

[BUUCTF]REVERSE解题记录 [ACTF新生赛2020]easyre

原创

警臣 于 2022-02-27 21:40:59 发布 133 收藏

文章标签: [网络安全](#)

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_44192213/article/details/123170994

版权

1.查壳, 发现upx壳, 先脱壳, 再放进32位ida中

```
__main();
v4 = 42;
v5 = 70;
v6 = 39;
v7 = 34;
v8 = 78;
v9 = 44;
v10 = 34;
v11 = 40;
v12 = 73;
v13 = 63;
v14 = 43;
v15 = 64;
printf("Please input:");
scanf("%s", &v19);
if ( (_BYTE)v19 == 65 && HIBYTE(v19) == 67 && v20 == 84 && v21 == 70 && v22 == 123 && v26 == 125 )
{
    v16 = v23;
    v17 = v24;
    v18 = v25;
    for ( i = 0; i <= 11; ++i )
    {
        if ( *(&v4 + i) != _data_start__[*((_BYTE *)&v16 + i) - 1] )
            return 0;
    }
    printf("You are correct!");
    result = 0;
}
else
{
    result = 0;
}
return result;
}
```

2.可以看出v4的值是 `_data_start` 数组中每一位-1得到的。可以看到 `_data_start` 的值是

```
.data:00402001 azyxwvutsrqponm db '{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA?@'
.data:00402001 db '<.:9876543210/.-,*)(',27h,'&$$# !"',0
```

```
main.py
C:\Users\Administrator\PycharmProjects
flag{U9X_1S_W6@T?}
Process finished with exit code 0
```

编写脚本可以得到结果:

所以答案是flag{U9X_1S_W6@T?}