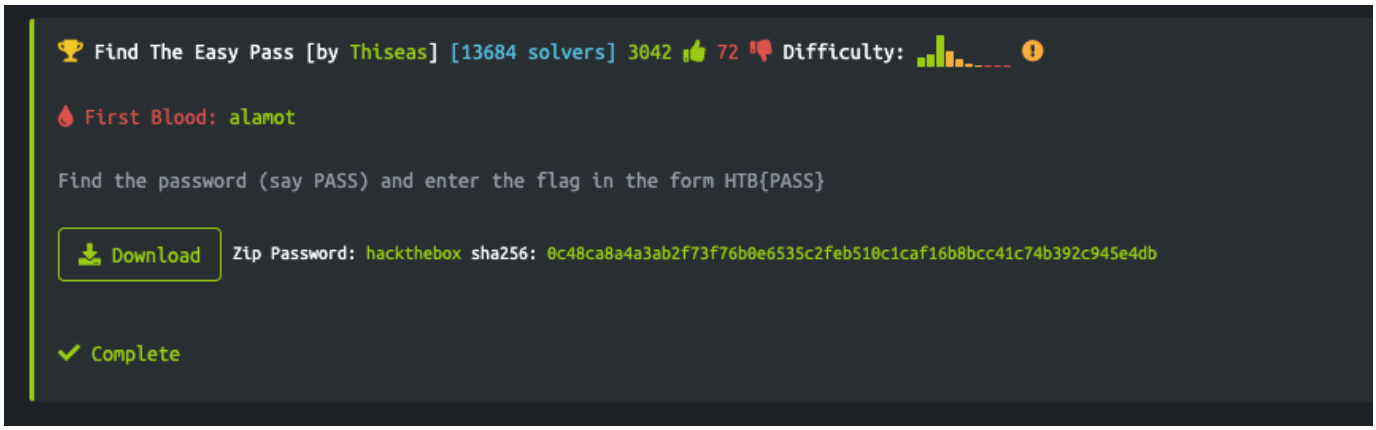
前言

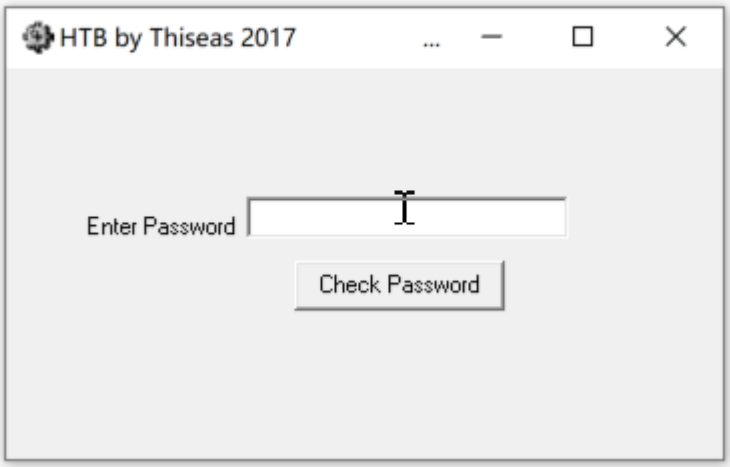
Author: 0x584A



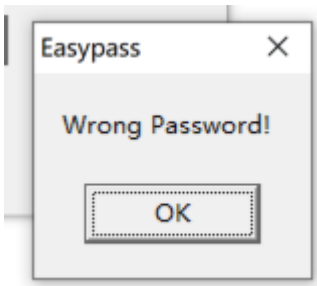
这是一道破解题目，下载完成后查看文件类型：

```
~/Downloads via ⬢ v15.0.1 via 🐃v7.3.24
→ file EasyPass.exe
EasyPass.exe: PE32 executable (GUI) Intel 80386, for MS Windows
```

