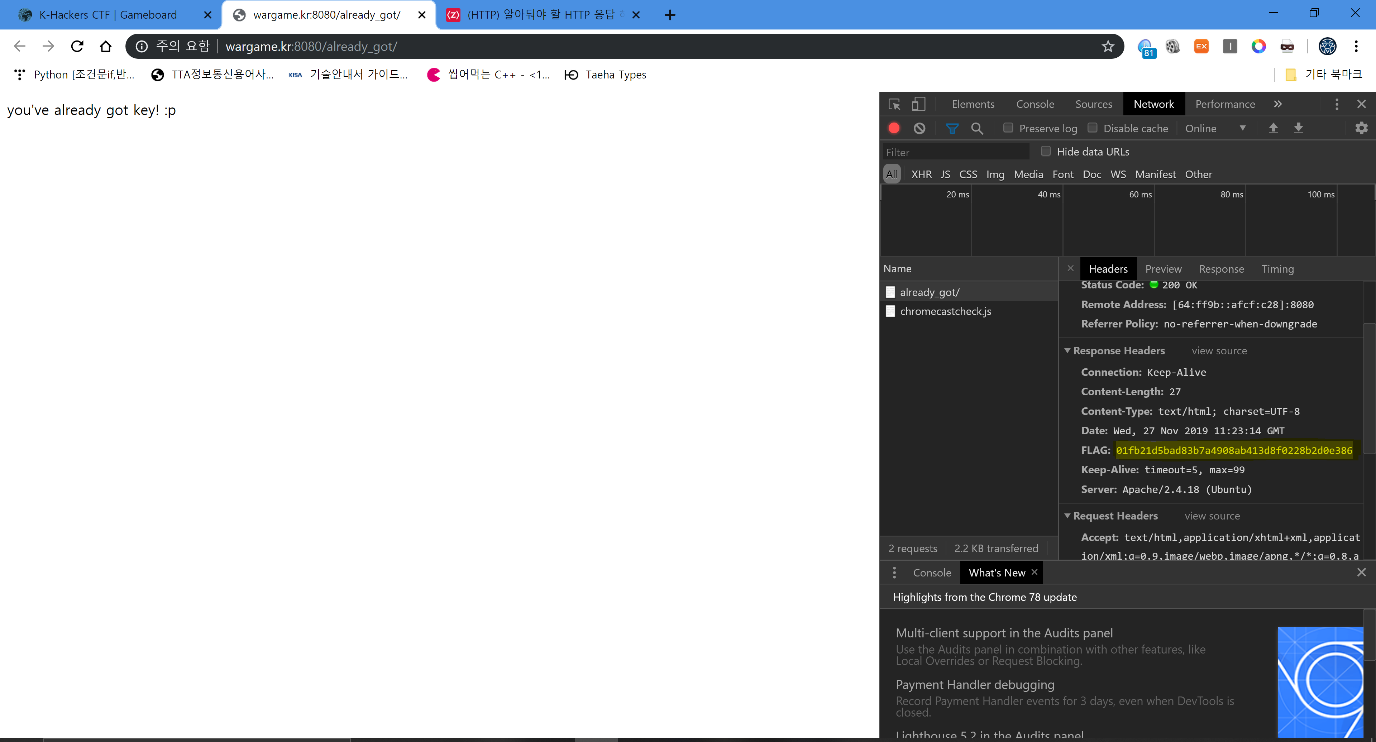
20191235 이형규 3주차 CTF 보고서 2019년11월30일

* 방글라데시

문제: HTTP Response header를 찾을 수 있니?

해답: HTTP 응답 헤더가 일단 무엇일까? 먼저 HTTP는 Hyper Text Transfer Protocol 의 약자로, 인터넷에서 데이터를 주고 받을 수 있는 통신 규약입니다. 그렇다면 응답 헤더는 또 무엇일까요? 간단하게 HTTP 헤더 내 응답 헤더입니다. 특정 유형의 요청이나 헤더를 수신하였을 때 이에 응답을 하게 되는데, 제가 사용하는 크롬 버전에서는 F12를 눌러 네트워크 탭으로 이동, 탭을 넘기다 보면 HTTP Response Header 항목을 찾을 수 있습니다.



