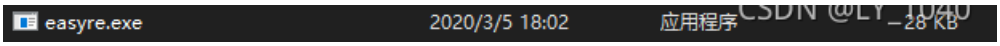
LY的ctf练习———[ACTF新生赛2020]easyre

原创

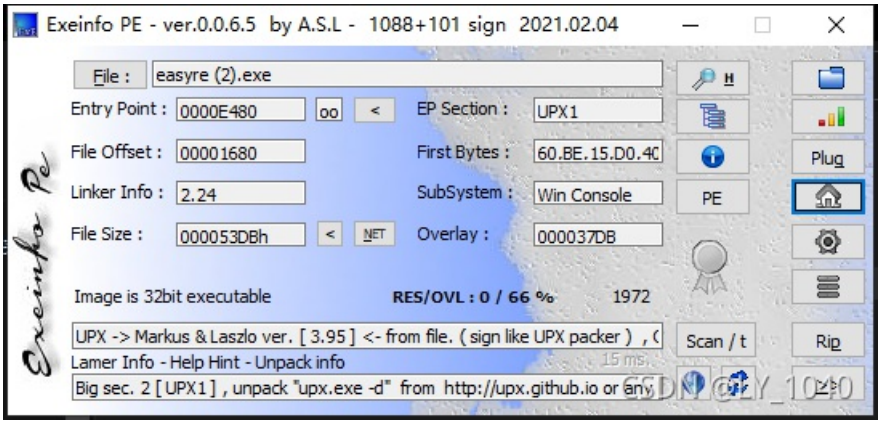
LY1040 于 2021-11-25 16:26:53 发布 35 收藏
文章标签： 安全

本文链接：https://blog.csdn.net/LY_1040/article/details/121539941

题目给出一个压缩包，解压后得到



那么先检查是否加壳



发现套了一个upx壳，3.95版本，找个工具解壳之后丢进ida

```
__main();
qmemcpy(v4, "*F'\"N,\"(I?+@", sizeof(v4));
printf("Please input:");
scanf("%s", v6);
if ( v6[0] != 65 || v6[1] != 67 || v6[2] != 84 || v6[3] != 70 || v6[4] != 123 || v10 != 125 )
  return 0;
v5[0] = v7;
v5[1] = v8;
v5[2] = v9;
for ( i = 0; i <= 11; ++i )
{
  if ( v4[i] != _data_start__[*((char *)v5 + i) - 1] )// 从这些里面找
                                                      // '7eh'}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>=<;:9876543210/.-,+*)('&%$# !"
    return 0;
}
```


发现大概逻辑就是从_data_start给出的内一长串字符串中找出与v4对应的位置，即为flag-1

直接上脚本

```
#include<iostream>
#include<cstring>
using namespace std;
int main()
{
 string s = "z}|{zyxwvutsrqponmlkjihgfedcba`_^]\\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>=<;:9876543210/.-,+*)('&%$#
 string v4 = "*F'\"N,\"(I?+@";
 for(int i = 0; i < v4.length() ; i++ )
 {
     for(int j = 0 ; j < s.length() ; j++ )
     {
         if(v4[i]==s[j])
         {
             cout<<char(j+1);
         }
     }
 }
}
```

得到flag：

flag{U9X_1S_W6@T?}