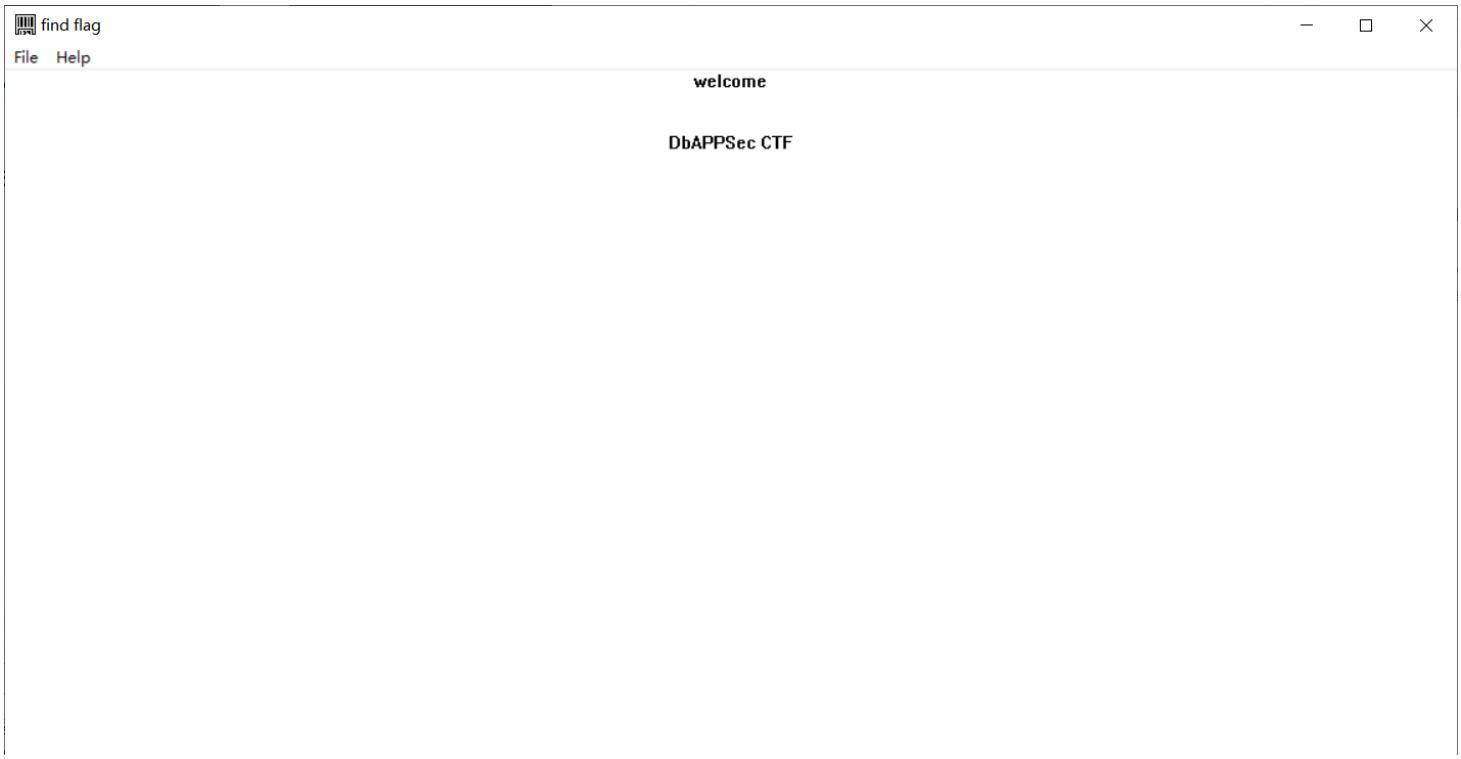
看起来是一道mfc题目
其实感觉跟mfc没啥大关系



没有跟flag有关的按钮
也就是说winmain没啥卵用
这时候考虑隐藏了啥代码

```
1 // attributes: thunk
2 void sub_401014()
3 {
4   JUMPOUT(0x401640);
5 }
```

翻到了这个
在0x401640处翻到了

```
.text:00401640 Paint           = tagPAINTSTRUCT ptr -48h
.text:00401640 var_8           = dword ptr -8
.text:00401640 var_4           = dword ptr -4
.text:00401640 hWndParent      = dword ptr  8
.text:00401640 Msg             = dword ptr  0Ch
.text:00401640 wParam          = dword ptr  10h
.text:00401640 lParam          = dword ptr  14h
.text:00401640
.text:00401640                 push    ebp
.text:00401641                 mov     ebp, esp
.text:00401643                 sub     esp, 440h
.text:00401649                 push    ebx
.text:0040164A                 push    esi
.text:0040164B                 push    edi
.text:0040164C                 lea     edi, [ebp+var_440]
.text:00401652                 mov     ecx, 110h
.text:00401657                 mov     eax, 0CCCCCCCCh
.text:0040165C                 rep stosd
.text:0040165E                 mov     esi, esp
.text:00401660                 push    64h ; 'd'       ; cchBufferMax
.text:00401662                 lea     eax, [ebp+Buffer]
.text:00401668                 push    eax             ; lpBuffer
.text:00401669                 push    6Ah ; 'j'       ; uID
.text:0040166B                 mov     ecx, hInstance
```

