Let us look at the system calls

find/rm

Attacker

```
mkdir ("/tmp/badetc")

creat ("/tmp/badetc/passwd")

readdir ("/tmp") \rightarrow "badetc"

lstat ("/tmp/badetc") \rightarrow DIRECTORY
```

readdir ("/tmp/badetc") → "passwd"

unlink ("/tmp/badetc/passwd")

TOCTOU attack

find/rm

```
readdir ("/tmp") \rightarrow "badetc"
lstat ("/tmp/badetc") \rightarrow DIRECTORY
readdir ("/tmp/badetc") \rightarrow "passwd"
```

unlink ("/tmp/badetc/passwd")

Attacker

```
mkdir("/tmp/badetc")
creat("/tmp/badetc/passwd")
```

```
rename ("/tmp/badetc" \rightarrow "/tmp/x") symlink ("/etc", "/tmp/badetc")
```

Time-of-check-to-time-of-use (a.k.a TOCTOU) bug

- find checks that /tmp/badetc is not symlink
- · but meaning of file name changes before it is used