







- Keep in mind that the bot user do what developer demands.
- Do not grant more access permissions that you'll grant to developers.





The mighty **ClBOT**



Unchecked Privileges:

[https://portswigger.net/daily-swig/
unresolved-github-actions-flaw-allows-
code-to-be-approved-without-review](https://portswigger.net/daily-swig/unresolved-github-actions-flaw-allows-code-to-be-approved-without-review)



The mighty CI BOT

- Is your CI/CD executed as root?
- There is only one all mighty bot user?
- Your bot user has admin permissions over production?

- Keep in mind that the bot user do what developer demands.
- Do not grant more access permissions that you'll grant to developers.



Unchecked Privileges:
<https://portswigger.net/daily-swig/unresolved-github-actions-flaw-allows-code-to-be-approved-without-review>



The EVIL AGENT (1 / 3)

- Do you control what can download a developer when they runs in a pipeline?
- Do you control which command can launch a developer in a C.I. / C.D. configuration file? (Jenkinsfile, gitlab.yaml...)
- Is your C.I / C.D. in different network? Are you sure?