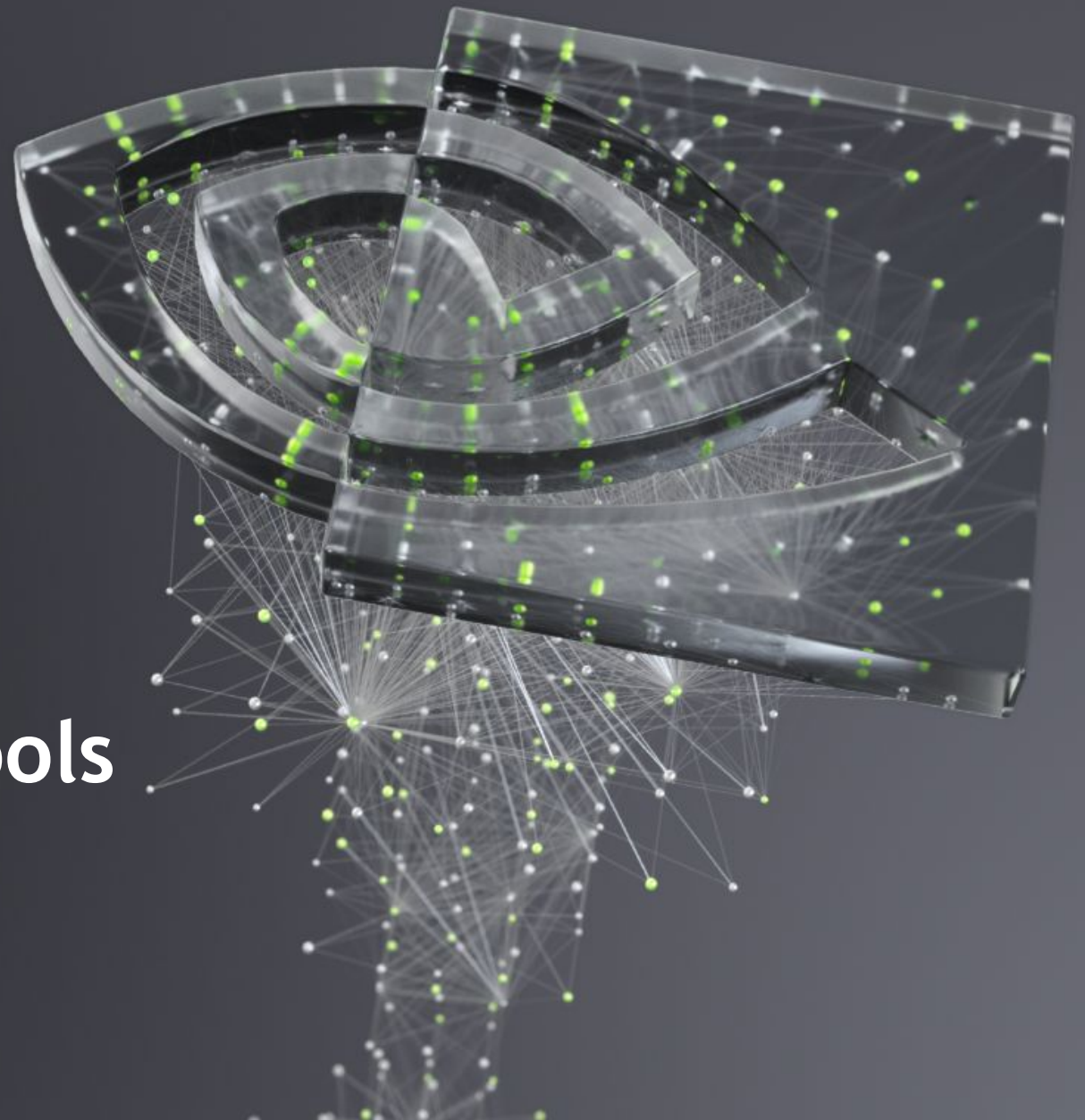


Product Security Tools Friend or Foe

FIRST - PSIRT Technical Colloquium 2020 - March 4-5

About Us

NVIDIA Product Security Tools

Adam Wallis

NVIDIA Product Security Tools Development

awallis@nvidia.com

Jessica Butler

NVIDIA Product Security Tools Development

jessicab@nvidia.com

Intro

Moving the Ball Forward

Foe - Security's Bad Reputation

Tools Developers Need *& WANT*

Friend - Delivering Actionable Results

Integrating Security into *Speed of Light* Culture

DEMO 1 - GitHub built-in vulnerability detection

