CTF题目部分解析

原创

阿峰啊啊啊 于 2021-05-24 18:08:01 发布 1635 收藏 2

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_56817426/article/details/117225939

一、题目一：exe逆向

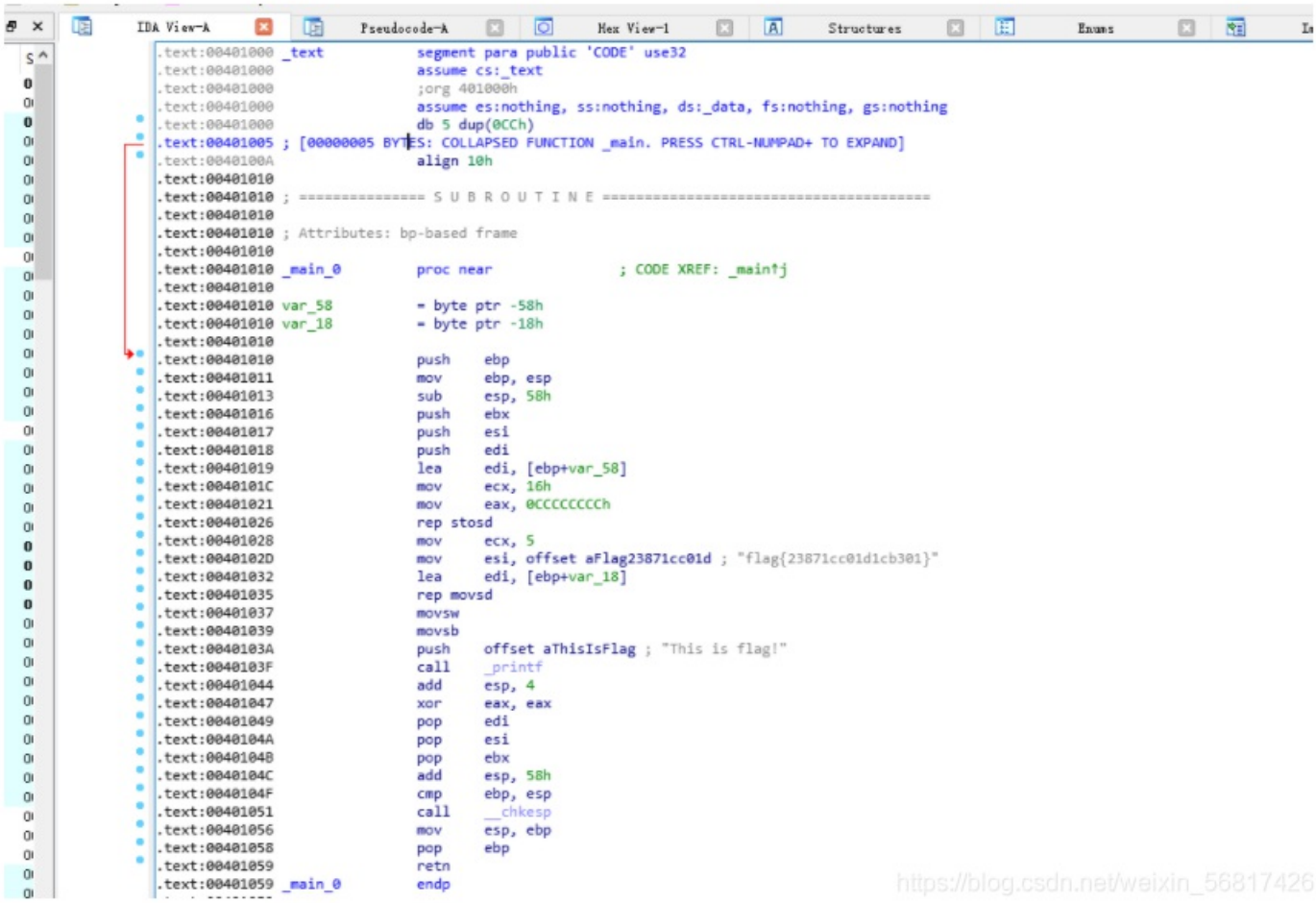
二、读题

描述：我们获得了敌方某个exe文件，尝试逆向这个exe文件，获得里面的flag{字符串}，以SeBaFi{}的形式提交字符串。

三、审题

找到隐藏在exe中的flag。

IDA打开该文件。就能得到flag。



一、题目二：看本质

二、读题

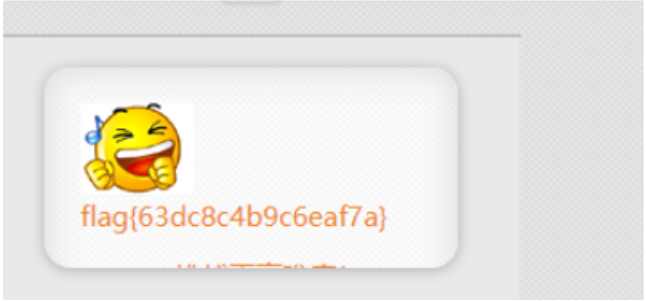
描述：在渗透过程中，我们要透过现象，看本质。

三、审题

第一步：打开给出的网页发现是一个扫雷游戏，但是无论选择那种难度游戏开始后都是困难。

```
//游戏结束
function GameOver(num) {
    gameState = false;
    if (num == 0) {
        $('text').style.display = 'block';
        $('Difficu').style.display = 'none';
        $('text').getElementsByTagName('img')[0].src = 'images/defeat
        $('text').getElementsByTagName('p')[0].innerHTML = '呀！踩到炸
        $('butt').innerHTML = '再来一次！';
    } else if (num == 1) {
        $('text').style.display = 'block';
        $('Difficu').style.display = 'none';
        $('text').getElementsByTagName('img')[0].src = 'images/victor
        if(formTime<120)
        {
            eval(function(d,f,a,c,b,e){b=function(a){return a.toStrin
32,32,"  text getElementsByTagName innerHTML style display if none gi
        }
        else
        {
            $('text').getElementsByTagName('p')[0].innerHTML = '居然只
        }
        $('butt').innerHTML = '挑战更高难度！';
    }
    $('hint').className = 'animati2';
}
```


通过代码分析发现当GameOver（）的参数为1时，游戏胜利，所以我们直接到Console中去执行ver（1），获得Flag。



一、题目三：apk逆向1

> 实训描述：　我们截获了个apk，请反编译这个apk，获得里面的flag{字符串}，并以SeBaFi{}的形式提交该字符串。

二、读题

找到隐藏在apk中的flag。

三、审题

Jadx打开apk，查看得到答案 flag{01E5DFFFC37E7C21}，根据题目要求提交flag：SeBaFi{01E5DFFFC37E7C21}。

```
25
        } else {
27          Toast.makeText(MainActivity.this, "password error", 0).show();
```