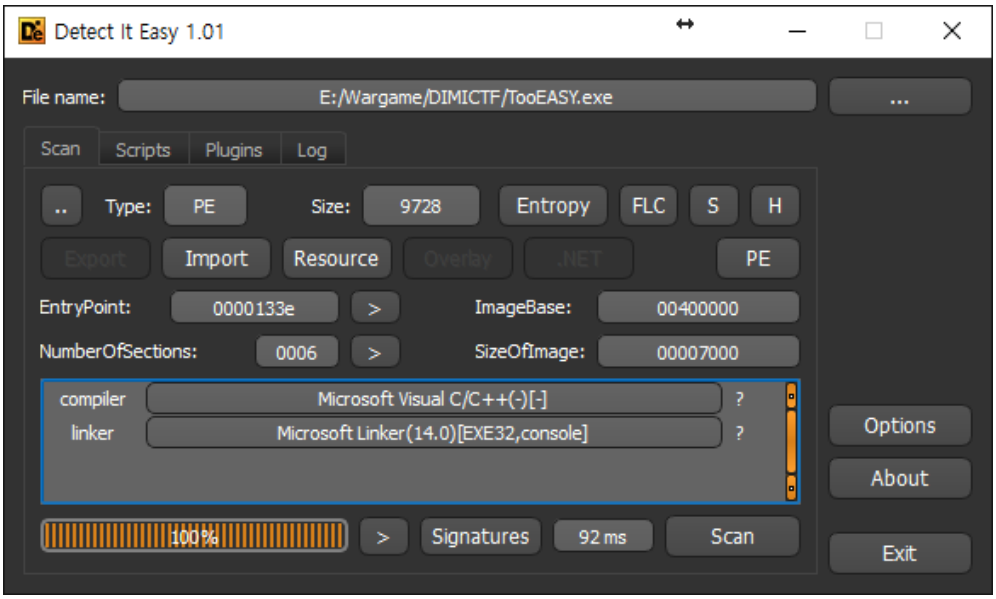
문제를 열어보니



이렇게 되어있다. 파일을 다운받아봤다.

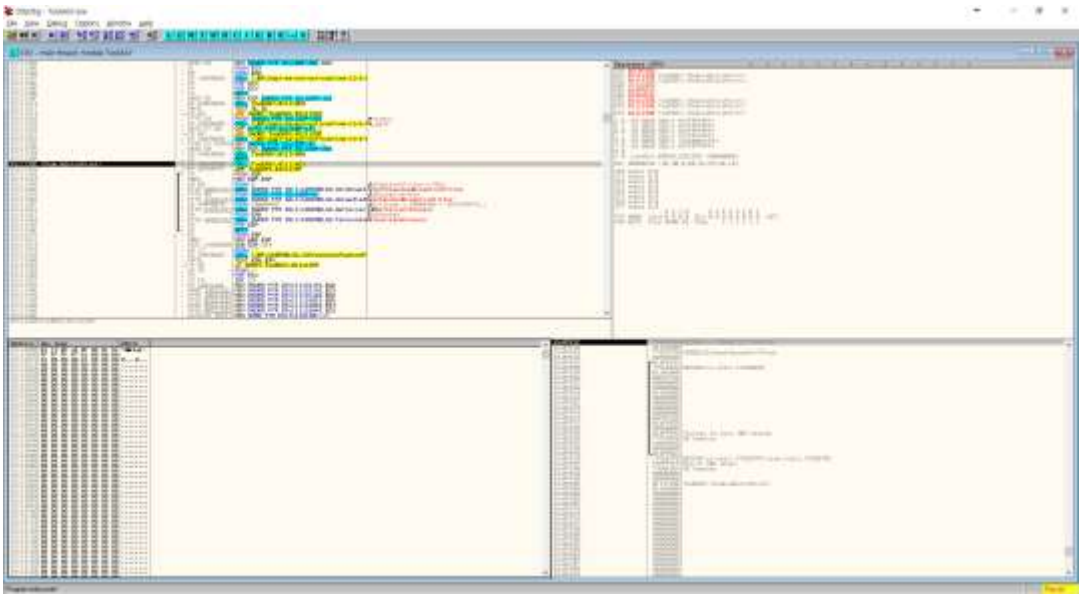
TooEasy.exe이다.

