Pwn2Win 2016

Crypto Simple Cryptography(crypto 60) Write Up

Author : hideroot(M.O.K)

Data : 9/29 2017

암호화된 스트링(flag)는 다음과 같다.

```
GA3TCYZRGU2DKXZXG5PTENZTHAZDSXZQHEYTKMJUGBSV6
MBXGFSF6MTDGIYTGYJSMMZTIM3FL4YDOMLCL42GENJRGU2
TIOBVGQ2WIXZRGBPTAZQ=
```

마지막의 문자가 =로 끝나는 걸로 봐서는 base64로 Encoding이 되어 있는 걸로 보인다.

Base64 Decoding을 해보자.

```
₩x18
        ₩x86Q₩x19M₩x83)vW₩x1b₩x93èΦ₩x1c₩x06CIvP₩x1cF₩x13(T
₩x18₩x14₩x95迭₩x18T₩x85酃₩x18₩x86₩x13₩x19₩x82R0œ
/₩x86₩x038Â/₩x8d₩x86₩x10ë₩x19M₩x93 □₩x96!vQ₩x18₩x13c₩x94
```

Base64로 디코딩을 했더니 깨져서 출력이 된다. 의심이 가는건 =로 끝났을 때 생각해볼수 있는 Crypto로는 base 시리즈와 base처럼 보이게 하는 Crypto로 생각해볼수 있다. 일단 Base 시리즈로 돌려보았다.

Base32 Decode

071c1545_77_273829_0915140e_071d_2c213a2c343e_071b_4b515548545d_10_0f

한번만에 성공했다. 이제야 좀 암호화 중간단계의 Text로 보인다. 보아하니 Single XOR 기법을 사용한것 같다. (Simple 이라니까 어려운건 사용하지 않았을 거라 생각해서 Single XOR 이겠지 했는데 맞았다)

Script를 짜서 돌려보자

플래그는 CTF-BR{}로 시작하므로 이에 해당하는 값을 찾아보면 되겠다. (Script 첨부)

CTF-BR{This_encryption_is_crazy_bro!_Thinking_different...}