32位Windows的程序，放Windows 10里去运行：

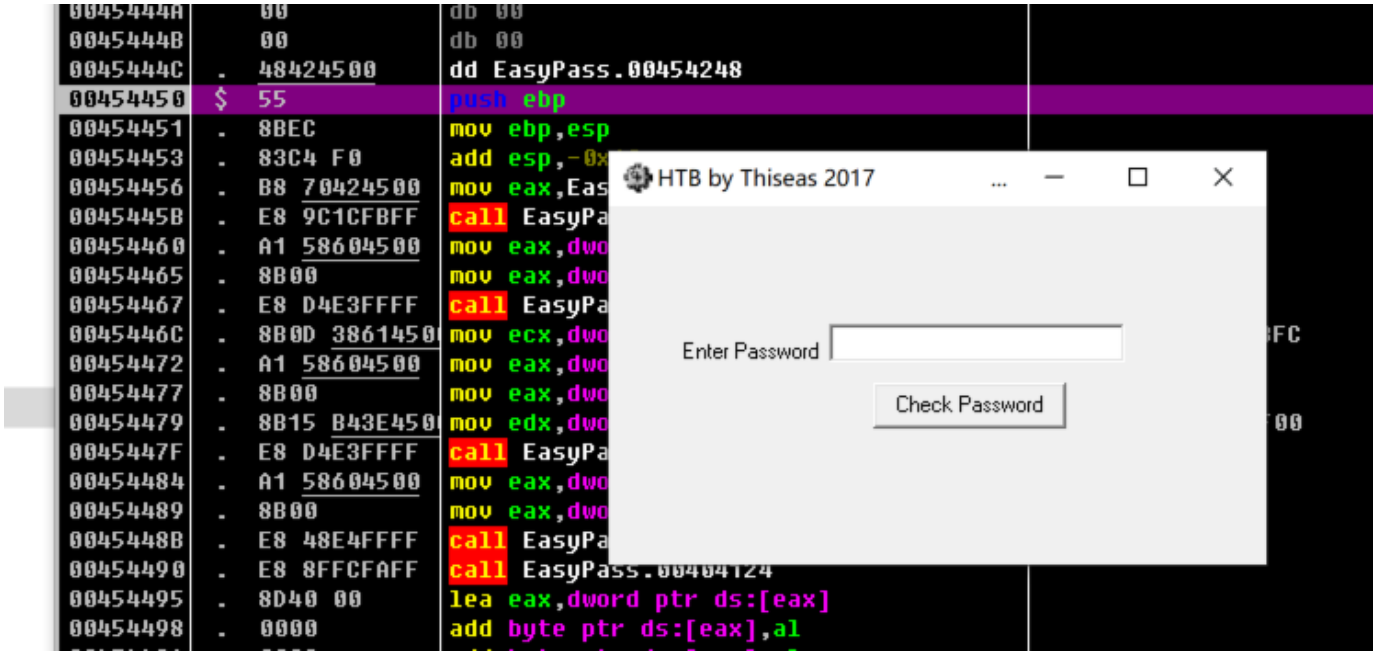


输入密码，并验证输入结果是否正确，当输入错误时会提示："Wrong Password!"