DIE(Detect It Easy) 라는 프로그램으로 파일을 확인해보니

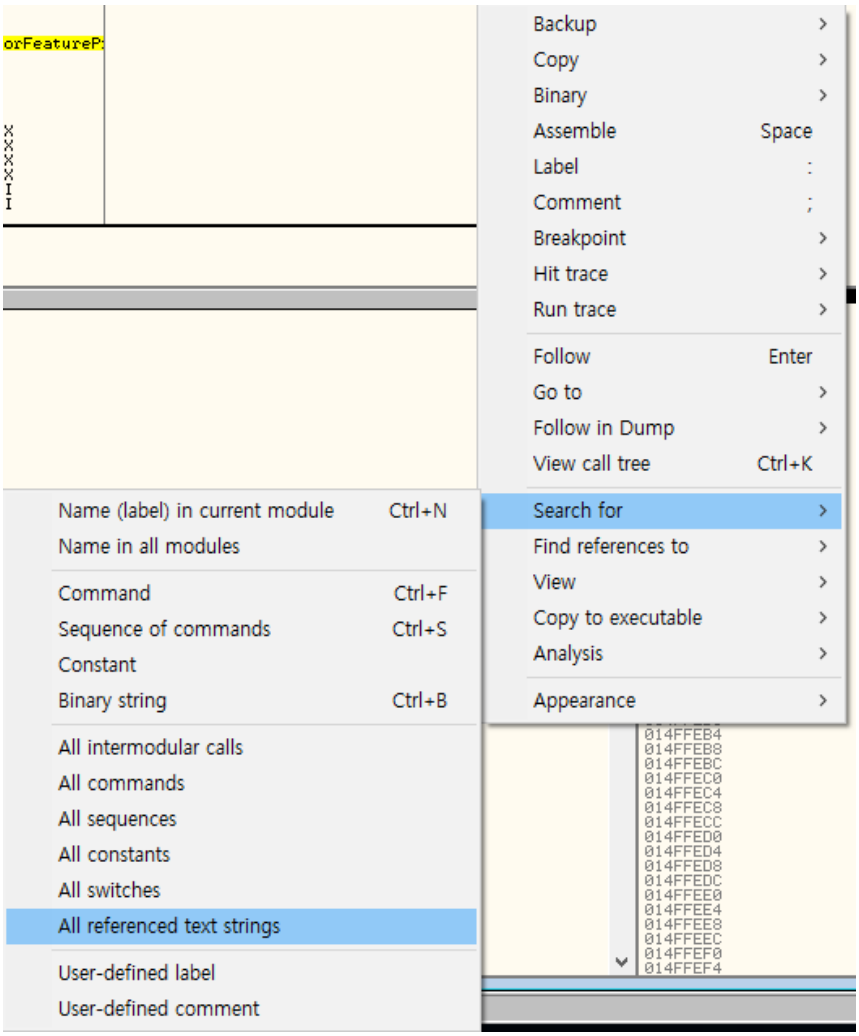


윈 32 콘솔 응용프로그램이다.

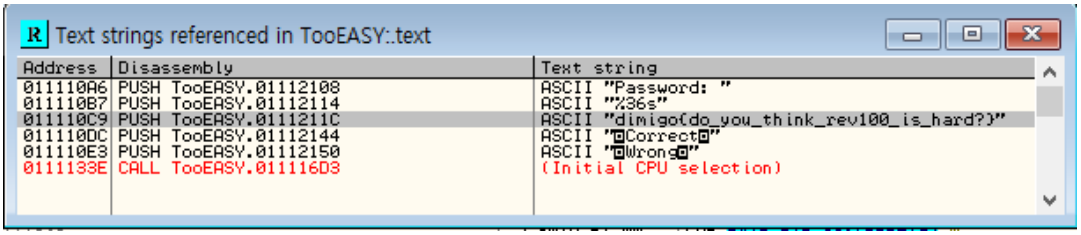
Ollydbg를 통해서 파일을 열어보았다.



그리고 텍스트 들을 확인하기 위해서 다음과 같이 접근하였다.



..그랬더니



바로 나왔다.

