




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](#)

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_56817426/article/details/117225939

版权



[CTF 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

一、题目一: exe逆向

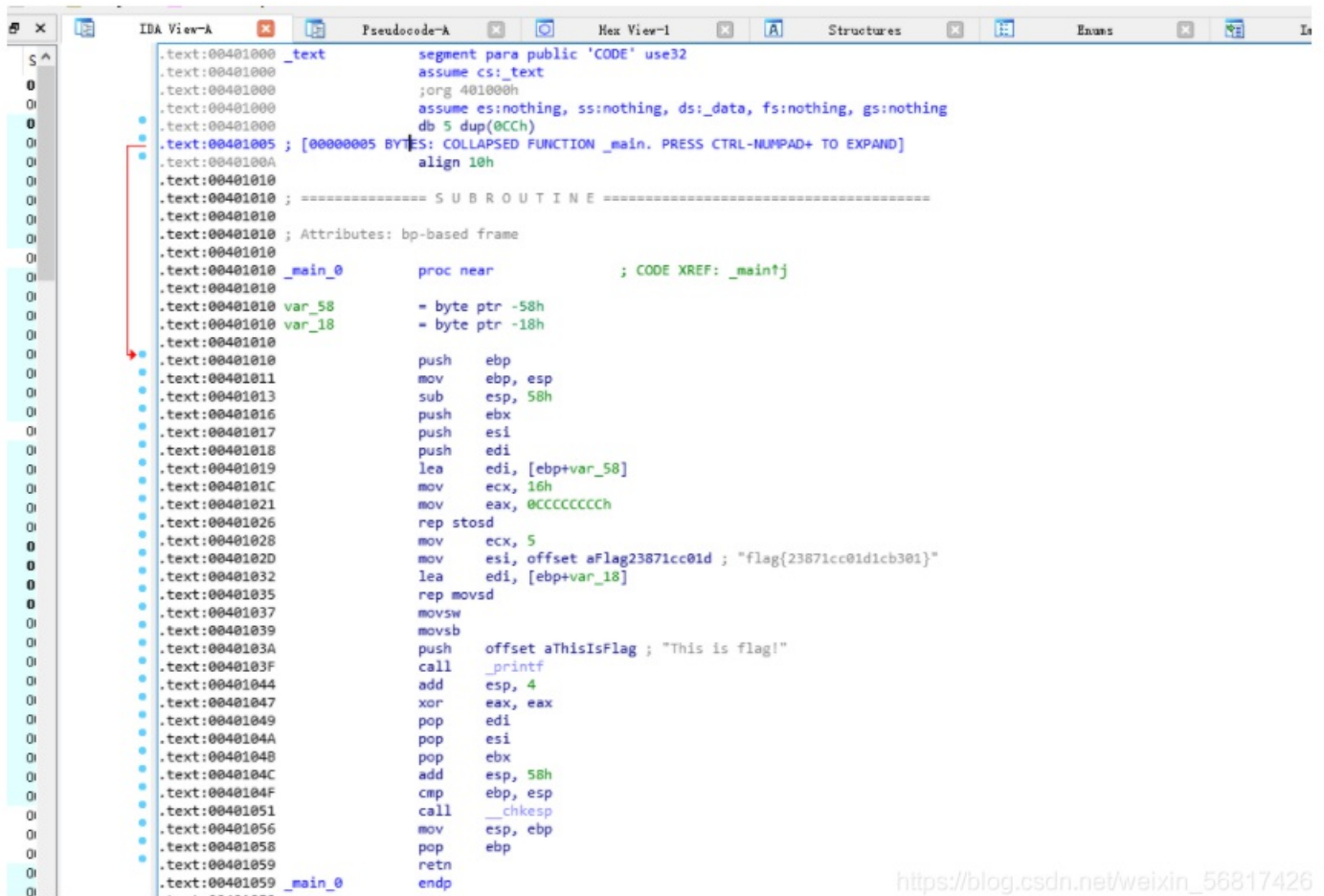
二、读题

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。



```
.text:00401000 _text      segment para public 'CODE' use32
.text:00401000      assume cs:_text
.text:00401000      ;org 401000h
.text:00401000      assume es:nothing, ss:nothing, ds:_data, fs:nothing, gs:nothing
.text:00401000      db 5 dup(0CCh)
.text:00401005 ; [00000005 BYTES: COLLAPSED FUNCTION _main. PRESS CTRL-NUMPAD+ TO EXPAND]
.text:0040100A      align 10h
.text:00401010      ; ===== SUBROUTINE =====
.text:00401010      ;
.text:00401010      ; Attributes: bp-based frame
.text:00401010      _main_0    proc near          ; CODE XREF: _main!j
.text:00401010      var_58     = byte ptr -58h
.text:00401010      var_18     = byte ptr -18h
.text:00401010      push     ebp
.text:00401011      mov      ebp, esp
.text:00401013      sub     esp, 58h
.text:00401016      push     ebx
.text:00401017      push     esi
.text:00401018      push     edi
.text:00401019      lea     edi, [ebp+var_58]
.text:0040101C      mov     ecx, 16h
.text:00401021      mov     eax, 0CCCCCCCCh
.text:00401026      rep stosd
.text:00401028      mov     ecx, 5
.text:0040102D      mov     esi, offset aFlag23871cc01d ; "flag{23871cc01d1cb301}"
.text:00401032      lea     edi, [ebp+var_18]
.text:00401035      rep movsd
.text:00401037      movsw
.text:00401039      movsb
.text:0040103A      push    offset aThisIsFlag ; "This is flag!"
.text:0040103F      call   _printf
.text:00401044      add     esp, 4
.text:00401047      xor     eax, eax
.text:00401049      pop     edi
.text:0040104A      pop     esi
.text:0040104B      pop     ebx
.text:0040104C      add     esp, 58h
.text:0040104F      cmp     ebp, esp
.text:00401051      call   __chkesp
.text:00401056      mov     esp, ebp
.text:00401058      pop     ebp
.text:00401059      retn
