Another example - xterm

`xterm` Provides a terminal window in X-windows - used to run with setuid root privileges

- Requires kernel pseudo-terminal (`pty`) device
- Required root privileges to change ownership of `pty` to user
- Also writes protected `utmp`/`wtmp` files to record users

Had feature to log terminal session to file

```
if (access (logfile, W_OK) < 0)
  return ERROR;

fd = open (logfile, O_CREAT|O_WRONLY|O_TRUNC, 0666);
/* ... */
```

➡ `xterm` is root, but should not log to file user cannot write

✓ `access` call does permission check with real, not effective UID

◉ .... but another TOCTOU bug

Another TOCTOU attack

xterm	**Attacker**
	creat (“/tmp/log”)
access (“/tmp/log”) → OK	
	unlink (“/tmp/log”)
	symlink (“/tmp/log” → “/etc/passwd”)
open (“/tmp/log”)	

Attacker changes `/tmp/log` between check and use

➡ `xterm` unwittingly overwrites `/etc/passwd`

- OpenBSD man page - "CAVEATS : access() is a potential security hole and should never be used."