



IN THE BUILDING STEP

User

Code

Building step

Deployment step

Production



CODE



COMMIT



RELATED CODE



TEST



CI PIPELINE



CD PIPELINE





Control **Artefacts** Repository

- What if a developer can publish an arbitrary code into artefacts / libraries repository?
- What if a developer publish a trojanized version of a library?
- What if a developer publish, intentionally, an artefact with known vulnerabilities?