Ollydbg

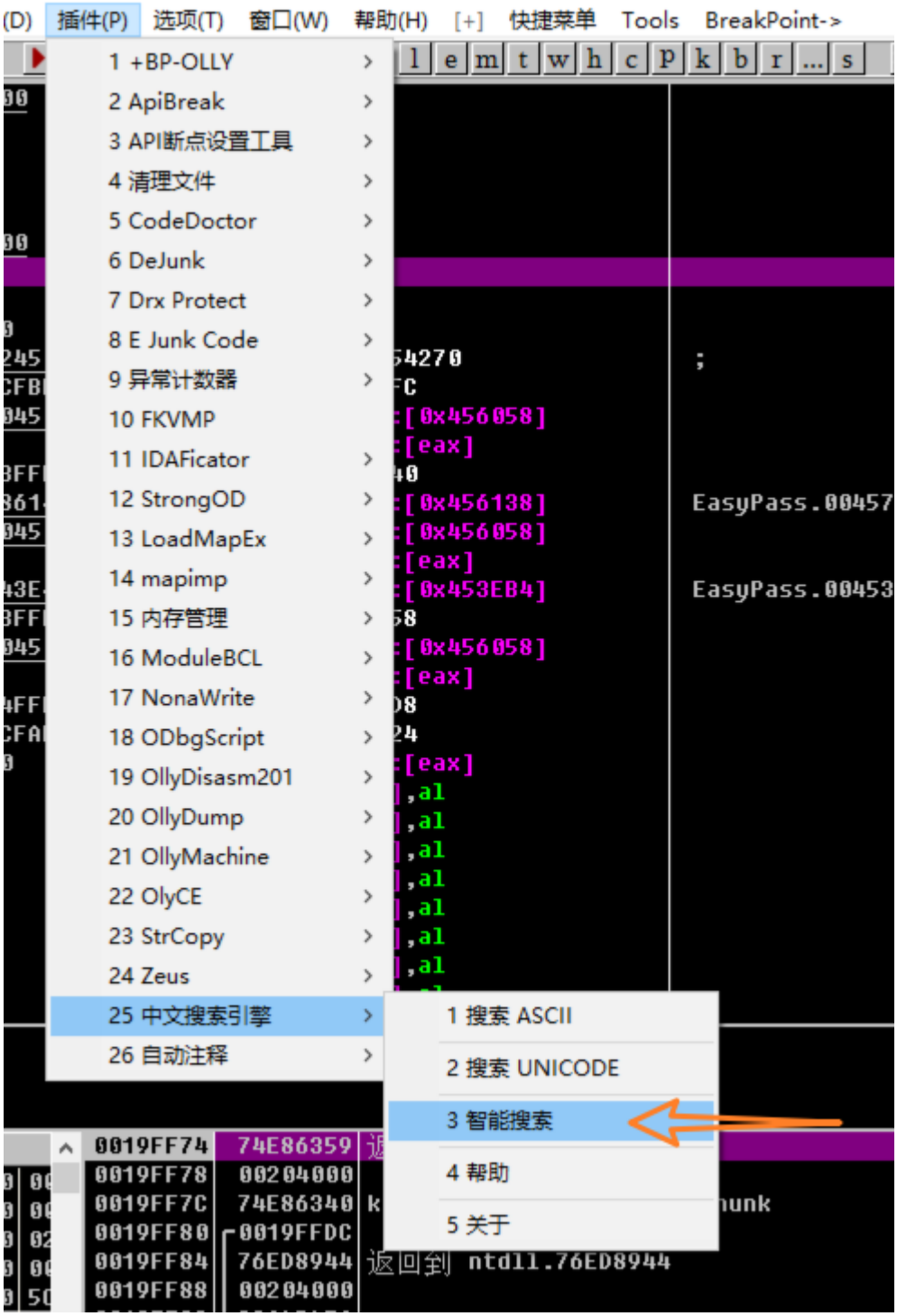
开启 Ollydbg 加载它，并运行调试。

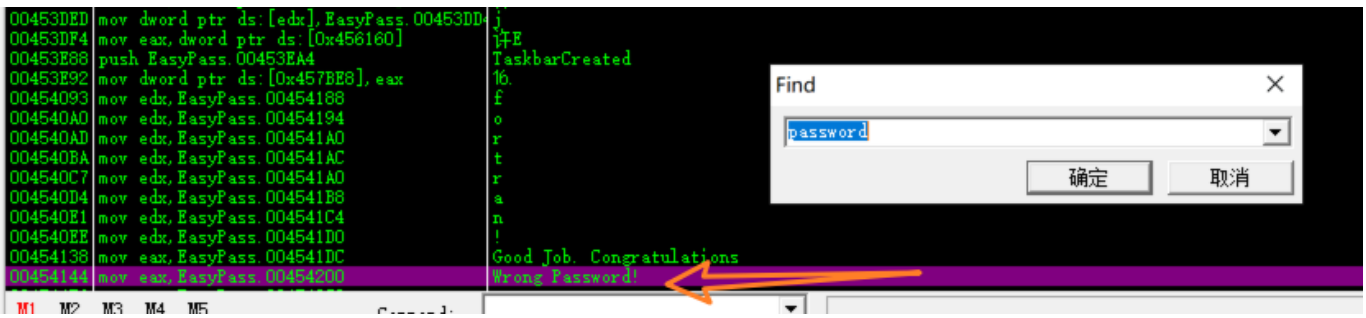


