More Notable TOCTOU Attacks

- **Dirty COW** (CVE-2016-5195)
  Race condition in Linux kernel's copy-on-write mechanism leading to privilege escalation

- **Dirty Pipe** (CVE-2022-0847)
  Linux kernel race in pipe buffer handling bypassing sandboxing for privilege escalation

Input Validation Attack

➡ Untrusted input is mixed into a command or query without proper validation or separation

◉ Execute unintended instructions instead of treating the input as data

✓ Can be mitigated with proper inout validation/sanitization