

# 攻防世界 Reverse高手进阶区 2分题 tt3441810

原创

思源湖的鱼 于 2020-12-14 11:03:45 发布 73 收藏

分类专栏: [ctf](#) 文章标签: [ctf](#) [攻防世界](#) [reverse](#)

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\\_44604541/article/details/111152133](https://blog.csdn.net/weixin_44604541/article/details/111152133)

版权

## CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

### 前言

继续ctf的旅程

攻防世界Reverse高手进阶区的2分题

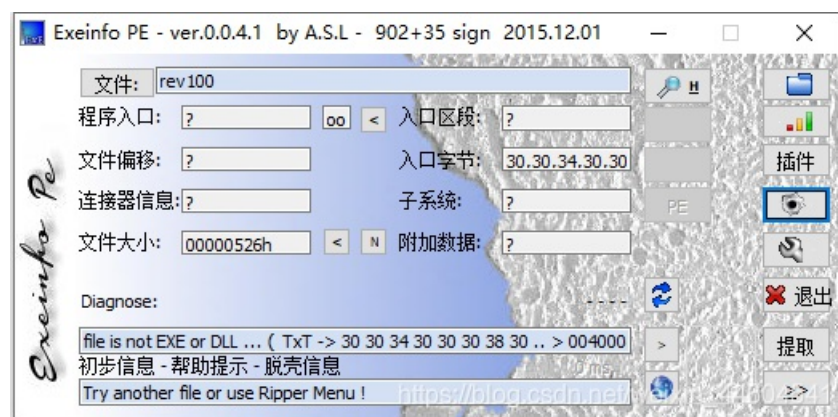
本篇是tt3441810的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

### 解题过程

PE查壳



提示是个txt

notepad打开

```

00400080 68 66 6C 00 00 48 BF 01 00 00 00 00 00 00 48
00400090 8D 34 24 48 BA 02 00 00 00 00 00 00 48 B8 01
004000A0 00 00 00 00 00 00 00 0F 05 68 61 67 00 00 48 BF
004000B0 01 00 00 00 00 00 00 00 48 8D 34 24 48 BA 02 00
004000C0 00 00 00 00 00 00 48 B8 01 00 00 00 00 00 00
004000D0 0F 05 68 7B 70 00 00 48 BF 01 00 00 00 00 00
004000E0 00 48 8D 34 24 48 BA 02 00 00 00 00 00 00 48
004000F0 B8 01 00 00 00 00 00 00 0F 05 68 6F 70 00 00
00400100 48 BF 01 00 00 00 00 00 00 00 48 8D 34 24 48 BA
00400110 02 00 00 00 00 00 00 00 48 B8 01 00 00 00 00
00400120 00 00 0F 05 68 70 6F 00 00 48 BF 01 00 00 00
00400130 00 00 00 48 8D 34 24 48 BA 02 00 00 00 00 00
00400140 00 48 B8 01 00 00 00 00 00 00 0F 05 68 70 72
00400150 00 00 48 BF 01 00 00 00 00 00 00 00 48 8D 34 24
00400160 48 BA 02 00 00 00 00 00 00 00 48 B8 01 00 00
00400170 00 00 00 00 0F 05 68 65 74 00 00 48 BF 01 00
00400180 00 00 00 00 00 48 8D 34 24 48 BA 02 00 00 00
00400190 00 00 00 48 B8 01 00 00 00 00 00 00 0F 05 68
004001A0 7D 0A 00 00 48 BF 01 00 00 00 00 00 00 48 8D
004001B0 34 24 48 BA 02 00 00 00 00 00 00 48 B8 01 00
004001C0 00 00 00 00 00 00 0F 05 48 31 FF 48 B8 3C 00 00
004001D0 00 00 00 00 00 0F 05

```

去掉地址转ascii

Unicode编码 UTF-8编码 URL编码/解码 Unix时间戳 Ascii/Native编码互转 Hex编码/解码

hflH...hagH...H...V...H...4\$H...H...H...4\$H...hpoH...BD...  
H...hpr...B...H...V...W@...H...4\$H...V...  
H...BD...H1...H...<...

utf-8 Hex编码 Hex解码 清空结果

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

发现h后面跟的两个字符连起来就是flag

flag{poppopret}

## 结语

无