73: Whitzard OJ逆向（三）——DotNet Reversing

原创

S1lenc3 于 2020-02-11 22:43:21 发布 112 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_41858371/article/details/104270914

Easy DotNet

使用dnspy打开，

```
private void Button_Click(object sender, RoutedEvent
{
    string value = new string(new char[]
    {
        this.Letters[5],
        this.Letters[14],
        this.Letters[13],
        this.Letters[25],
        this.Letters[24]
    });
```

找到Letters，

```
// Token: 0x04000001 RID: 1
public char[] Letters = "ABCDEFGHIJKLMNOPQRSTUVWXYZ{}_".ToCharArray();
```

拿到key输入即可得到flag，也可以直接写脚本跑出flag。

SmartEnough

dnspy打开发现加了混淆。

hint是de4dot

使用de4dot进行反混淆。

然后可以直接拿到flag。

```
if (Class0.smethod_0(Console.ReadLine()))
{
    Console.WriteLine("FLAG-46FSi601E9MLz1G0spD0LDSTu58JSe9A");
    Console.ReadLine();
```

Where is my 13th count

unity写的游戏，C#代码需要反编译Assembly-CSharp.dll
游戏是控制一个白球吃分，一共能得到12分。
题目是第13个数在哪，猜测需要改程序得到13分。

```
private void Start()
{
    this.test();
    base.InvokeRepeating("test", 5f, 5f);
    this.rb = base.GetComponent<Rigidbody>();
    this.count = 12;
    this.SetCountText();
    this.winText.text = string.Empty;
}
```

直接修改count为12，然后运行游戏，得到13分发现没什么反应。
又看了看代码，发现：

```
private void SetCountText()
{
    this.countText.text = "Count: " + this.count.ToString();
    if (this.count >= 14)
    {
        this.winText.text = "Don't Eat Your Flag!";
        this.floor.transform.position = new Vector3(this.floor.transf
          this.floor.transform.position.z);
    }
}
```


吃到14分，flag就出现在屏幕上了。

Roughlike

又是一道游戏题。
这道题没做出来，没想到这种操作。。。
dnspy打开Assembly-CSharp.dll

```
case 5:
{
    Vector3 position = this.RandomPosition();
    UnityEngine.Object.Instantiate<GameObject>(S3cretArray[0].tile, position, Quaternion.identity);
    num = 0;
    continue;
}
case 6:
```

感觉有用的代码就是这里，而且这段代码是执行不到的，但找了半天也不知道S3creArray是什么。
所以直接修改逻辑使num=5。
然后游戏地图上多了一个东西，也不知道是啥，我把键盘滚了一遍才发现还有道具这种东西，‘I’键是道具，然后会看到一串base64.解开提交不对，看来还有别的flag，最后也不知道在哪，所以看了writeup。
它说在游戏开始的动画里提示了SPELL，谁没事干看这个，我去。好吧，我太菜了。
然后代码里搜了一下SPELL

```
private void InitGame()
{
    if (true)
    {
    }
    this.doingSetup = true;
    this.levelImage = GameObject.Find("LevelImage");
    this.levelText = GameObject.Find("LevelText").GetComponent<Text>();
    this.SPText = GameObject.Find("SPELLText").GetComponent<Text>();
    this.levelText.text = "Day " + this.level;
    this.SPText.enabled = true;
    this.levelImage.SetActive(true);
    base.Invoke("HideLevelImage", this.levelStartDelay);
    this.enemies.Clear();
    this.fadinglist.Clear();
    BagSystem.instance.Initialize();
    this.controllerScript.initialize();
    this.boardScript.SetupScene(this.level);
    Debug.Log(this.dMonster);
```


原来SPText.enabled是Flase，我改成了true。
注意，有时候右键编辑方法不能反编译成功，所以最好修改IL指令。
然后运行游戏，就会出现另一部分flag。
flag是WeLC0mE_70_5uc7F
参考：https://www.anquanke.com/post/id/146419