Flag: dimigo{do_you_think_rev100_is_hard?}

B. 100

Warm REV (100p)

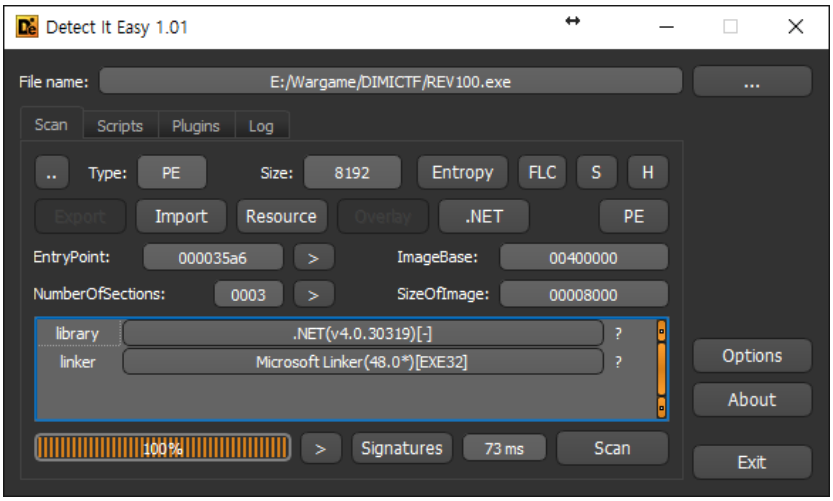
도샵 리버싱
Download

Close

문제를 보니 파일을 한 개 주고 도샵 리버싱이라고 한다.

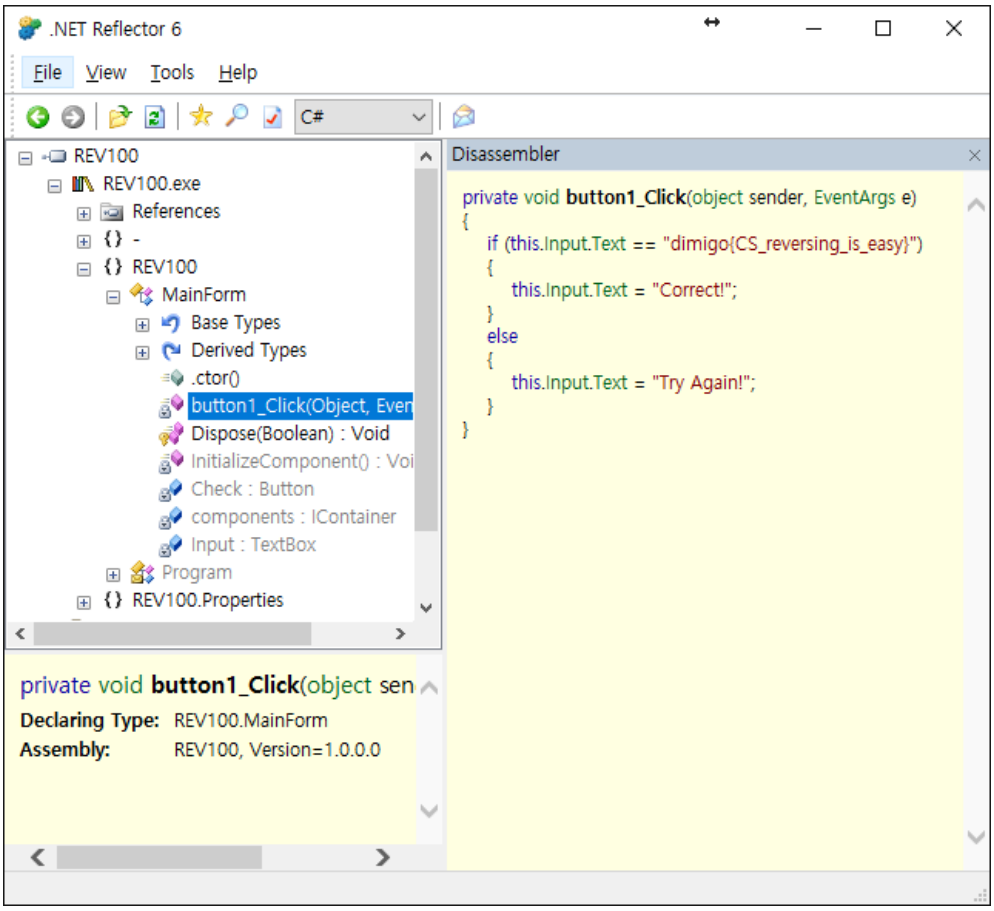
(지금 생각해보니 도샵은 C#이네..? 빼ㅐㅇ애애ㅐ앵ㄱ 머 어짜피 간단히 풀었지만)

DIE 프로그램을 통해서 확인해보았다.