DEMO 2 - pipeline vulnerability detection using *Safety*

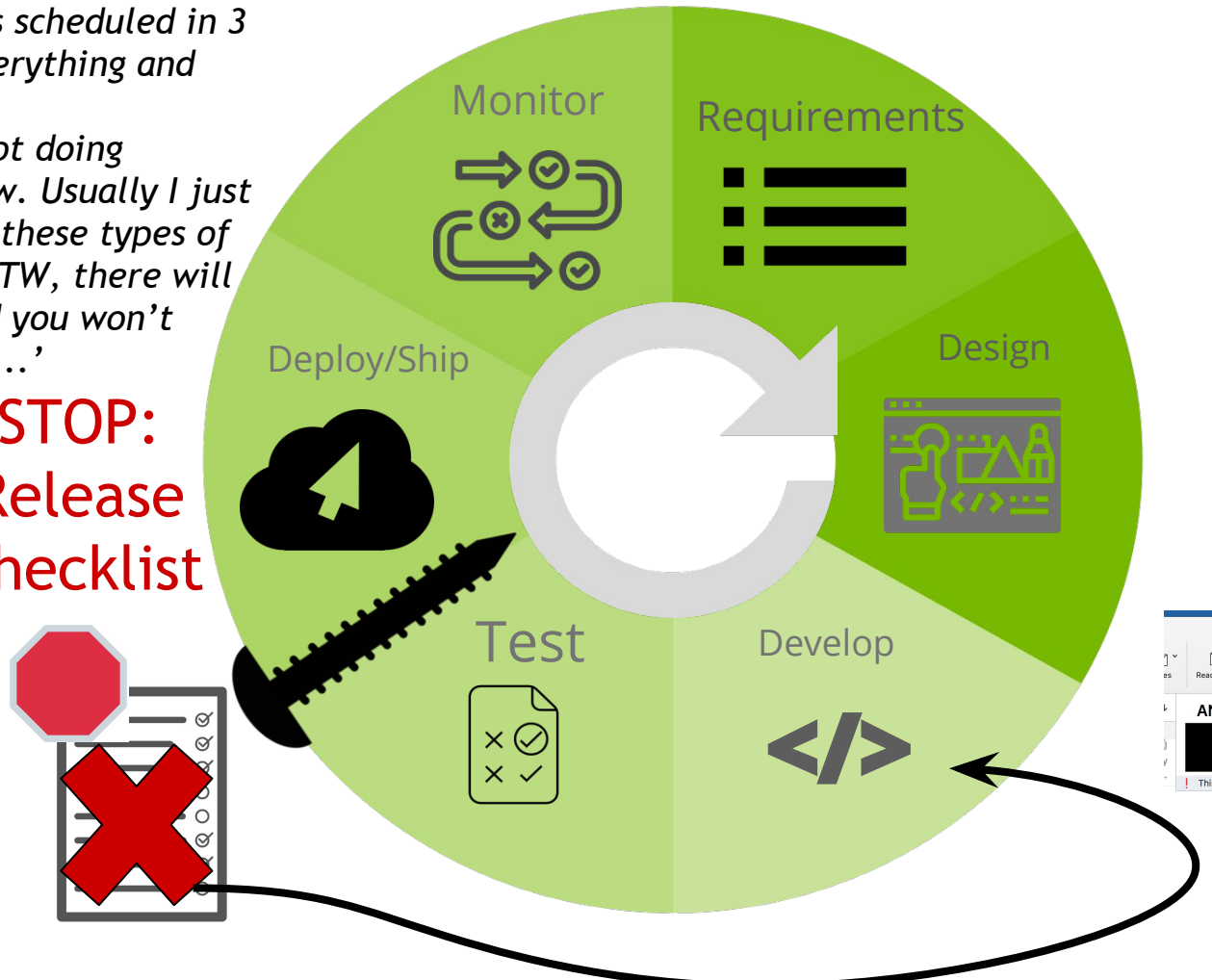
DEMO 3 - more advanced configuration using *Clair*

DEMO 4 - integrating external scanning tools like *WhiteSource BOLT*

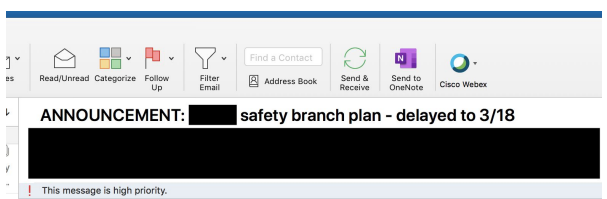
Security's Bad Rep

***Developer**: 'Release is scheduled in 3 days. Can you drop everything and help me now?!'*
***Security**: 'Sure, I'm not doing anything else right now. Usually I just sit around waiting for these types of reactive requests. :) BTW, there will probably be issues and you won't have time to fix them...'*

