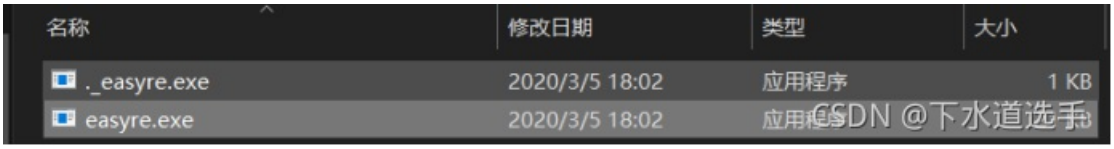
# buuctf_easyre

原创

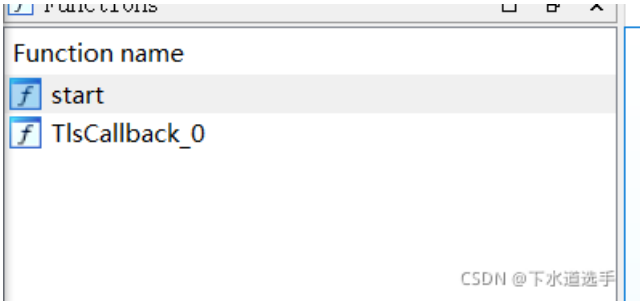
下水道选手 于 2021-09-19 23:23:31 发布 146 收藏
文章标签： unctf


**[ACTF新生赛2020]easyre**

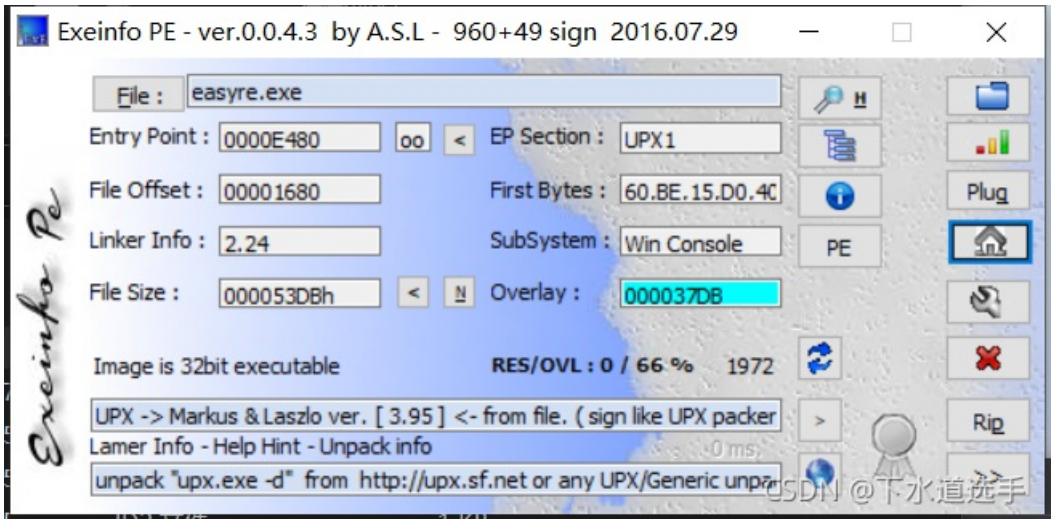

下载附件解压得到两个exe文件




第一个只有1kb大小，双击打开说不适用于我的电脑版本，拖进010看一下，发现是Mac OS X的exe文件，既然是水果的那就没事了，看下一个，第二个让输入，咱不清楚输入啥，先拖进ida看看，发现只有两个函数，应该是加壳了




那咱就来查一下壳




普通的UPX壳，32位

用Qunpackchs去壳（失败了，不知道为啥）换OllyDBG，发现我不会用

直接找了个万能去壳工具，一键去壳


将去壳后的文件拖进ida，上来直接找到main函数，直接反编译main函数

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  _BYTE v4[12]; // [esp+12h] [ebp-2Eh] BYREF
  _DWORD v5[3]; // [esp+1Eh] [ebp-22h]
  _BYTE v6[5]; // [esp+2Ah] [ebp-16h] BYREF
  int v7; // [esp+2Fh] [ebp-11h]
  int v8; // [esp+33h] [ebp-Dh]
  int v9; // [esp+37h] [ebp-9h]
  char v10; // [esp+3Bh] [ebp-5h]
  int i; // [esp+3Ch] [ebp-4h]

  sub_401A10();
  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] != byte_402000[*((char *)v5 + i) - 1] )
      return 0;
  }
  printf("You are correct!");
  return 0;
}
```



```
byte_402000     db 7Eh                  ; DATA XREF: _main+EC↑r
aZyxwvutsrqponm db '}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>='
                db '<;:9876543210/.-,+*)(',27h,'&%$# !"',0
                align 40h
```



发现这个v4字符串和第二个for有点东西，跟进查看

是字符串，那应该就是用for循环在这个字符串里面查找v4的字符，方法是字符串的字符下标-1等于v4字符的ASCII码值

那拿v4来逆变换应该就能得到flag了

上脚本

```
#include"bits/stdc++.h"
using namespace std;
int main() {
    char v5[]="~}|{zyxwvutsrqponmlkjihgfedcba`_^]\\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>=<;:9876543210/.-,+*)('&%$# !\"";
    //char v4[]={'*','F','\'','"','N',',','"','(','I','?','+','@'};
    char v4[]="*F'\"N,\"(I?+@";
    char flag[strlen(v4)];
    for(int i=0; i<strlen(v4); i++) {
        for (int j=0; j<strlen(v5); j++) {
            if(v4[i]==v5[j])
                flag[i]=char(j+1);
        }
    }
    cout<<flag;
//  for(int i=0;i<12;i++){
//      printf("%c",flag[i]);
//  }
}
```



脚本要注意的是字符串这里'\'和双引号前要加转义符，7Eh和27h要转成字符。

运行脚本，得flag

```
U9X_1S_W6@T?
--------------------------------

Process exited after 0.01784 seconds with return
```

包上flag{}提交即可