首先记一下程序的入口地址，方便以后返回该处。

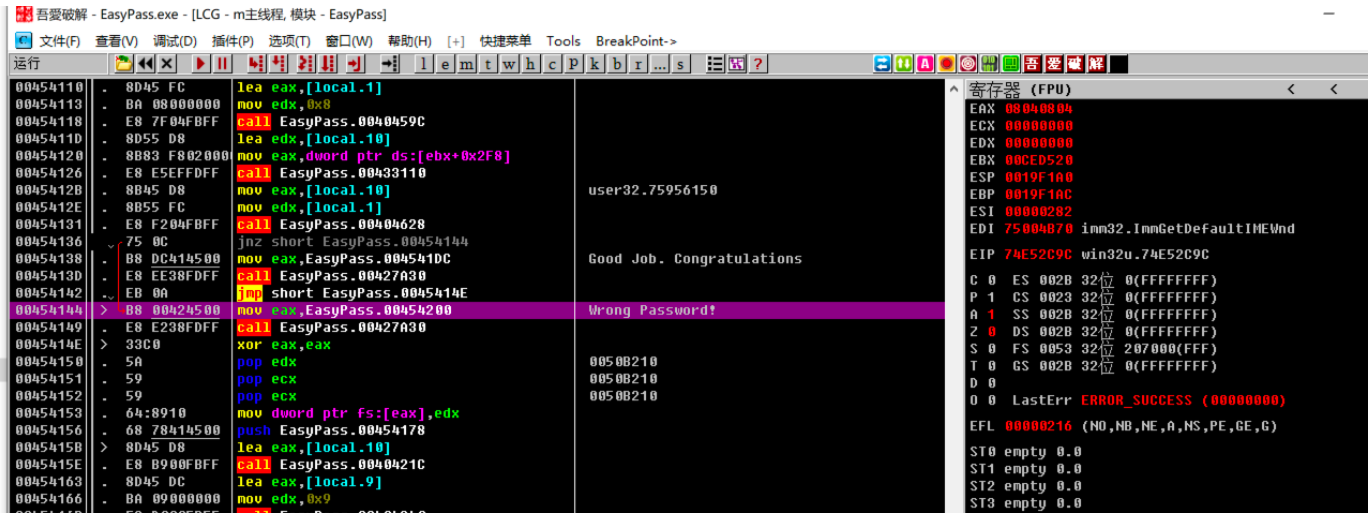
```
1 00454450 > $  55            push ebp
```