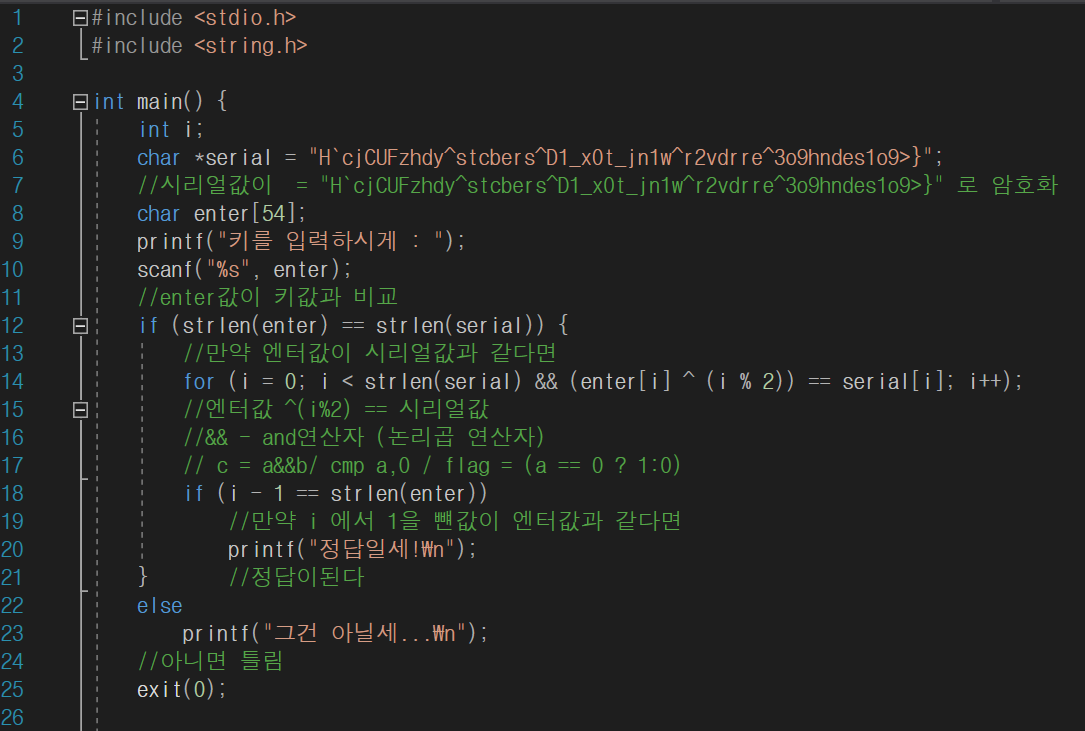
응답 헤더의 플래그 부분이 정답 되겠습니다.

* 카자흐스탄 문제

문제: 리버싱을 해봐

해답:

아래는 확인한 문제의 코드를 읽고 주석을 달아본 것입니다.



문제를 보면 enter[i] ^ (i%2)로 암호화 되어있는 것을 보아 XOR 연산으로 암호화 되어있음을 알수 있다. Xor 연산은 비트 연산의 다른 말로, 한 개 혹은 두개의 이진수에 대해 비트단위로 적용되는 연산임을 알 수가 있습니다. 그렇다면 문제를 풀기 위해서는 디코딩할 코드를 제작하거나, 다시 한번 더 연산을 해주면 원래의 값을 얻을 수가 있을 것 입니다.

저는 파이썬으로 위의 코드를 풀 수 있도록 코딩을 하였습니다.

밑의 코드는 파이썬으로 제작한 디코딩 코드이고, 정답은

HackCTF{hey\_success\_D0\_y0u\_kn0w\_r3verse\_3n9ineer1n9?} 입니다.

dap = "H`cjCUFzhdy^stcbers^D1\_x0t\_jn1w^r2vdrre^3o9hndes1o9>}"

flag = ""

for i in range(len(dap)):