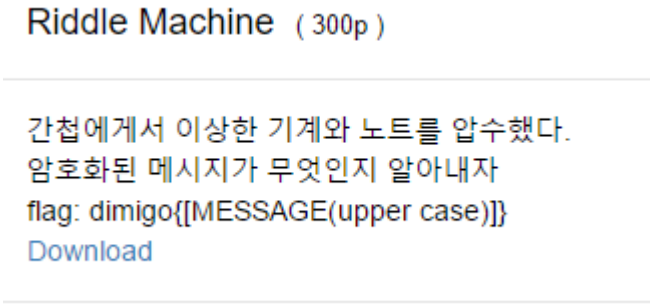
.NET 위에서 동작하는 exe 파일이다.

.NET 디컴파일러인 Reflector를 사용해서 디컴파일링 하였다.



Flag: dimigo{CS_reversing_is_easy}

C. 300



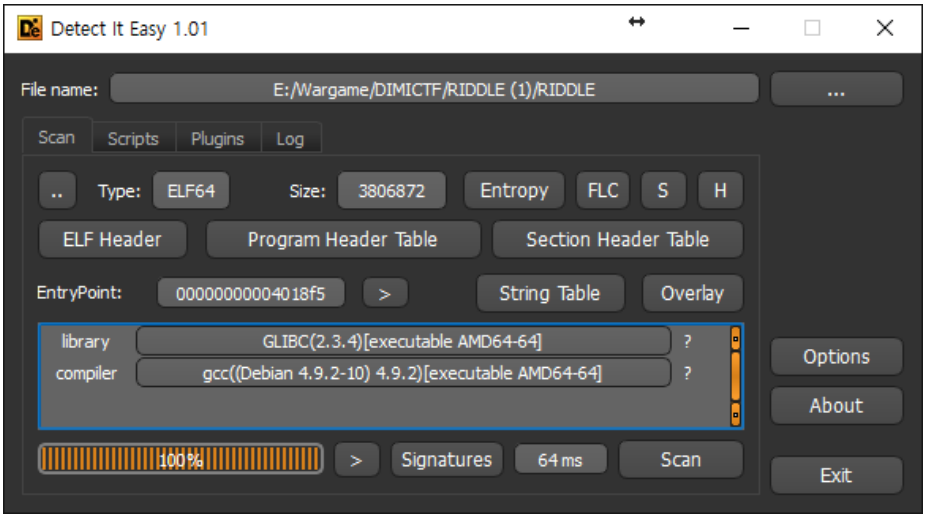
문제가 되게 재미있게 생겼다.

암호화 하는 프로그램을 주고 문자열 주고 복호화 하라 하겠지

하면서 열어봤는데

??? 파일 확장자가 없고 용량이 되게 큰데

DIE 로 확인해보니



리눅스 AMD 64 바이너리이다.

.. 리눅스 켜서 확인을 해봤다.