先前已经知道了当密码输入错误时，会提示错误的字符，尝试使用智能搜索下，看能否查到该字符串。





可以看到，已经搜到了对应的是 `00454144` 这个地址，双击后会进入该地址的反汇编窗口。

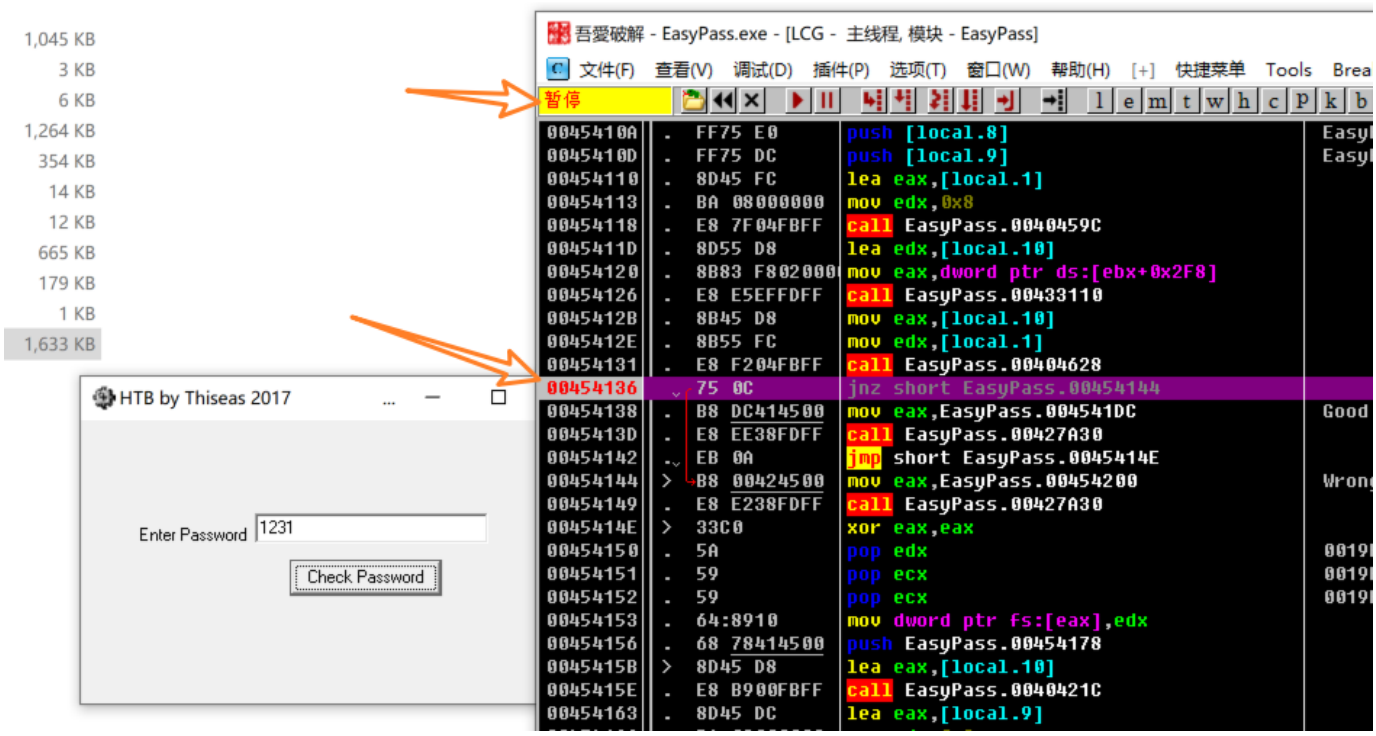


在高亮的这一行中可以看到来源地址是 `00454136`，代表是从它那跳转过来的。

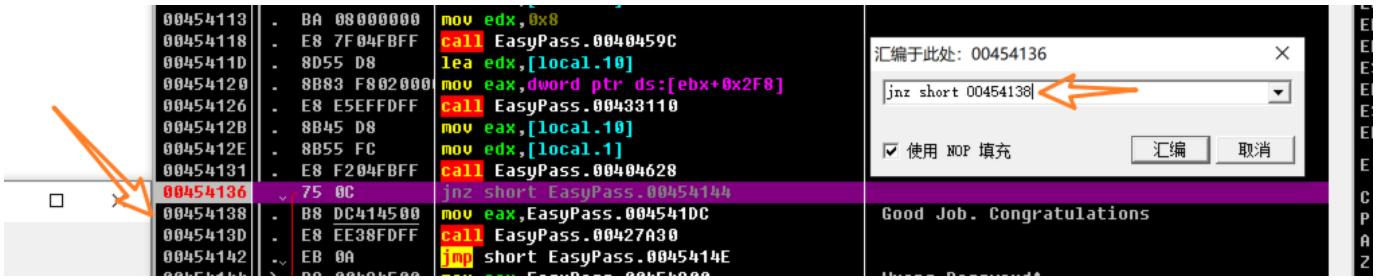
`jnz short EasyPass.00454144` 中的 `jnz` 在汇编中代表的是条件跳转，也就是不满足条件则跳转到 `00454144` 这个地址。

```
1 nop是删除跳转，就是代表什么也不做的意思
2 je是条件跳转，满足条件就跳转，不满足就不跳转
3 jnz也是条件跳转，不满足条件就跳转
4 jmp是无条件跳转，强制跳转到
```