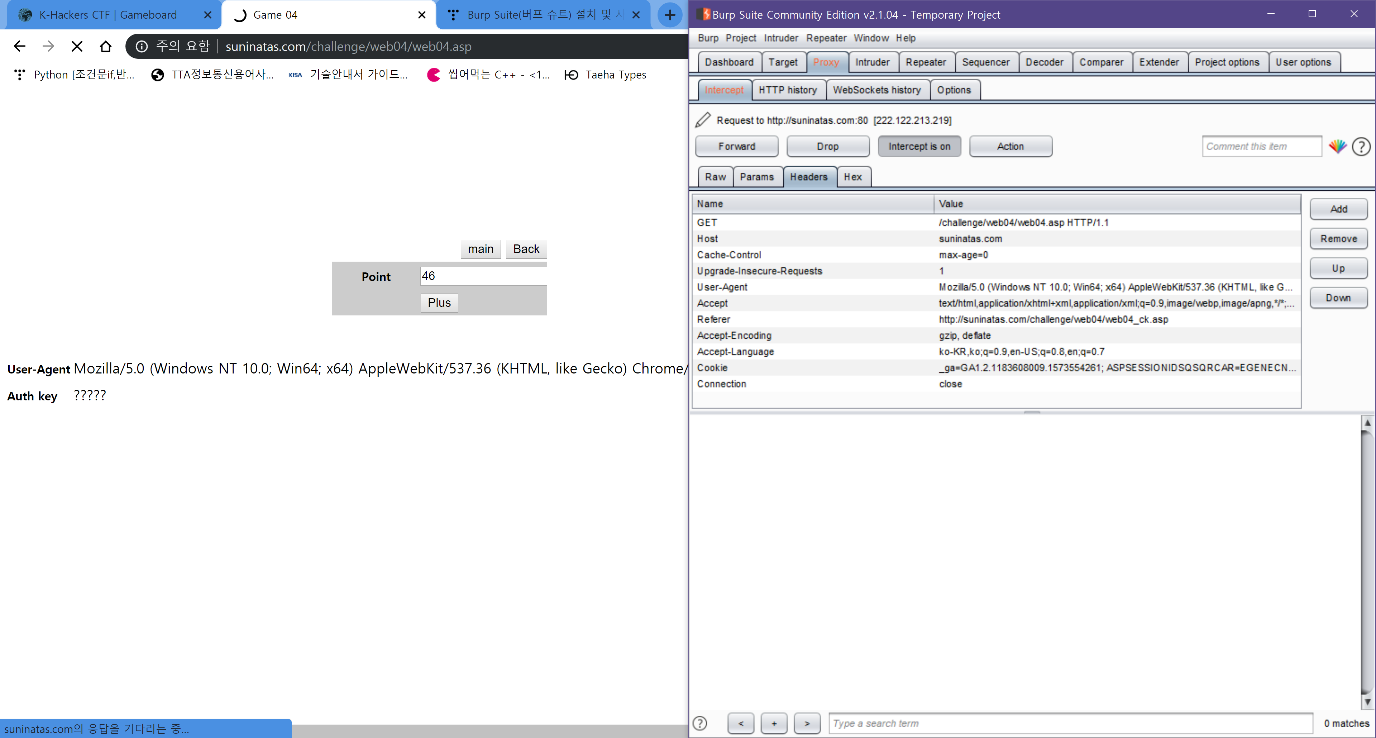
flag = chr(ord(dap[i]) ^ (i%2))

print(flag, end='')

