Capability Leaking

```
#include <stdio.h>
#include <stdlib.h>
#include <fcntl.h>
void main()
{
int fd; // 1
char v[2];
fd = open("/etc/zzz",O_RDWR | O_APPEND); // 2
if( fd == -1)    // 3
{
printf("Cannot open /etc/zzz\n");
exit(0);
} // end if
printf("fd is %d\n",fd);
setuid(getuid());     // 4
v[0] = "/bin/sh";
v[1] = 0;
execve(v[0],v,0); // 5
} // end main
```

1 - قمنا بتعريف متغير int، يحمل قيمة الـ file descriptor

2 - دالة الـopen ستقوم بعملية فتح الملف، الـ parameter الخاصة بالدالة هنا هي :

- مسار الملف المراد فتحه
- مجموعتين من الـ Flags
- **O_RDWR :** فتح الملف ومن ثم **القراءة والكتابة** عليه
- **O_APPEND :** كتابة البيانات في آخر الملف (**الإضافة** عليه)

3 - دالة الـ open تُعيد القيمة -1 في حالة حدوث أي خطأ خلال فتح الملف

مجموعتين من ال flags، يسبقهم مسار الملف المراد فتحه .

4 - هذه الخطوة تقوم بتغيير الصلاحيات الخاصة بهذا البرنامج (الكود) كالآتي:

تخزين قيمة الـ uid الخاصة بالمستخدم في الـ effective user ID

أي بإختصار نقوم **بخفض الصلاحيات** الخاصة بالبرنامج (في الأصل البرنامج يقوم بفتح الملف zzz والذي لايملك صلاحية الكتابة عليه سوى الـ Root)

5 - الدالة execve تقوم **بتنفيذ** برنامج ما، تستقبل هذه الـ Parameters (حسب ترتيبها في الكود أعلاه من اليسار إلى اليمين):

- المسار الخاص بالبرنامج المراد تنفيذه
- الـ arguments الخاصة بالبرنامج
- الـ environment variable

مرجع:

http://man7.org/linux/man-pages/man2/getuid.2.html

http://man7.org/linux/man-pages/man2/setuid.2.html

http://man7.org/linux/man-pages/man2/execve.2.html

https://www.computerhope.com/jargon/f/file-descriptor.htm

https://linux.die.net/man/3/open