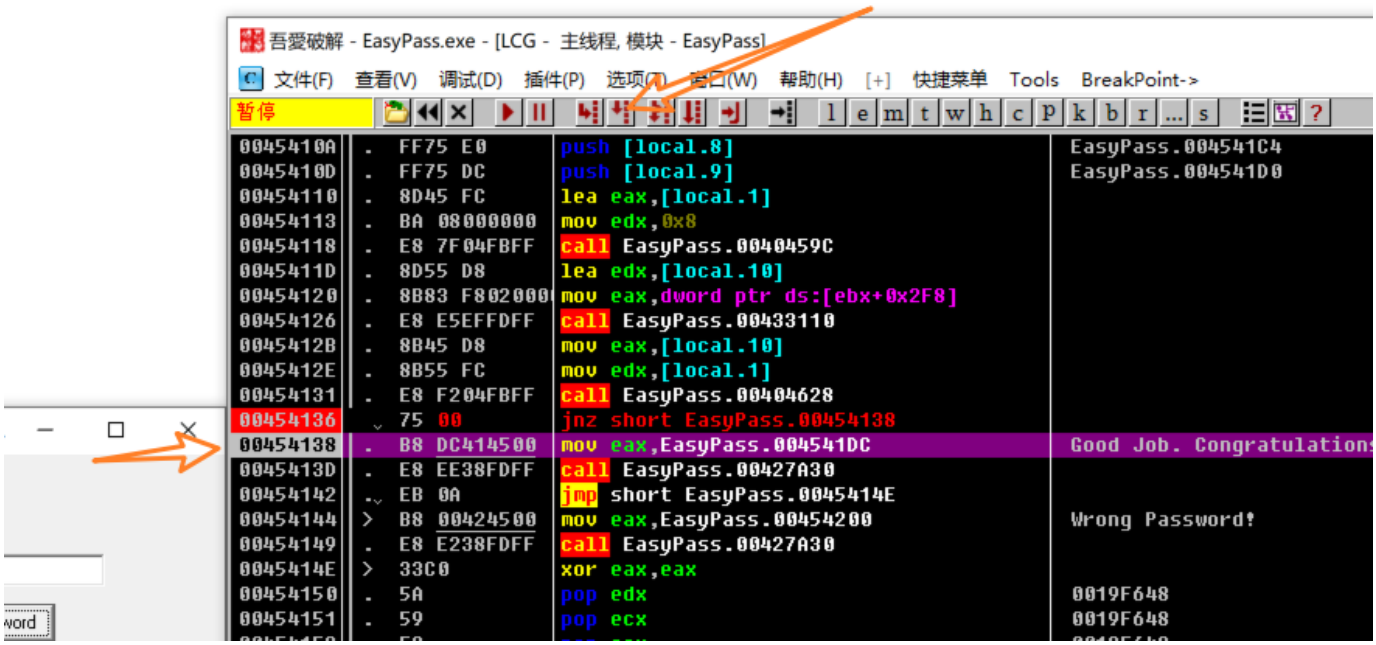
在 `00454136` 地址下个点断 f2，随后随便输入一个密码，我这里用1231



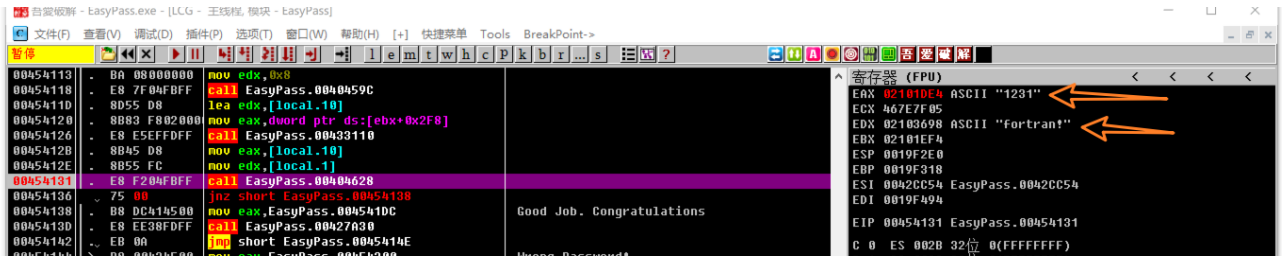
此时调试状态处于暂停，双击它，将 jnz 的地址改为 `00454138`，也就是它的下一行，改变它的逻辑。



