BUUCTF：小易的U盘

原创

末 初 于 2020-11-07 21:46:01 发布 998 收藏 2

分类专栏： CTF_MISC_Writeup

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/mochu7777777/article/details/109552833

版权

CTF_MISC_Writeup 专栏收录该内容

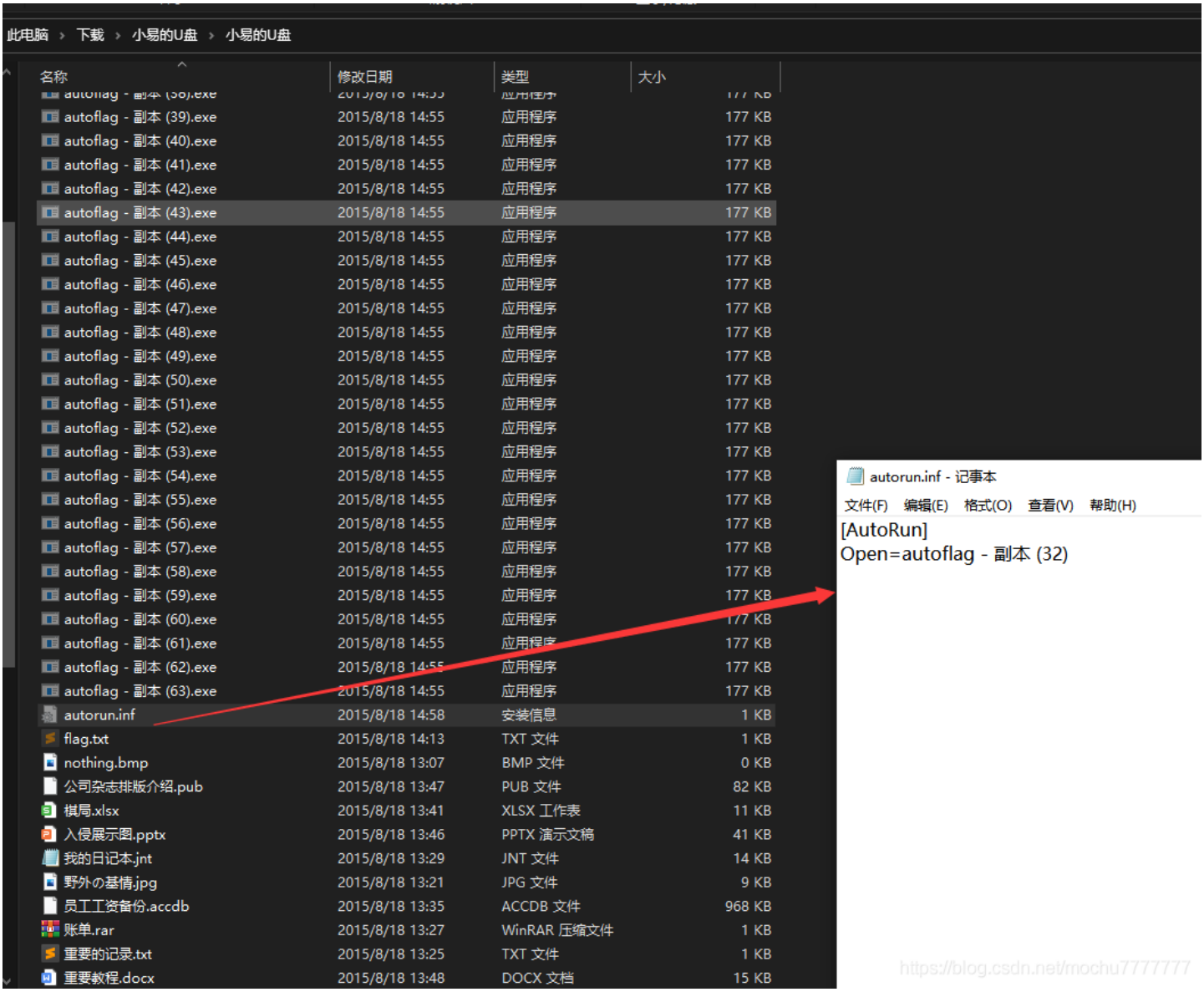
246 篇文章 45 订阅

订阅专栏

```
https://buuoj.cn/challenges#%E5%B0%8F%E6%98%93%E7%9A%84U%E7%9B%98
```

下载下来是`iso`文件，但是文件头是`Rar`文件，修改后缀为`rar`，解压

`autorun.inf`



使用`IDA`打开`autoflag - 副本 (32).exe`，直接搜索`flag`

```
; Attributes: bp-based frame

_main_0 proc near

var_44= byte ptr -44h
var_4= dword ptr -4

push    ebp
mov     ebp, esp
sub     esp, 44h
push    ebx
push    esi
push    edi
lea     edi, [ebp+var_44]
mov     ecx, 11h
mov     eax, 0CCCCCCCCh
rep stosd
push    offset aW       ; "w+"
push    offset aDProgramFlagTx ; "D:/Program/flag.txt"
call    _fopen
add     esp, 8
mov     [ebp+var_4], eax
mov     eax, [ebp+var_4]
push    eax             ; FILE *
push    offset aFlag29a0vkrlek ; "flag{29a0vkrlek3eu10ue89yug9y4r0wdu10}"
call    _fputs
add     esp, 8
mov     ecx, [ebp+var_4]
push    ecx             ; FILE *
call    _fclose
add     esp, 4
pop     edi
pop     esi
pop     ebx
add     esp, 44h
cmp     ebp, esp
call    __chkesp
mov     esp, ebp
pop     ebp
retn
_main_0 endp
```

```
flag{29a0vkrlek3eu10ue89yug9y4r0wdu10}
```