.text:00401059      _main_0    endp
```

https://blog.csdn.net/weixin_56817426

一、题目二：看本质

看本质？

实训描述：在渗透过程中，我们要透过现象，看本质。最后以SeBaFi{}的形式提交flag。

实训环境：

创建环境

https://blog.csdn.net/weixin_56817426

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。

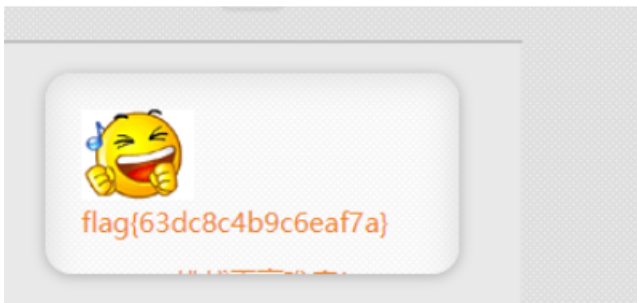
```

,
//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.toString(
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';
    }
}

```

https://blog.csdn.net/weixin_56817426

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。



https://blog.csdn.net/weixin_56817426

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         Toast.makeText(MainActivity.this, "Login Success", 0).show();
26     }
27     } else {
        Toast.makeText(MainActivity.this, "password error", 0).show();
    }
}
```

jadx-gui - android.apk

文件 视图 导航 工具 帮助



- android.apk
 - 源代码
 - android
 - androidx
 - com.example.xk.test
 - BuildConfig
 - MainActivity
 - R
 - 资源文件
 - 证书

```
com.example.xk.test.MainActivity X
package com.example.xk.test;

import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.view.View.OnClickListener;
import android.widget.Button;
import android.widget.EditText;
import android.widget.Toast;

public class MainActivity extends AppCompatActivity {
    EditText et;
    String pass = "flag{01E5DFFFC37E7C21}";

    15 protected void onCreate(Bundle savedInstanceState) {
    16     super.onCreate(savedInstanceState);
    17     setContentView((int) R.layout.activity_main);
    18     this.et = (EditText) findViewById(R.id.editText);
    31     ((Button) findViewById(R.id.button)).setOnClickListener(new OnClickListener() {
    22         public void onClick(View v) {
    24             if (MainActivity.this.pass.equals(MainActivity.this.et.getText().toString())) {
    25                 Toast.makeText(MainActivity.this, "Login Success", 0).show();
    27             } else {
                Toast.makeText(MainActivity.this, "password error", 0).show();
            }
        }
    });
}
```

https://blog.csdn.net/weixin_56817426