点击 单步步过 已经进入了我们想要的地址行

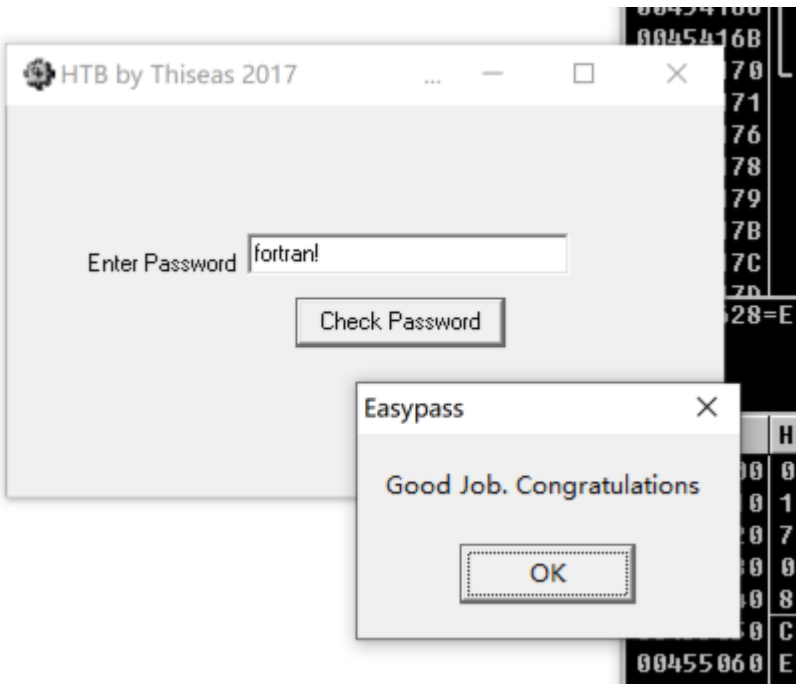


但是这样并没有什么意义，仅是将 `Good Job. Congratulations` 弹框输入而已，我们在 `00454131` 处下断。



这个时候就获取到了与我们输入1231 进行比对的密码：fortran!

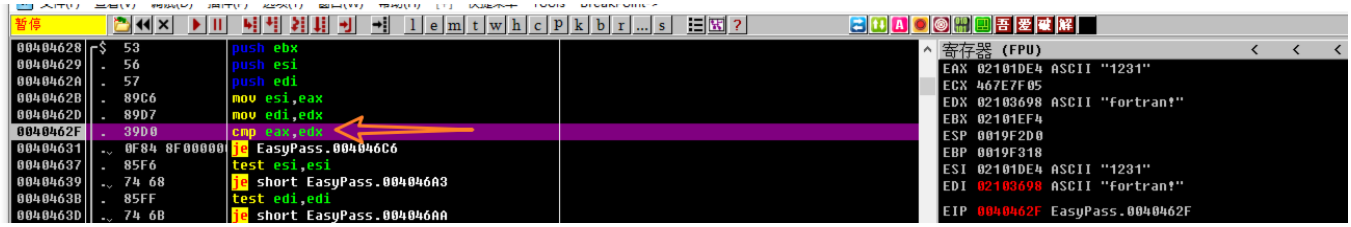
从新运行这个程序，直接输入需要对比的密码，提示正确。



直接提交flag：HTB{fortran!}

原因

单步步入 至这个 class，可以看到存在 cmp。



可以看到 EAX 已移动到 ESI，然后 EDX 移动到 EDI

cmp 语句用于比较两个寄存器(整数，字符代码也是整数，因此可以用 CMP 指令)：

- EAX：包含我们输入的密码
- EDX：其中包含正确的密码

所以直接查看 EDX 寄存器的内容解决这题。

其他

- https://www.cnblogs.com/dotnetcrazy/p/8417213.html