실행 시키니까

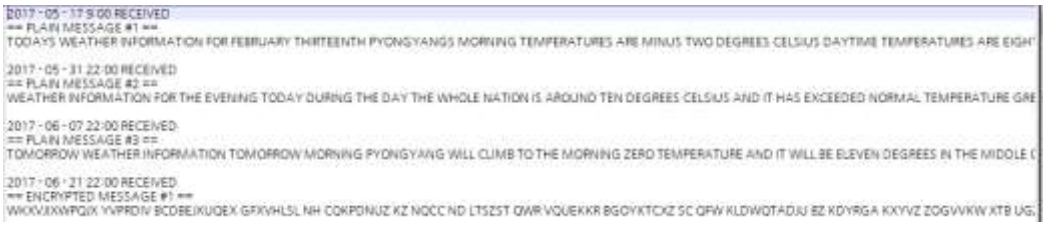
```
shgroup@ubuntu:~/Desktop/ctf/DIMICTF$ cd RIDDLE\ \(1\)/
shgroup@ubuntu:~/Desktop/ctf/DIMICTF/RIDDLE (1)$ ls
auto.py  NOTE.txt  RIDDLE
shgroup@ubuntu:~/Desktop/ctf/DIMICTF/RIDDLE (1)$ ./RIDDLE
Ring Setting(AAA-ZZZ): 132
Traceback (most recent call last):
  File "RIDDLE.py", line 81, in <module>
AssertionError
Failed to execute script RIDDLE
shgroup@ubuntu:~/Desktop/ctf/DIMICTF/RIDDLE (1)$
```

이런식으로 AAA-ZZZ 까지 입력을 받게 한 다음에 문자열 한 개를 입력 받는다.

근데 AAA-ZZZ 가 아닌 문자열을 입력하면 위에처럼 파이썬에서 주로 보던 오류가 터진다.

아마 컴파일된 파이썬이려나..? 하는 생각을 가지고 그냥 브루트 포싱을 하기로 했다.

같이 준 NOTE.txt 파일을 보면



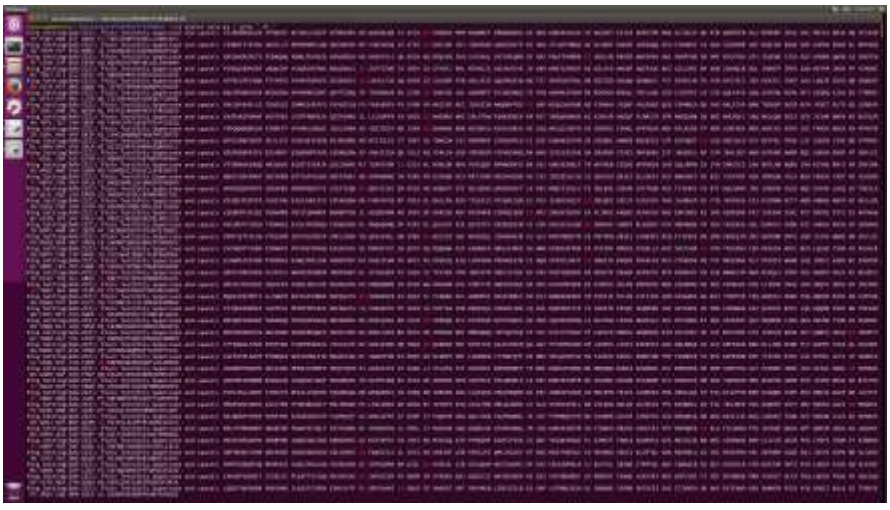
Plain Text 3개에 문장이 들어있고 암호화된 문자열이 있는데, AAA-ZZZ 중 한 개를 입력하고, 암호화 된 문자열을 넣으면 되는 문제라고 생각해서 일반 문자열 중에 꼭 나오는 문자열인 " IS "를 포함한 문자열을 찾도록 하고, AAA부터 ZZZ 까지 돌려보았다.

(여기서 " IS "인 이유는 단어 중간의 IS 가 아닌, be동사 IS 로 하기 위해서이다.)

```
1  import os
2
3  lst = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
4
5  for z in lst:
6      for y in lst:
7          for x in lst:
8              os.system("(python -c 'print ₩"" + x + y + z + "₩₩nWKXVJIXWPQJX YVPRDIV BCDBEJXUQEX GFXVHLSL
                   NH CQKPDNUZ KZ NQCC ND LTSZST QWR VQUEKKR BGOYKTCXZ SC QFW KLDWQTADJU BZ KDYRGA
                   KXYVZ ZOGVVKW XTB UGZZIGO VJ QPV YORGPPY RQN ZNDART HYCV DRG NLKYN SQWG VX DUAHQU
                   CW UTOT ZGA INI BFYC SO FEVNOBDGJUGYPGMJOYTEJY₩"') | ./RIDDLE")
9
```

다음처럼 페이로드를 짰다.