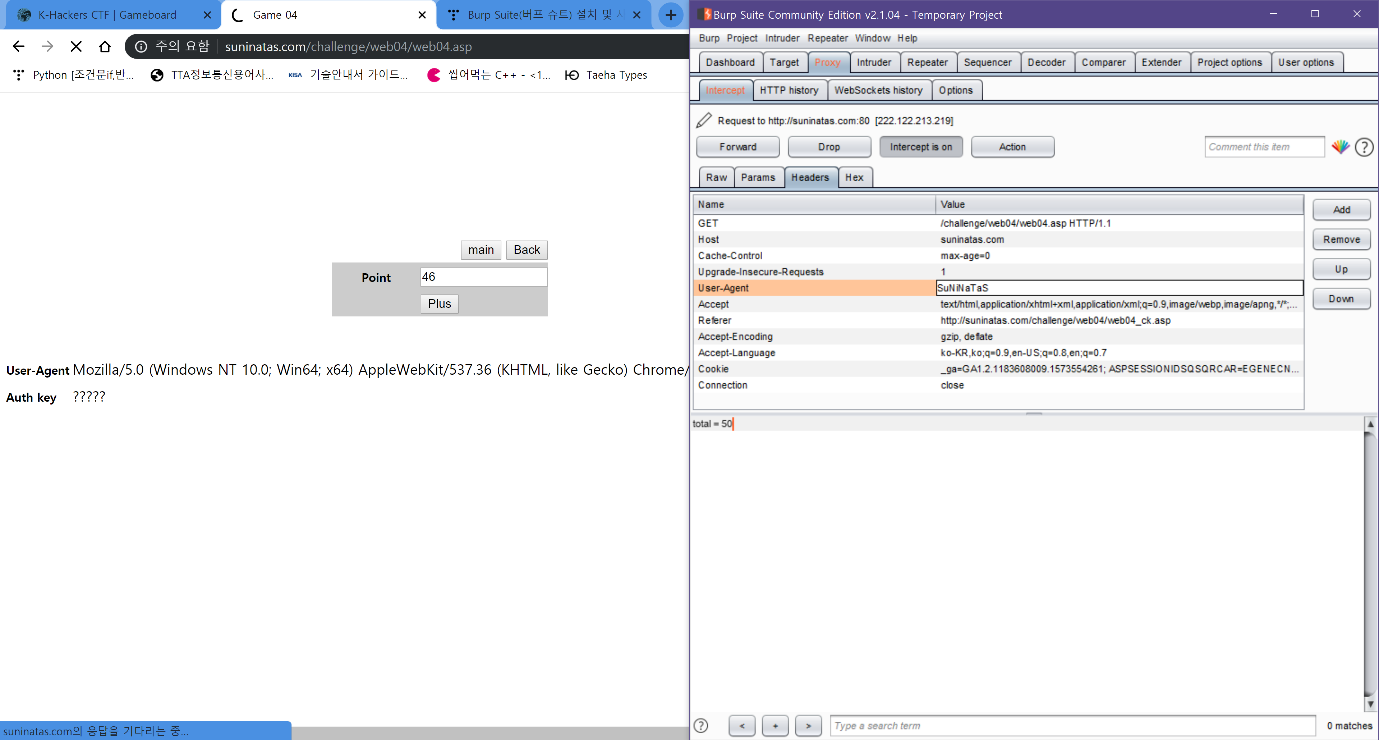
* 케냐 문제

문제: 유저 에이전트를 사용할 줄 아니?

해답: 먼저 문제를 알 수 없으니 F12로 보면 다음과 같은 힌트가 있음을 알 수가 있다.

<!-- Hint : Make your point to 50 & 'SuNiNaTaS' --> 0점부터 시작해서 50점까지 올려라. 그리고, SuNiNaTaS임을 알 수가 있는데, 밑에 유저 에이전트 값도 나와 있는 것을 보니, 먼저 유저 에이전트가 뭔 지 알아야 할 것 같다. 유저 에이전트 또는 사용자 에이전트는 사용자를 대신하여 일을 수행하는 소프트웨어 에이전트로, 대개 웹 브라우저를 말한다. 웹 페이지에 접속할 때 각 플렛폼에 맞는 페이지에 접속하기 위해 그것에 맞는 정보가 필요한데, 이 정보가 바로 사용자 에이전트라고 할 수 있는 것이다. 점수를 계속 올리다 보면 25점에서 멈추게 되고, 에코로 나는 SuNiNaTaS 브라우저가 좋다! 라는 알람을 보내는데, 그렇다면 유저 에이전트 값을 변조해서 서버로 보내게 되면 점수가 올라가지 않을까? 라고 생각이 가능하다. 패킷을 보낼 때 이를 탈취하여 정보 수정이 가능하게 도와주는 버프슈트 툴을 이용하여 유저 에이전트 값을 변조하면 점수가 올라 가는 것이다. 

