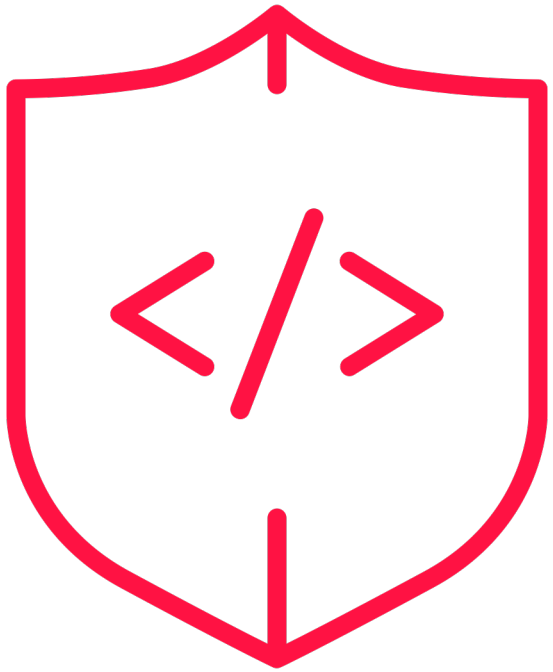
AppSec Demo

RCE via legacy dependency in Python

Reduce cybersecurity risk in Equinor's SDLC



AppSec

https://appsec.equinor.com

Example Problem

CONTEXT

- Reservoir simulation software that is configured using *yaml* files
- The simulator is tested and reliable, but old and hard to maintain
- Data is *restricted,* all the processing must happen in a confined environment

REQUIREMENTS

- Build a simple tool to check that *yaml* configurations are valid
- Validation performed via a library that comes with the simulator
- Only *Python v3.4* is available in the confined environment

DEMO #1

How hard can it be?

Awesome!

- That was easy, time to

Awesome!

- That was easy, time to
  - Deploy
  - Host a demo for my colleagues

Awesome!

- That was easy, time to
  - Deploy
  - Host a demo for my colleagues
  - Add an *Achievement* to my People@Equinor
  - Take a selfie and post it on LinkedIn

Awesome!

- That was easy, time to
  - Deploy
  - Host a demo for my colleagues
  - Add an *Achievement* to my People@Equinor
  - Take a selfie and post it on LinkedIn
  - Go out and celebrate!


LOCKBIT2.0
ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!
All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.
Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:
3085B89A0C515D2FB124D645906F5D3DA5CB97CE8EA975959AE4F95302A04E1D709C3C4AE9B7
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion

equinor

DEMO #2

WTF?!

