코드엔진 Basic RCE L13

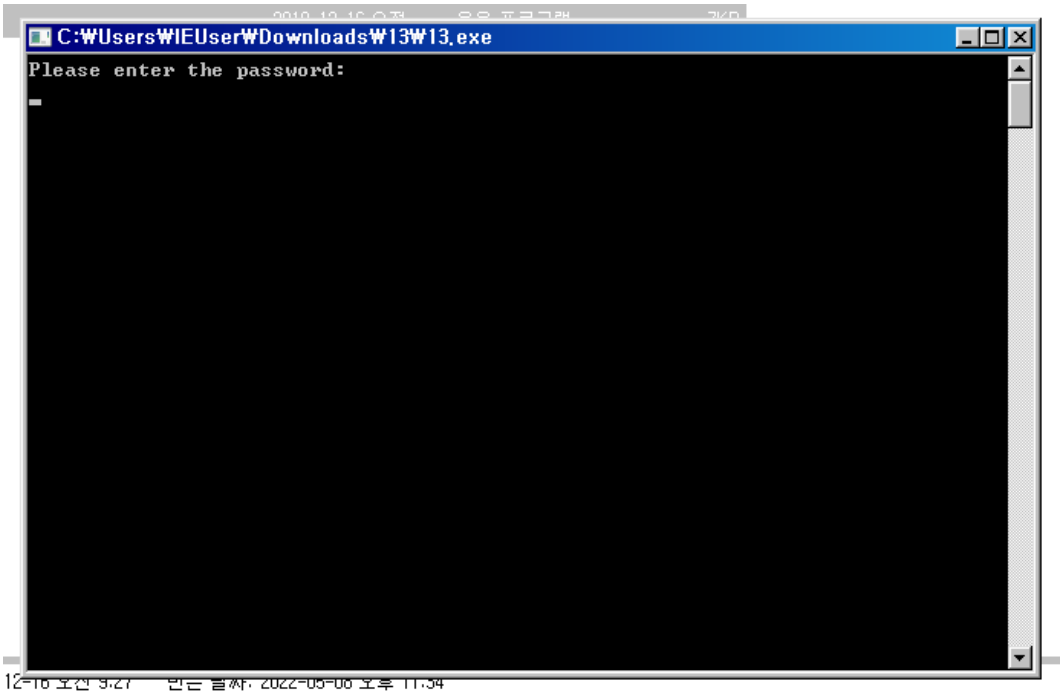
문제

> CodeEngn.com [코드엔진]
>
> 코드엔진은 국내 리버스엔지니어링 정보공유를 위해 2007년 부터 리버스엔지니어링 컨퍼런스 및 세미나, 워크숍을 현업 실무자들과 함께 운영하고 있는 비영리 커뮤니티입니다.
>
> https://ch.codeengn.com/