파이썬의 os.system 으로 AAA부터 ZZZ, \n과 인코딩된 문자열을 출력하고 그 문자열을 파이프라인을 통해 ./RIDDLE 의 표준 입출력으로 넣어줬다.



그리고 python ./auto.py | grep " IS " 를통해서 출력중에서 " IS "를 포함하는 문자열을 찾도록 하였다.

그리고 인내심을 가지고 보니 플래그가 나왔다.

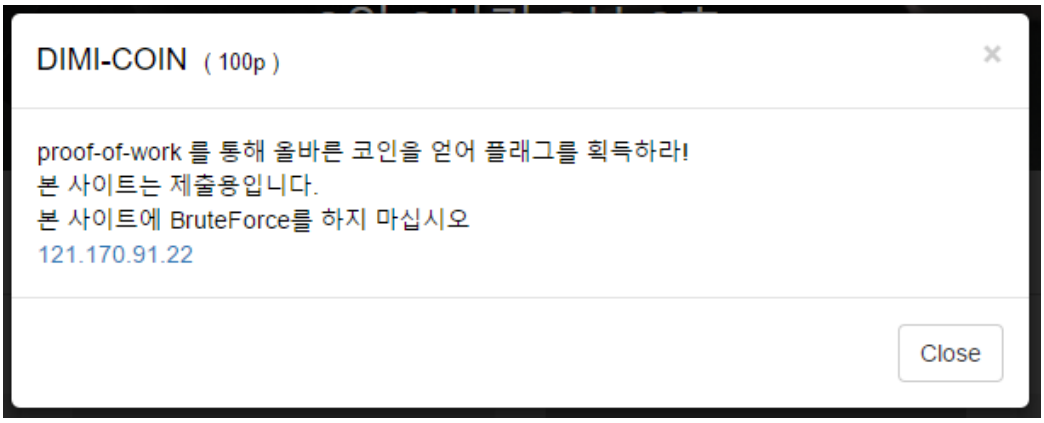
Flag : dimigo{IPAYHOMAGETOALANTURING}

3. MISC
   A. 1

입력했더니 플래그였다.

Flag: dimigo{Welcome_to_DIMICON}

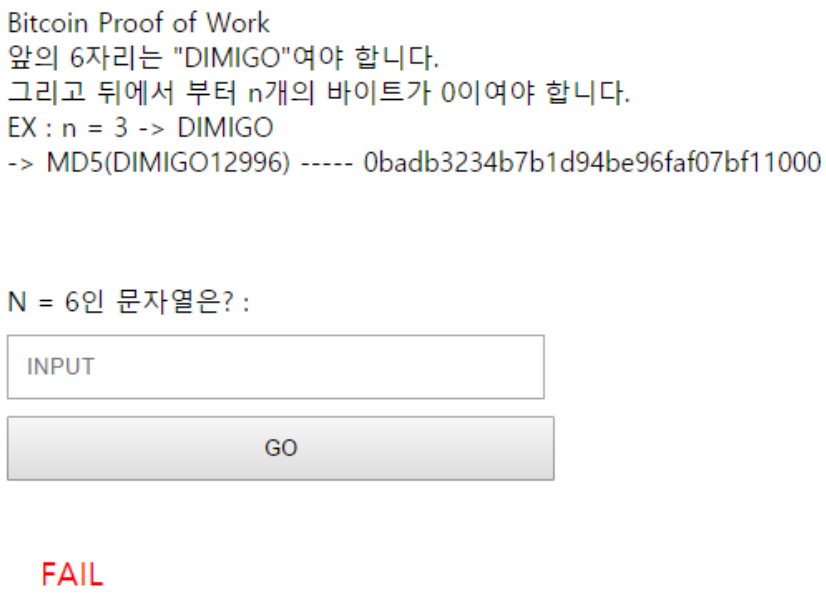
   B. 100 (DIMI-COIN)



디미 코인 이라는 문제이다.

가상화폐 채굴을 본딴 것 같다.

