BUUCTF Reverse [BJDCTF2020]JustRE WriteUp

原创

PlumpBoy 于 2021-09-11 16:14:10 发布 27 收藏

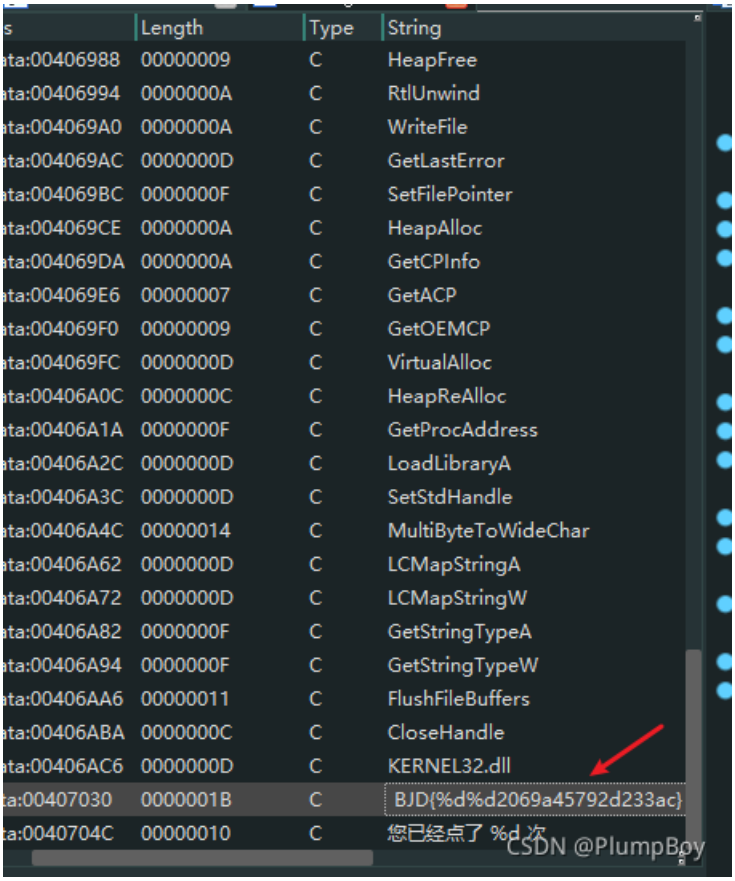
分类专栏： BUUCTF 逆向题解 文章标签： 系统安全 安全

本文链接：https://blog.csdn.net/weixin_45723661/article/details/120228013

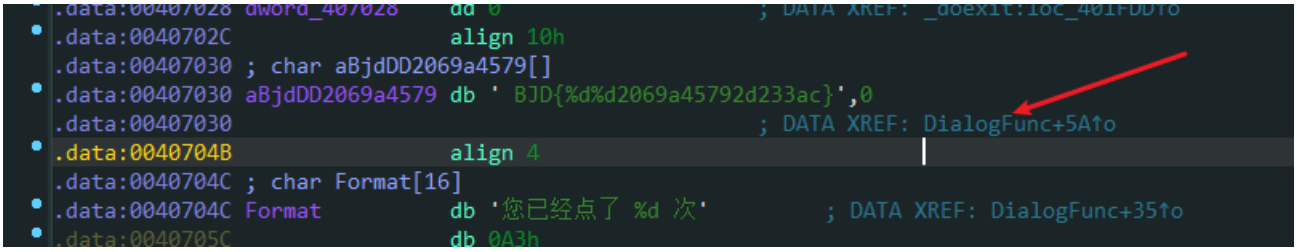
JustRE-WP

首先打开看看，发现有个getflag标签，点击会显示现在点了多少次。

拖入IDA中，按shift+F12查看字符串，发现一个很像flag的值



双击转到地点，再双击转到汇编窗口



再按F5显示反汇编代码

```
INT_PTR __stdcall DialogFunc(HWND hWnd, UINT a2, WPARAM a3, LPARAM a4)
{
  CHAR String[100]; // [esp+0h] [ebp-64h] BYREF

  if ( a2 != 272 )
  {
    if ( a2 != 273 )
      return 0;
    if ( (_WORD)a3 != 1 && (_WORD)a3 != 2 )
    {
      sprintf(String, Format, ++dword_4099F0);
      if ( dword_4099F0 == 19999 )
      {
        sprintf(String, " BJD{%d%d2069a45792d233ac}", 19999, 0);
        SetWindowTextA(hWnd, String);
        return 0;
      }
      SetWindowTextA(hWnd, String);
      return 0;
    }
    EndDialog(hWnd, (unsigned __int16)a3);
  }
  return 1;
}
```

发现输出的值应该是`BJD{1999902069a45792d233ac}`，改为`flag{1999902069a45792d233ac}`提交成功。

tip：虽然题目写出来了，但是搞点好玩的，这个19999结合之前的界面判断应该是点击19999次出现flag，用CE找到目标地址，修改后发现确实是这样。