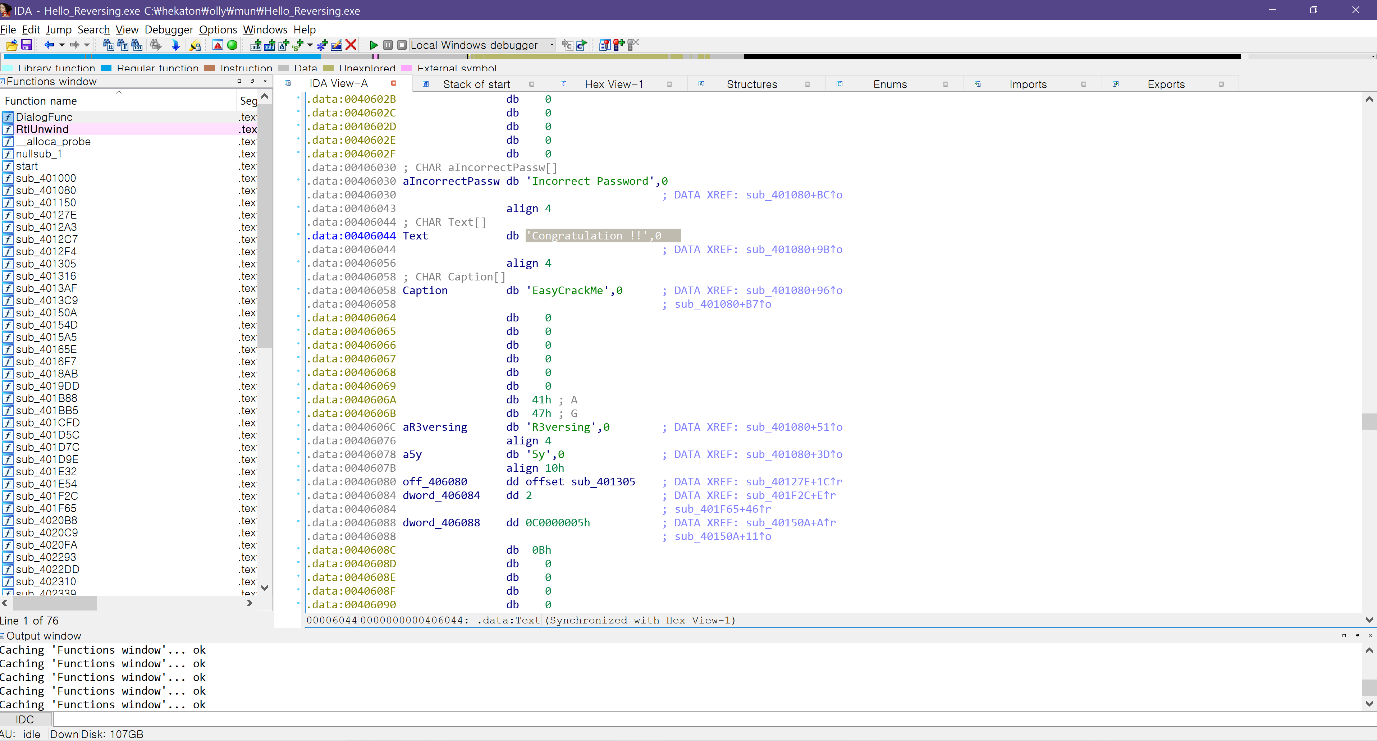
이렇게 유저 에이전트 값을



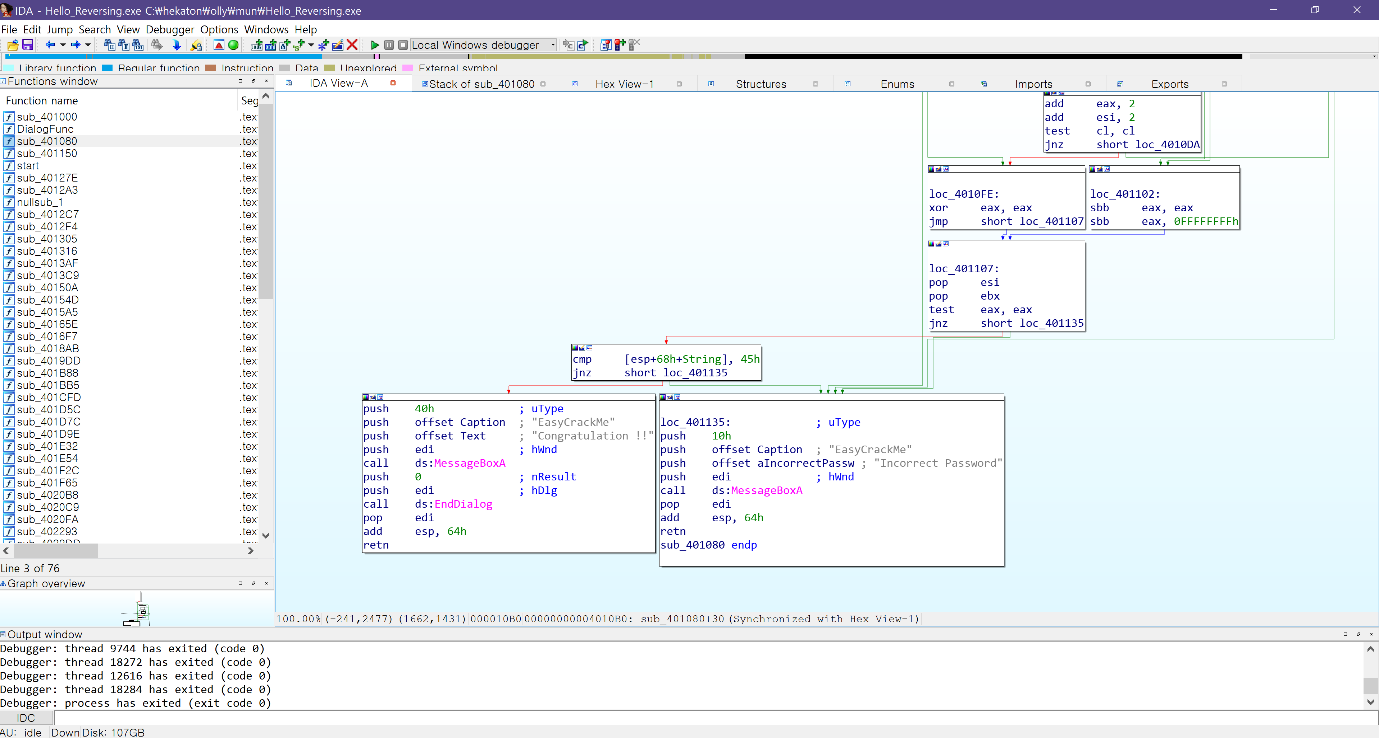
SuNiNaTaS 로 바꾸어 주고, 코드를 보면 포인트로 저장되는 값이 total이기 때문에 위의 값을 변조하여 점수를 바꾸는 것이 가능하겠지만 본인은 50까지 올렸을 때 46으로 숫자가 고정되는 것을 확인하여 멘붕이 왔었지만 동혁이형의 도움으로 이때부터 수동으로 숫자를 올려 50까지의 값을 얻어낼 수 있었다.

