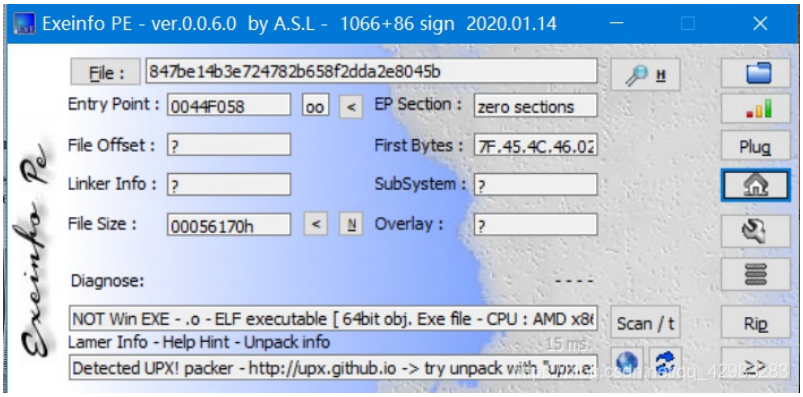
xctf攻防世界simple-unpack writeup

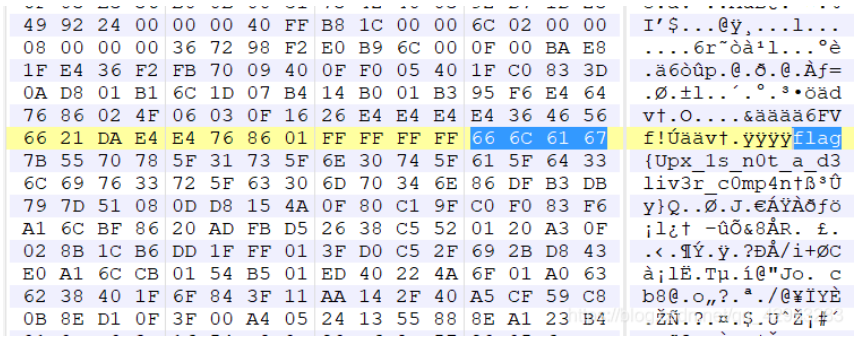
原创

qq_112419837 于 2020-11-04 10:17:48 发布 104 收藏

下载附件查看，发现upx：



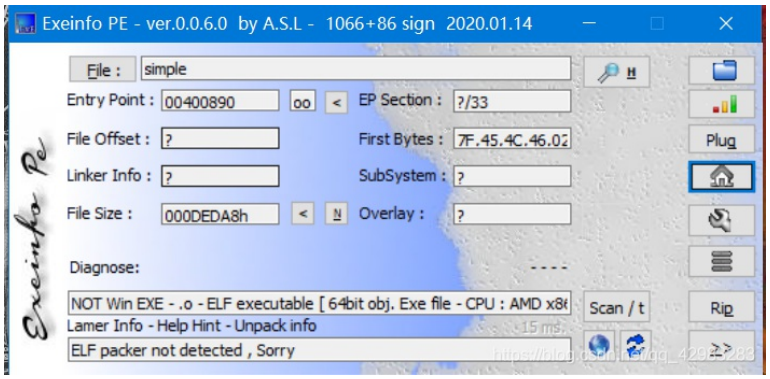
010editor搜索flag发现：



使用kali 脱壳：

upx -d 847be14b3e724782b658f2dda2e8045b -o simple

查看：



ida64打开，f5伪代码，可以直接找到flag：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int result; // eax@4
  __int64 v4; // rdx@4
  char v5; // [sp+0h] [bp-70h]@1
  __int64 v6; // [sp+68h] [bp-8h]@1

  v6 = *MK_FP(__FS__, 40LL);
  _isoc99_scanf((unsigned __int64)"%96s");
  if ( sub_400360(&v5, flag) )
    puts("Try again!");
  else
    puts("Congratulations!");
  result = 0;
  v4 = *MK_FP(__FS__, 40LL) ^ v6;
  return result;
}
```

双击flag：

```
.data:00000000006CA09E                  dd    0
.data:00000000006CA09F                  db    0
.data:00000000006CA0A0                  public flag
.data:00000000006CA0A0 flag             db 'flag{Upx_1s_n0t_a_d3liv3r_c0mp4ny}',0
.data:00000000006CA0A0                                          ; DATA XREF: main+31↑o
.data:00000000006CA0C3                  align 8
.data:00000000006CA0C8                  public _dl_tls_static_size
.data:00000000006CA0C8 _dl_tls_static_size dq 800h              ; DATA XREF: __libc_setup_tls+7E↑r
.data:00000000006CA0C8                                          ; __libc_setup_tls+1B5↑r ...
.data:00000000006CA0D0                  public _nl_current_default_domain
.data:00000000006CA0D8 _nl_current_default_domain dq offset _nl_default_default_domain
```