DEMO #3

Let’s take some precautions

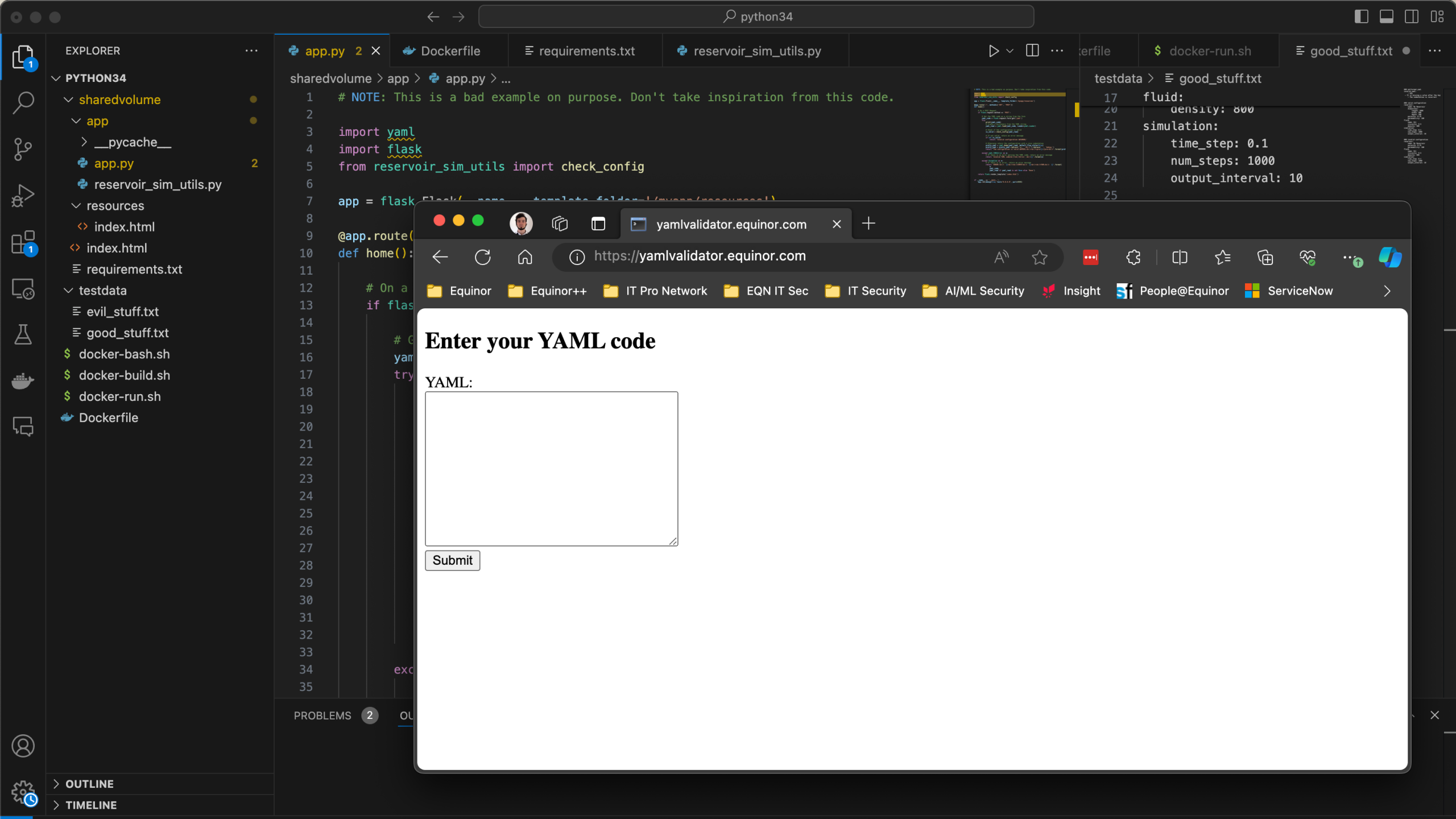
Key Takeaways

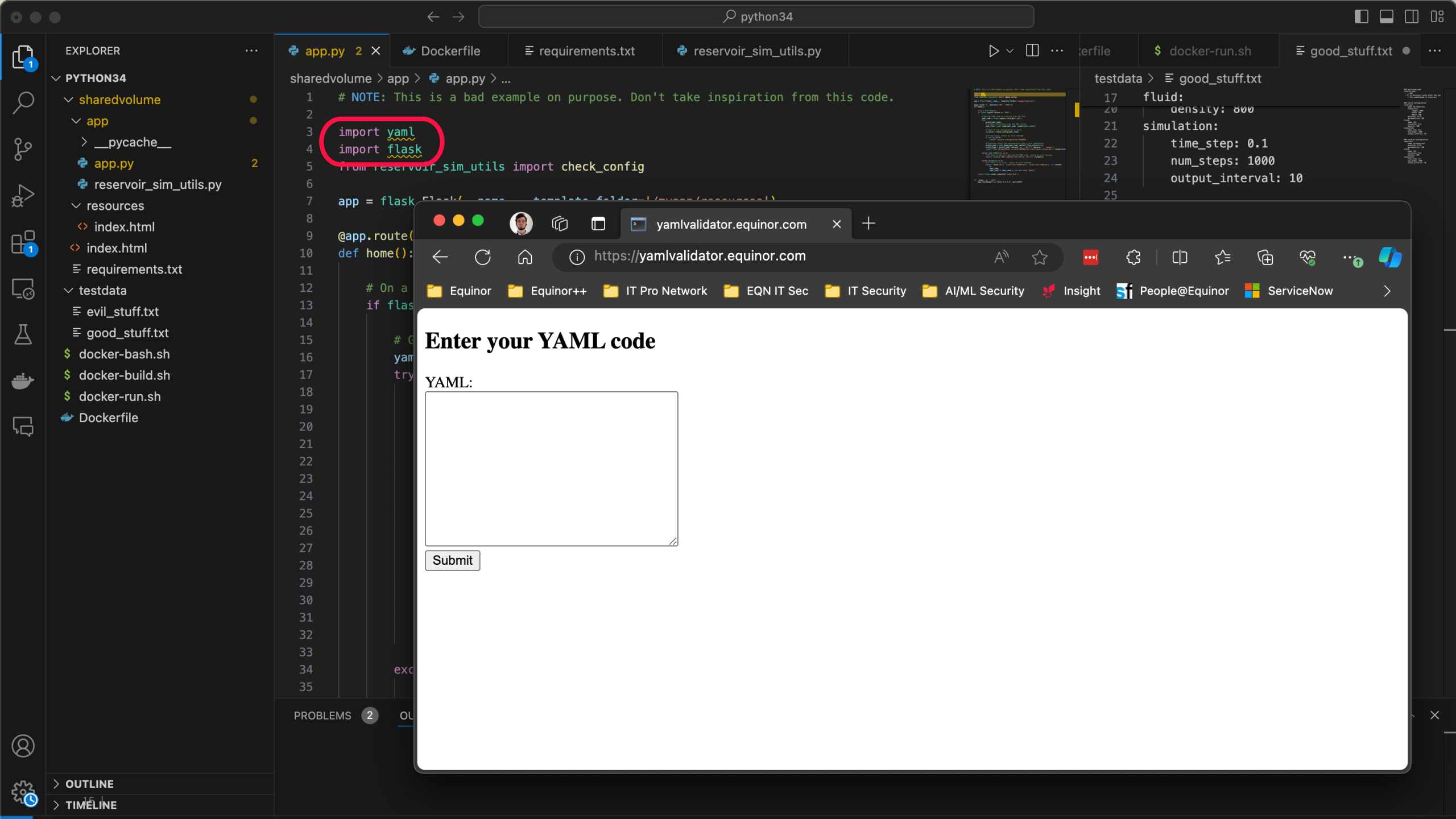
- When you write your own code …
  - Use *Snyk Code* in your IDE