* 에티오피아 문제

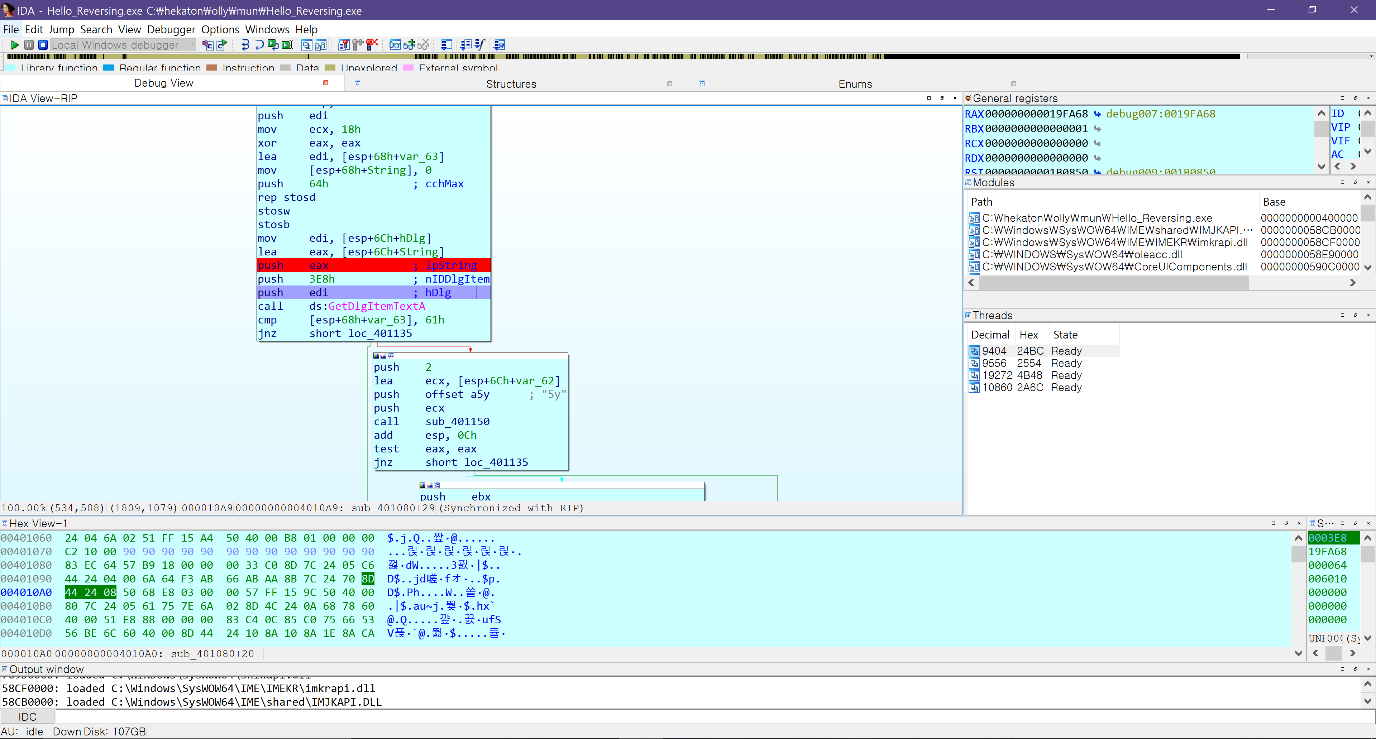
문제: 리버싱으로 일치하는 비밀번호를 찾아봐

해답: 

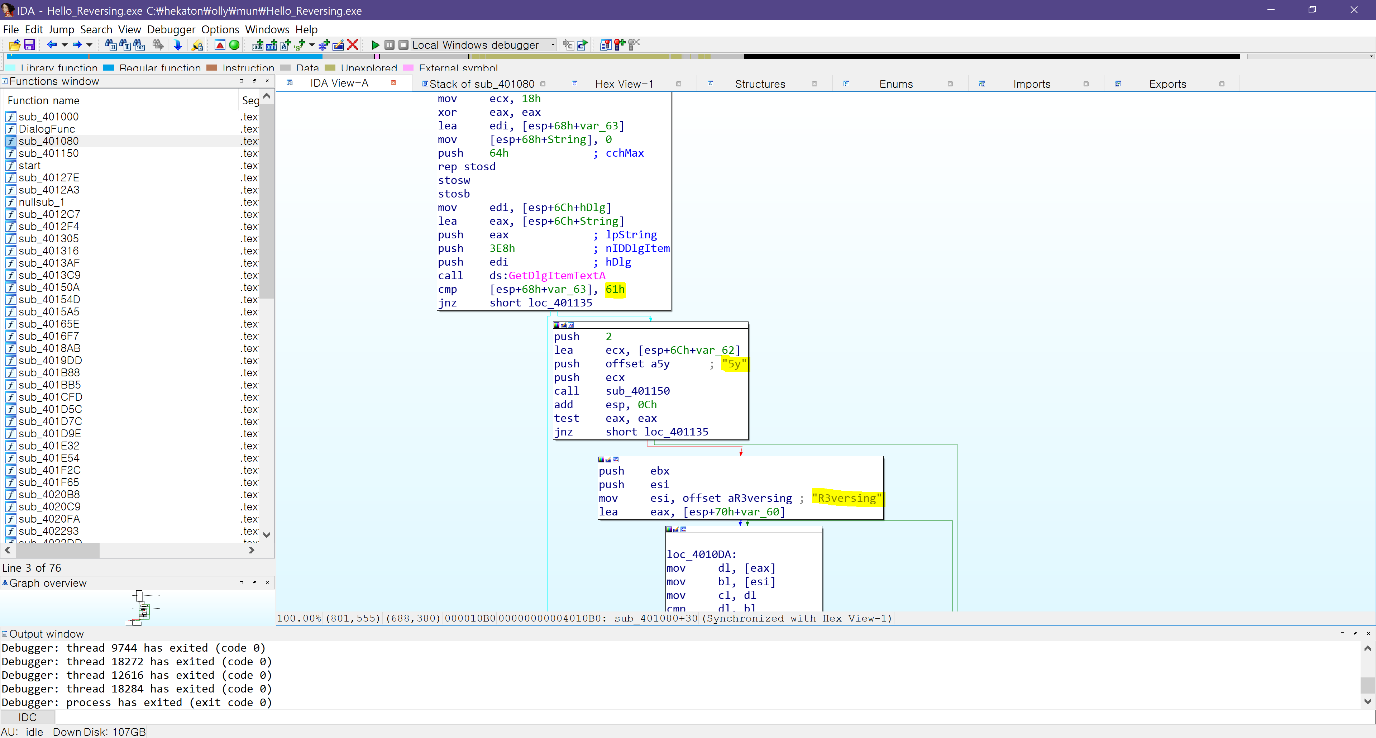
먼저 텍스트 값을 돌려보다 보니 congratulation! 이라는 문구를 발견할 수 있다. 더 자세히 들어가보자.