의 Basic RCE L13

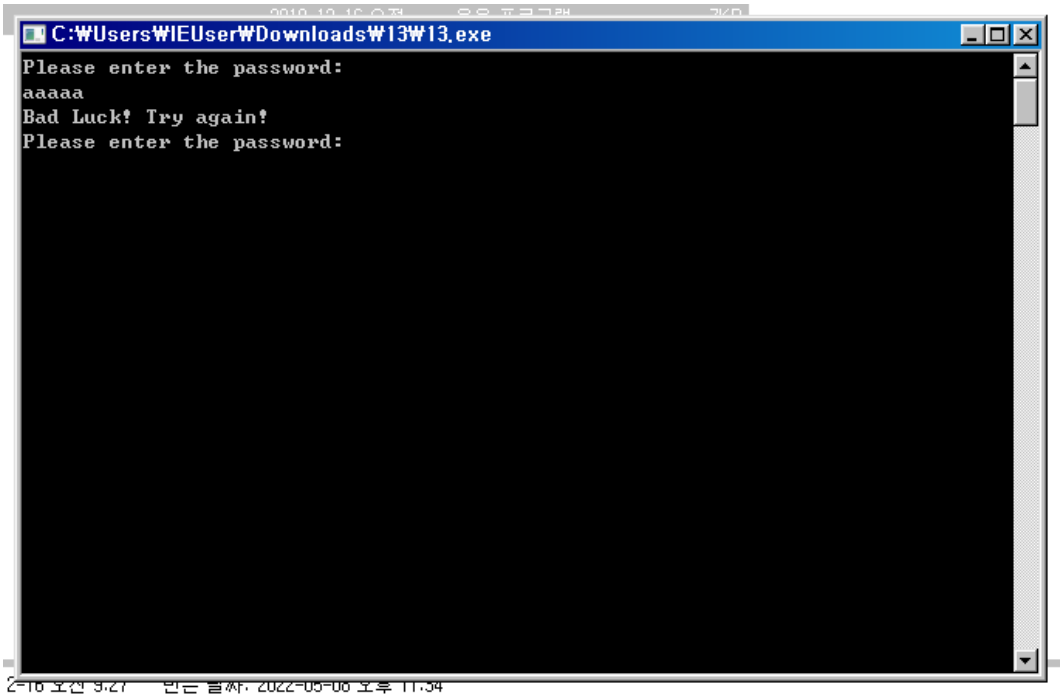
해결 과정

- 실행파일을 실행하여 어떠한 것이 나타나는지 확인



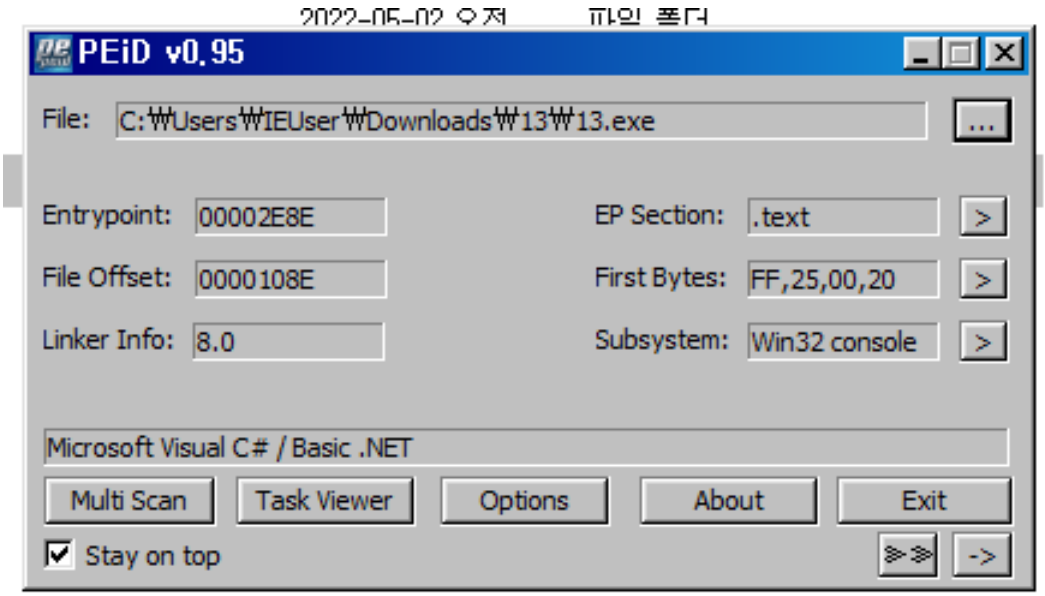
실행파일 실행 결과

- 아무 값이나 입력해 보고 어떠한 결과를 출력하는지 확인



"aaaaa"를 입력한 뒤 출력된 결과

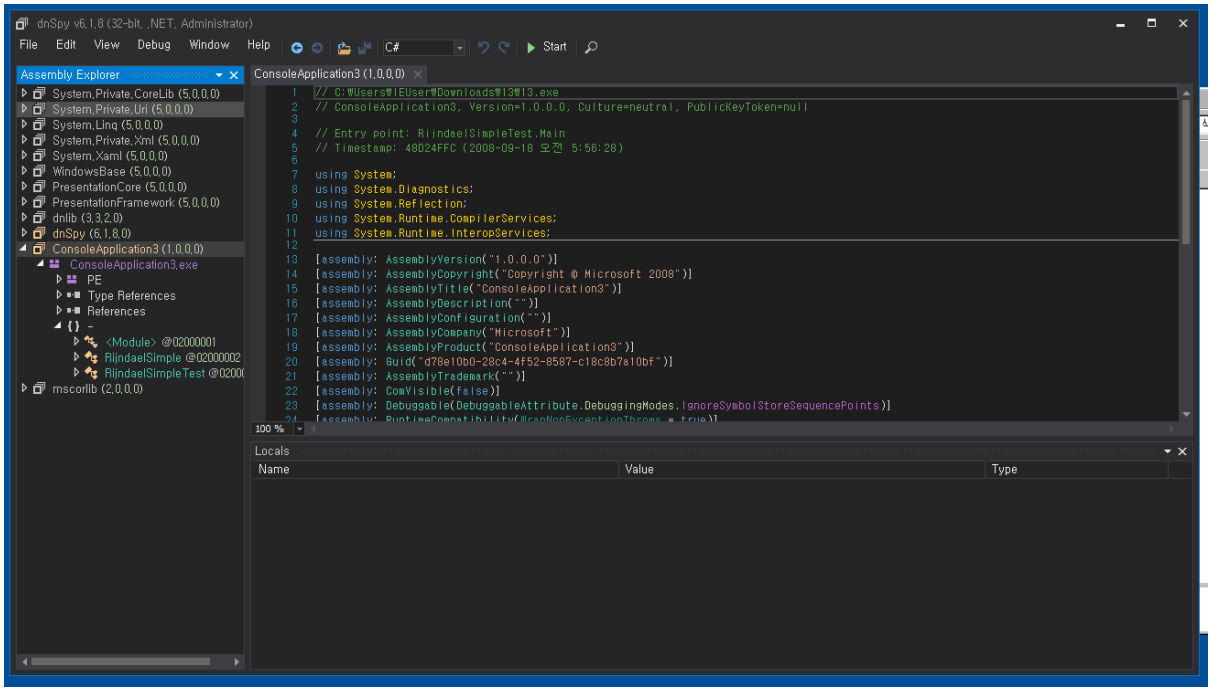
- PEiD를 통해 실행파일 분석(압축여부, 실행파일을 작성할 때 사용한 프로그래밍 언어 등)



PEiD로 실행파일을 분석한 결과

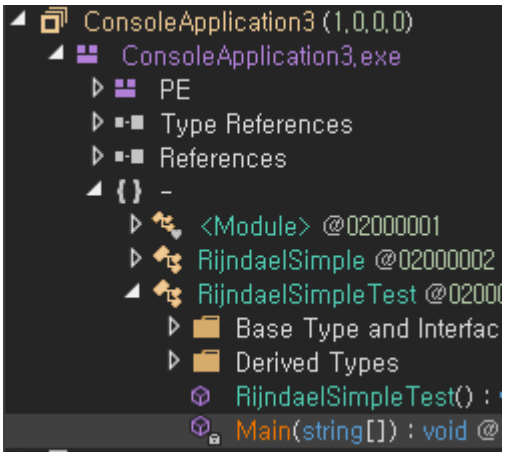
- 분석 결과, 실행 파일은 압축이 되어 있지는 않음
- 실행파일을 작성할 때 사용한 프로그래밍 언어는 C# 임을 파악
- C#은 ollyDbg로 제대로 된 분석을 수행할 수 없음

- 따라서, 다른 C#전용 디버거로 디버깅을 수행해야 함
- 이를 위한 디버거가 dnSpy라는 프로그램



dnSpy 실행 화면

- 이 디버거를 통해 실행 파일을 분석할 수 있고, 왼쪽의 박스에 있는 여러 요소들을 차례 차례 열어보면 Main 함수를 찾을 수 있음



왼쪽 박스에서 보이는 Main함수

- 이 Main함수를 클릭하여 들어가보면 Main함수에서 실행되는 코드들이 나오고 Main함수에서 어떠한 값을 입력값과 비교하는지 알아낼 수 있음

```
// RijndaelSimpleTest
// Token: 0x06000004 RID: 4 RVA: 0x000021B4 File Offset: 0x000003B4
[STAThread]
private static void Main(string[] args)
{
    string text = "";
    string cipherText = "BnCxGiN4aJDE+qUe2ylm8Q==";
    string passPhrase = "^F79ejk56$£";
    string saltValue = "DHj47&+)$h";
    string hashAlgorithm = "MD5";
    int passwordIterations = 1024;
    string initVector = "&!£$%^&+()CvHgE!";
    int keySize = 256;
    RijndaelSimple.Encrypt(text, passPhrase, saltValue, hashAlgorithm, passwordIterations, initVector, keySize);
    text = RijndaelSimple.Decrypt(cipherText, passPhrase, saltValue, hashAlgorithm, passwordIterations, initVector, keySize);
    for (;;)
    {
        Console.WriteLine("Please enter the password: ");
        string a = Console.ReadLine();
        if (a == text)
        {
            break;
        }
        Console.WriteLine("Bad Luck! Try again!");
    }
    Console.WriteLine("Well Done! You cracked it!");
    Console.ReadLine();
```