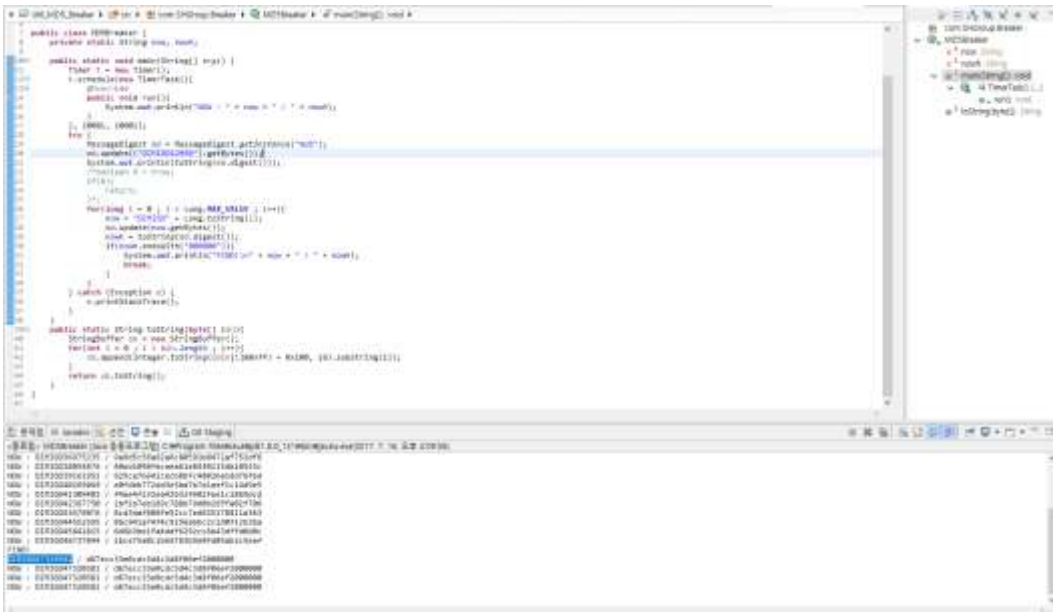
들어가보니



이렇게 뜬다.

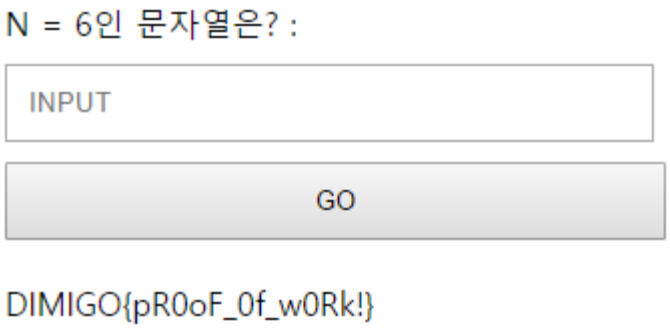
DIMIGO로 시작하는 문자열의 MD5 해시가 0 6개로 끝나면 되는 문제이다.

간단하게 파이썬으로 짰다가 속도의 한계를 느끼고 자바로 갈아탔다.



찾은 값을 사이트에 넣고 인증을 하니

-> MD5(DIMIGO12996) ----- 0badb5234b7b1d94



플래그가 나왔다.

Flag: DIMIGO{pR0oF_0f_w0Rk!}

C. 100 (DIMI-114)

중간에 쉬는 문제로 나온 것 같다.

(다른분들은 포렌식 툴을 이용해서 푸시던데 나는 그냥 구글 검색으로 풀었다.)

DIMI-114 (100p)

외쿡인으로 부터 전화가 왔다!
What is the name of this cultural heritage?
그래서 상담원이 하는 말 : GPS! GPS!
그랬더니 외쿡인으로부터 이미지가 한장 전송되었다!
외쿡이는 현재 무엇을 보고 있는 것일까?
(띄어쓰기 하지마세요!)
FLAG : DIMIGO{이름}
HINT : 사진과는 관련 없음
https://drive.google.com/open?id=0B-vUealQ_HWMb05reDhaRWEwZmc

Close

문제에서 주어진 링크에 들어가보면

이런 사진을 준다.

앞에 써있는 ‘부처님 오신날’ 과 9층을 연관지어

‘부처님 오신날 9층석탑’이라고 치니까

세계 간화선 무차대회 라는곳이 나왔고

광화문에서 개최된다고 한다.

Flag: dimigo{광화문}