

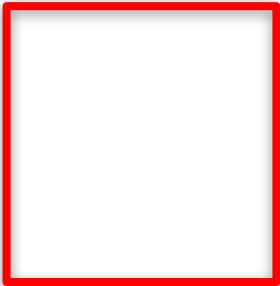




Ensure you mark as
Protected / Secret
sensitive variables in
your C.I. system

Type		Key	Value	State
Variable	⬆	KUBE_URL	https://1.2.3.4	Protected <input checked="" type="checkbox"/>
File	⬆	KUBE_CA_PEM	-----BEGIN CERTIFICATE--- -- MIICyDCCAbCg	Protected <input checked="" type="checkbox"/>





Then ENV Leak!! (2/2)



Secrets

Actions

[Dependabot](#)

Repository secrets



PYPI_PASSWORD

Updated on 28 Aug

Update

Remove





The ENV Leak! (2/2)


Ensure you mark as
Protected / Secret
sensitive variables in
your C.I. system

Type	Key	Value	State
Variable	KUBE_URL	https://1.2.3.4	Protected <input checked="" type="checkbox"/>
File	KUBE_CA_PEM	-----BEGIN CERTIFICATE--- == MIICyDCCAbCg	Protected <input checked="" type="checkbox"/>

Secrets

Actions
Dependabot

Repository secrets

 PYPI_PASSWORD Updated on 28 Aug





The Evil GitHub Actions!

- Usually C.I. / C.D. system stores sensitive information.
- They need them to access to productive environments, publish artefacts, perform some checks, etc
- They, usually, store as environment vars.

CodeCov:

<https://www.wolfe.id.au/2021/04/26/github-actions-supply-chain-attacks/>

<https://docs.gitlab.com/ee/ci/variables/>