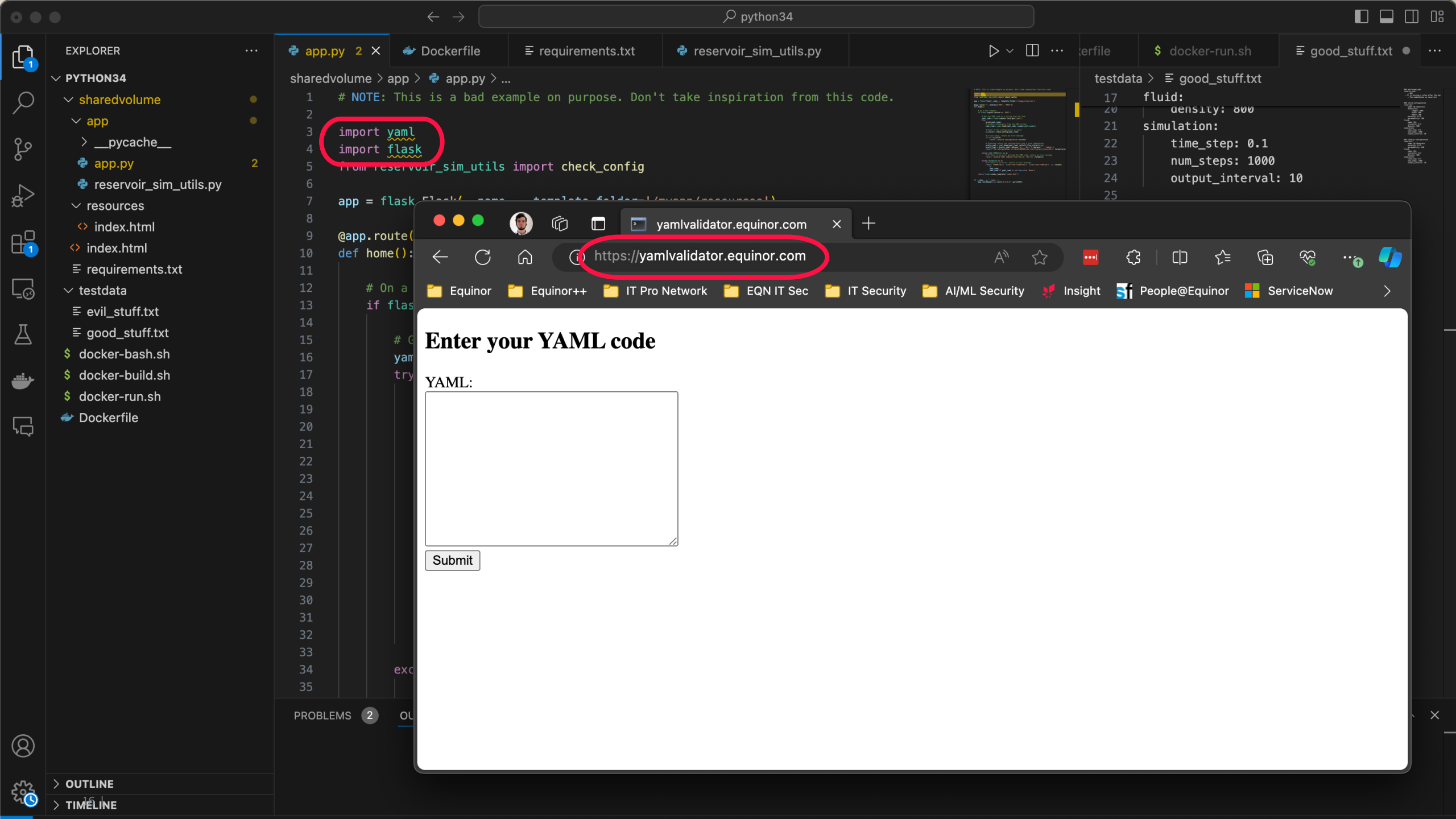
- When you use 3rd party libraries …
  - Use *Snyk Open Source* for checking your dependencies
  - Configure Snyk for monitoring your deployments
  - Establish routines for regularly updating libraries

