REPORT:

코드엔진 Basic RCE 13 Writeup

COLONY 1824275 정상지

정답은 무엇인가?

프로그램 이외에 아무것도 주어지지 않은 상태로 문제를 접했다

PEID vo		oute accommo		×
File: C:₩L	Jsers₩lg₩Desktop₩'&	지₩Reversing₩코드엔	진₩13.exe	
Entrypoint:	00002E8E	EP Section:	.text	>
File Offset:	0000108E	First Bytes:	FF,25,00,20	>
Linker Info:	8.0	Subsystem:	Win32 console	>
Microsoft Vi	sual C# / Basic .NET			
<u>M</u> ulti Scan	Task Viewer	Options Abo	out E <u>x</u>	it
✓ <u>S</u> tay on	top		**	->

해당 파일은 C#으로 만들어진 프로그램인 것을 알 수 있다

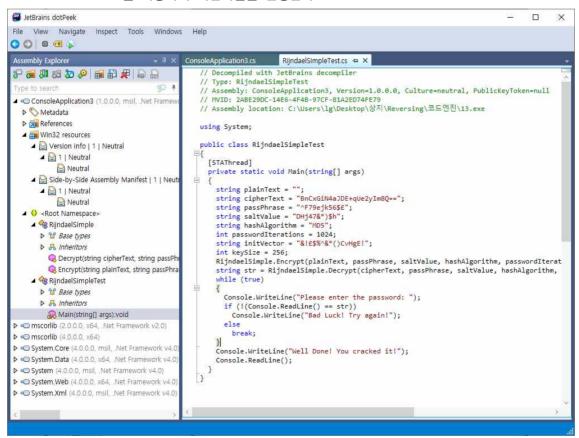


디버깅 없이 프로그램을 동작시켰을 때 위와 같은 콘솔창이 나오는 것을 보았으며, password입력을 필요로 하고 있다



아무 키나 입력하였을 때 Bad Luck! Try again! 이라는 메시지가 출력되었다

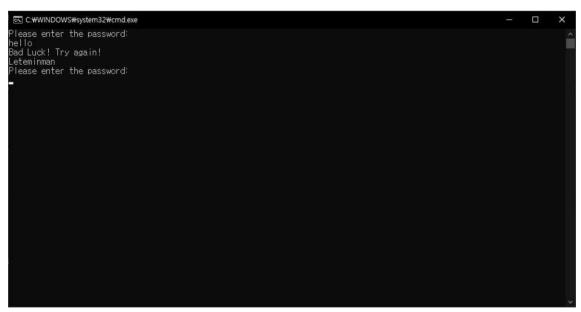
JetBrains dotPeek을 이용하여 디컴파일을 진행한다



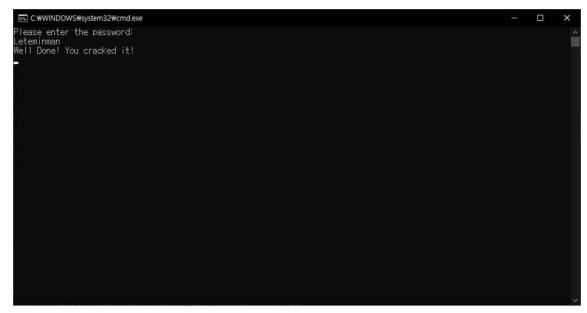
해당 디컴파일 코드에서 확인해본 결과 문자열 str과 비교하여 콘솔창에 결과를 알려준다

```
JetBrains dotPeek
                                                                                                                                                                                                   X
File View Navigate Inspect Tools Windows Help
G 6 0 0 0
Assembly Explorer
                                                                               RijndaelSimpleTest.cs ⇔ X
                                                  → <sup>1</sup> × 13 csproi
mniled with letBrains de
                                                                   // Dyce: RijndaelSimpleTest
// Assembly: ConsoleApplication3, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null
// MVID: 2ABE29DC-14E6-4F48-97CF-81A2ED74FE79
 ■ 13.csproj (assembly; ConsoleApplication3, 1.0.0.
                                                                   // Assembly location: C:\Users\lg\Desktop\상지\Reversing\코드엔진\13.exe
      AssemblyInfo.cs
      RijndaelSimple.cs
                                                                   using System:
      RijndaelSimpleTest.cs
                                                                public class RijndaelSimpleTest
무{
 ConsoleApplication3 (1.0.0.0, msil, .Net Frame
▶ corlib (2.0.0.0, x64, .Net Framework v2.0)
                                                                     [STAThread]
private static void Main(string[] args)
{
▶ • mscorlib (4.0.0.0, x64)
▶ System.Core (4.0.0.0, msil, .Net Framework v4.0
                                                                        string plainText = "";
string cipherText = "BnCxGiN4aJDE+qUe2yIm8Q==";
string passPhrase = "~F79ejk565£";
string satIvalue = "Dhj472&")$h";
string hashAlgorithm = "MD5";
int passwordIterations = 1024;
string initVector = "%1E$%~&"()CvHgE!";
int keySize = 256;
▶ C System.Data (4.0.0.0, x64, .Net Framework v4.0
> System (4.0.0.0, msil, .Net Framework v4.0)
▶ C System.Web (4.0.0.0, x64, .Net Framework v4.0
▶ «☐ System.Xml (4.0.0.0, msil, .Net Framework v4.0)
                                                                        RijndaelSimple.Encrypt(plainText, passPhrase, saltValue, hashAlgorithm, passwordIterations, i string str = RijndaelSimple.Decrypt(cipherText, passPhrase, saltValue, hashAlgorithm, passworwhile (true)
                                                                           Console.WriteLine("Please enter the password: ");
   if (!(Console.ReadLine() == str))
                                                                                         Console.WriteLine("Bad Luck! Try again!");
Console.WriteLine(str);
                                                                                   else
                                                                        Console.WriteLine("Well Done! You cracked it!");
                                                                        Console.ReadLine();
```

Visual Studio를 이용하여 해당 파일에 소스코드를 수정한다



아무런 키 값을 입력할 때 정답을 출력한다



해당 정답을 입력하니 Well Done! You cracked it!이라는 문자열이 출력되는 것을 확인했다

정답: Leteminman