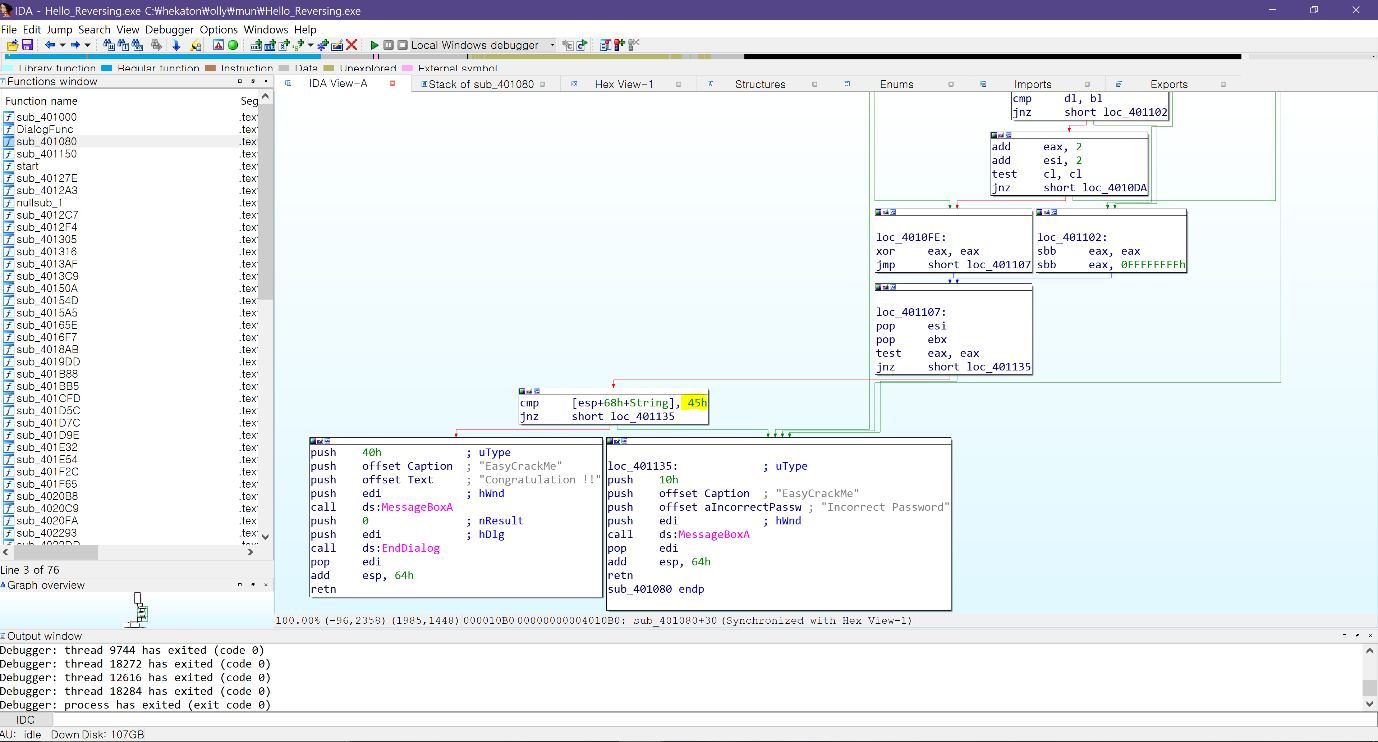


2가지 갈래길로 정답이 맞는 선택지와 틀린 선택지로 돌아가는 것을 확인할 수 있으니, 위쪽에서부터 하나씩 브레이크를 걸로 내려보며 값을 보았다.



브레이크 포인트를 걸어서 값을 확인하지 못하고 플래그값도 찾지 못해 헤매고 있다가 CTF 페이지에서 공짜 힌트를 통해 그냥 분석만 하면 된다고 하여 다시 보았는데,





다음과 같이 연결되어 있지 않은 값들이 있는 것을 확인하고 따라가 보았더니 총 4개의 값이 확인이 가능했다.  
45h , 61h, 5y, R3versing 중 값 45h와 61h 뒤에 붙은 h는 헥사테이터 즉 16진수라는 뜻이기 때문에 16진수를 10진수로 바꿔주면 45h -> 69 , 61h -> 97로 다음 값을 아스키 값으로 바꾸어 주면

순서대로 E 와 a가 되는 것을 확인 가능하다.

E, a, 5y, R3vering 으로 얻은 데이터가 바로 답이 됨을 알 수가 있다.

Ea5yR3versing