

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[BUUCTF 逆向题解](#) 专栏收录该内容

18 篇文章 1 订阅

订阅专栏

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

Address	Length	Type	String
ata:00406988	00000009	C	HeapFree
ata:00406994	0000000A	C	RtlUnwind
ata:004069A0	0000000A	C	WriteFile
ata:004069AC	0000000D	C	GetLastError
ata:004069BC	0000000F	C	SetFilePointer
ata:004069CE	0000000A	C	HeapAlloc
ata:004069DA	0000000A	C	GetCPIInfo
ata:004069E6	00000007	C	GetACP
ata:004069F0	00000009	C	GetOEMCP
ata:004069FC	0000000D	C	VirtualAlloc
ata:00406A0C	0000000C	C	HeapReAlloc
ata:00406A1A	0000000F	C	GetProcAddress
ata:00406A2C	0000000D	C	LoadLibraryA
ata:00406A3C	0000000D	C	SetStdHandle
ata:00406A4C	00000014	C	MultiByteToWideChar
ata:00406A62	0000000D	C	LCMapStringA
ata:00406A72	0000000D	C	LCMapStringW
ata:00406A82	0000000F	C	GetStringTypeA
ata:00406A94	0000000F	C	GetStringTypeW
ata:00406AA6	00000011	C	FlushFileBuffers
ata:00406ABA	0000000C	C	CloseHandle
ata:00406AC6	0000000D	C	KERNEL32.dll
ata:00407030	0000001B	C	BJD{%d%d2069a45792d233ac}
ata:0040704C	00000010	C	您已经点了 %d 次

双击转到地点，再双击转到汇编窗口

```

.data:00407028 dwWord_407028 dd 0 ; DATA XREF: _doexit:10c_401fdd10
.data:0040702C align 10h
.data:00407030 ; char aBjdDD2069a4579[]
.data:00407030 aBjdDD2069a4579 db 'BJD{%d%d2069a45792d233ac}',0
.data:00407030 ; DATA XREF: DialogFunc+5Afo
.data:0040704B align 4
.data:0040704C ; char Format[16]
.data:0040704C Format db '您已经点了 %d 次' ; DATA XREF: DialogFunc+35fo
.data:0040705C db 0A3h

```

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。