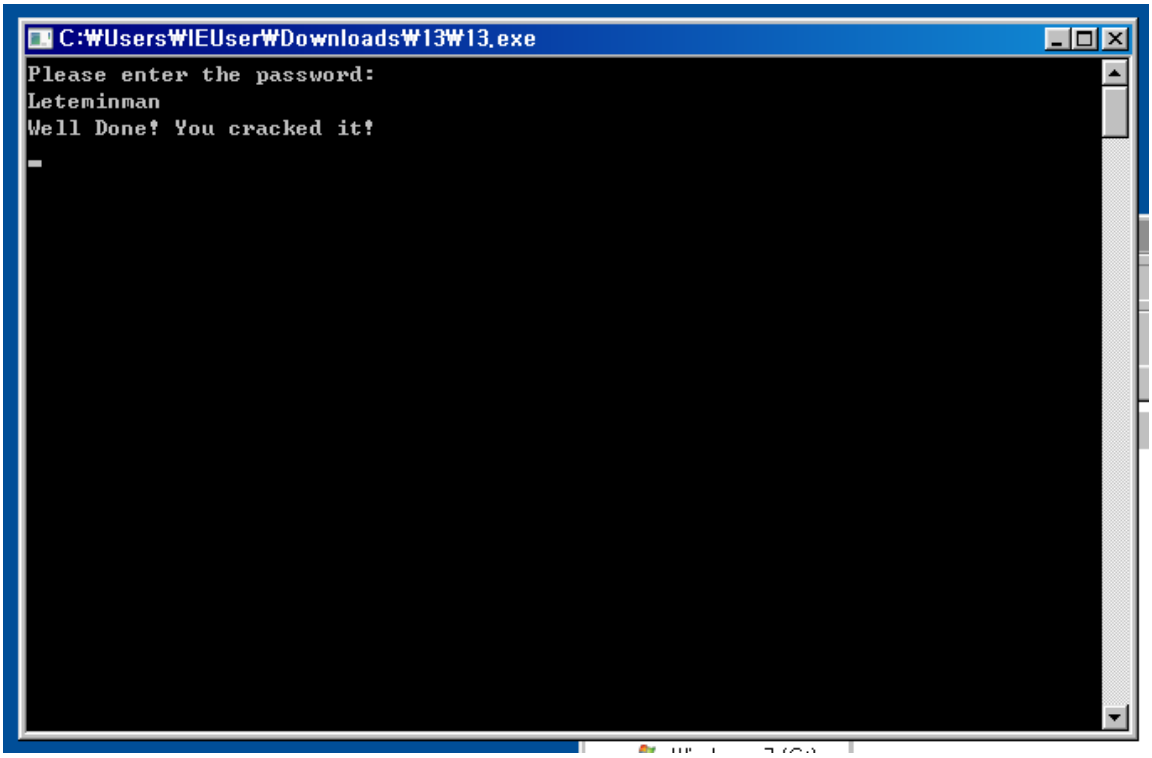
Main함수의 코드

- Main함수의 코드를 보면 입력값(변수 a)을 text라는 변수에 저장된 값과 비교하고 있음
- 그렇다면, 입력값과 text변수의 값을 비교하기 직전에 브레이크 포인트를 걸고 text 변수에 어떠한 값이 들어가있는지 확인하면 정답 입력값을 알아낼 수 있음

args	{string[0x00000000]}	string[]
text	"Leteminman"	string

text변수에 어떤 값이 들어가있는지 디버거를 통해 확인 가능

- 디버거를 통해 text 변수에 Leteminman이라는 값이 들어가 있는 것을 확인했으므로 정답 입력값이 Leteminman이라는 것을 알 수 있음
- 실제 Leteminman을 입력한 결과 정답을 입력했다는 결과가 출력되었음



Leteminman을 패스워드로 입력한 결과

- 따라서 Leteminman이 정답 입력값임을 알 수 있음