equinor

We are responsible for the code we write!


python34
EXPLORER
PYTHON34
sharedvolume
app
__pycache__
app.py 2
reservoir_sim_utils.py
resources
index.html
index.html
requirements.txt
testdata
evil_stuff.txt
good_stuff.txt
docker-bash.sh
docker-build.sh
docker-run.sh
Dockerfile
app.py 2
Dockerfile
requirements.txt
reservoir_sim_utils.py
docker-run.sh
good_stuff.txt
sharedvolume > app > app.py > ...
1 # NOTE: This is a bad example on purpose. Don't take inspiration from this code.
3 import yaml
4 import flask
5 from reservoir_sim_utils import check_config
7 app = flask.Flask(__name__, template_folder='/myapp/resources')
9 @app.route(
10 def home():
12 # On a
13 if flas
15 # C
16 yam
17 try
34 exc
testdata > good_stuff.txt
17 fluid:
20 density: 800
21 simulation:
22 time_step: 0.1
23 num_steps: 1000
24 output_interval: 10
25
PROBLEMS 2
OUTLINE
TIMELINE
yamlvalidator.equinor.com
https://yamlvalidator.equinor.com
Equinor
Equinor++
IT Pro Network
EQN IT Sec
IT Security
AI/ML Security
Insight
People@Equinor
ServiceNow
Enter your YAML code
YAML:
Submit


python34
EXPLORER
PYTHON34
sharedvolume
app
__pycache__
app.py 2
reservoir_sim_utils.py
resources
index.html
index.html
requirements.txt
testdata
evil_stuff.txt
good_stuff.txt
docker-bash.sh
docker-build.sh
docker-run.sh
Dockerfile
app.py 2
Dockerfile
requirements.txt
reservoir_sim_utils.py
docker-run.sh
good_stuff.txt
sharedvolume > app > app.py > ...
1 # NOTE: This is a bad example on purpose. Don't take inspiration from this code.
3 import yaml
4 import flask
5 from reservoir_sim_utils import check_config
7 app = flask.Flask(__name__, template_folder='/myapp/resources')
9 @app.route('/')
10 def home():
testdata > good_stuff.txt
17 fluid:
20 density: 800
21 simulation:
22 time_step: 0.1
23 num_steps: 1000
24 output_interval: 10
25
yamlvalidator.equinor.com
https://yamlvalidator.equinor.com
Equinor
Equinor++
IT Pro Network
EQN IT Sec
IT Security
AI/ML Security
Insight
People@Equinor
ServiceNow
Enter your YAML code
YAML:
Submit
PROBLEMS 2
OUTLINE
TIMELINE


python34
EXPLORER
PYTHON34
sharedvolume
app
__pycache__
app.py 2
reservoir_sim_utils.py
resources
index.html
index.html
requirements.txt
testdata
evil_stuff.txt
good_stuff.txt
docker-bash.sh
docker-build.sh
docker-run.sh
Dockerfile
app.py 2
Dockerfile
requirements.txt
reservoir_sim_utils.py
docker-run.sh
good_stuff.txt
sharedvolume > app > app.py > ...
1 # NOTE: This is a bad example on purpose. Don't take inspiration from this code.
3 import yaml
4 import flask
5 from reservoir_sim_utils import check_config
7 app = flask.Flask(__name__, template_folder='/myapp/resources')
9 @app.route('/')
10 def home():
testdata > good_stuff.txt
17 fluid:
20 density: 800
21 simulation:
22 time_step: 0.1
23 num_steps: 1000
24 output_interval: 10
25
yamlvalidator.equinor.com
https://yamlvalidator.equinor.com
Equinor
Equinor++
IT Pro Network
EQN IT Sec
IT Security
AI/ML Security
Insight
People@Equinor
ServiceNow
Enter your YAML code
YAML:
Submit
PROBLEMS 2
OUTLINE
TIMELINE

AppSec Demo

RCE via legacy dependency in Python

https://appsec.equinor.com