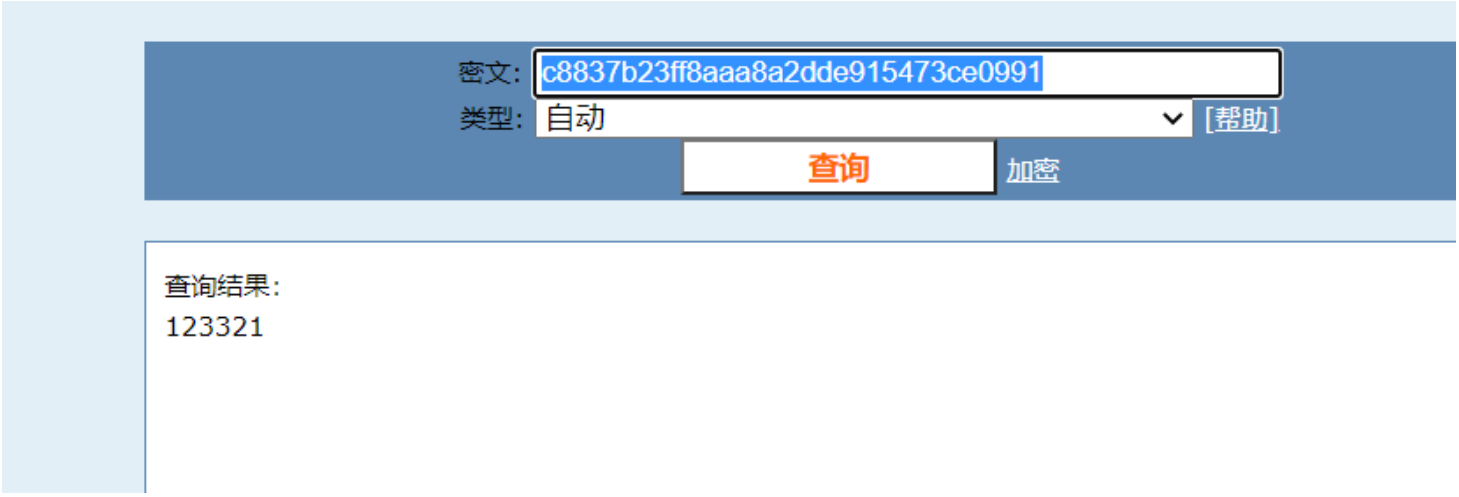
需要修改一下代码才可以编译

```
      v6 = strlen((const char *)String1);
      memcpy(v20, String1, v6);
      *v7 = __ES__;
      v8 = strlen((const char *)String1);
      hash(String1, v8, v11);
      strcpy(Str, "0kk`d1a`55k222k2a776jbfgd`06cjjb");
      memset(v17, 0, sizeof(v17));
      v18 = 0;
      v19 = 0;
      strcpy(v13, "SS");
      *(_DWORD *)&v13[3] = 0;
      v14 = 0;
      v15 = 0;
      v9 = strlen(Str);
      xor(v13, (int)Str, v9);
      if ( _strcmpi((const char *)String1, Str) )
      {
        SetWindowTextA(hWndParent, "flag{}");
        MessageBoxA(hWndParent, "Are you kidding me?", "^_^", 0);
        ExitProcess(0);
      }
      memcpy(v12, &unk_423030, 0x32u);
      v10 = strlen(v12);
      xor(v20, (int)v12, v10);
      MessageBoxA(hWndParent, v12, 0, 0x32u);
    }
    ++dword_428D54;
  }
```

首先是对string1进行了hash加密（md5）

得到的结果需要与Str的字符串与'SS'异或后的字符串必须相等

```
data.py
b'c8837b23ff8aaa8a2dde915473ce0991'
PS C:\Users\wsxk>
```



可以看出String1是‘123321’

```
58          MessageBoxA(hWndParent, "Are you kidding me?", "^_^", 0);
59          ExitProcess(0);
60        }
61        memcpy(v12, &unk_423030, 0x32u);
62        v10 = strlen(v12);
63        xor(v20, (int)v12, v10);
64        MessageBoxA(hWndParent, v12, 0, 0x32u);
65      }
66      ++dword_428D54;
67    }
68    else
69    {
70      if ( Msg != 520 )
71        return DefWindowProcA(hWndParent, Msg, wParam, lParam);
```

最后是和0x423030处的值和‘123321’循环异或即可得到flag

```
b'flag{n0_Zu0_n0_die}23321ba33\x02ZZRW\x02SQ\x04\x07X\x01\x00\x03Z\x00R\x04\x05\x07[P'
```