STOP: Release Checklist



https://gunshowcomic.com/648



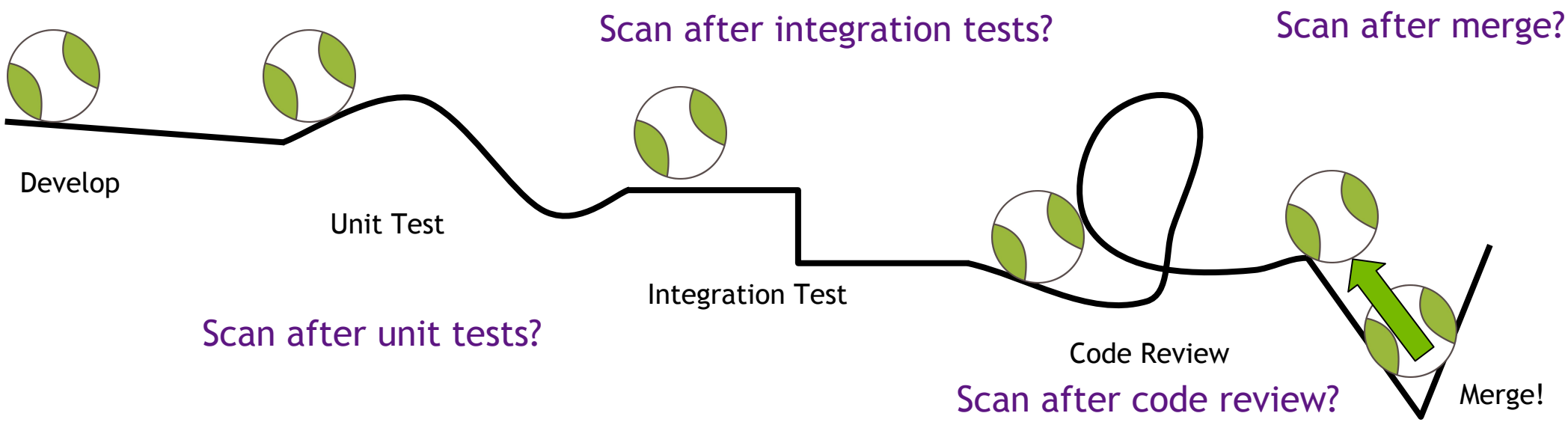
Tools Developers Need

… & *WANT*!

	Findings	examples
Open Source Security	Vulnerable Open Source Software (OSS) Dependencies	snyk, JFrog Xray, WhiteSource, BLACKDUCK
Static Analysis (SAST)	source code defects	Checkmarx, coverity
Sensitive Material Detection	detect passwords, profanity, porn	anchore
Dynamic Analysis (DAST)	input/output and configuration issues, unused ports	nexpose, CIS-CAT Pro
Container Scanning	detect vulnerabilities in image	clair, WhiteSource, JFrog Xray, BLACKDUCK

Delivering Actionable Results

Typical developer workflow using pipeline



Integrate into PIPELINE!!

INTEGRATING FOR *Speed of Light*

DEMO 1
GitHub built-in vulnerability detection

⚠ **We found a potential security vulnerability in one of your dependencies.**

Only the owner of this repository can see this message.

View security alert

requests

Dismiss

⚠ Open GitHub opened this alert 16 hours ago

Bump requests from 2.19.0 to 2.20.0 dependencies

#1 opened 16 hours ago by dependabot bot

1 **requests** vulnerability found in **requirements.txt** 16 hours ago

Remediation

Upgrade **requests** to version **`2.20.0`** or later. For example:

```
requests>=2.20.0
```

Always verify the validity and compatibility of suggestions with your codebase.

Details

CVE-2018-18074

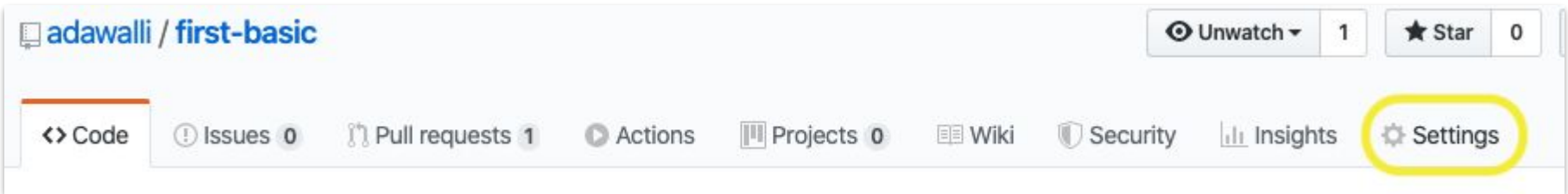
moderate severity

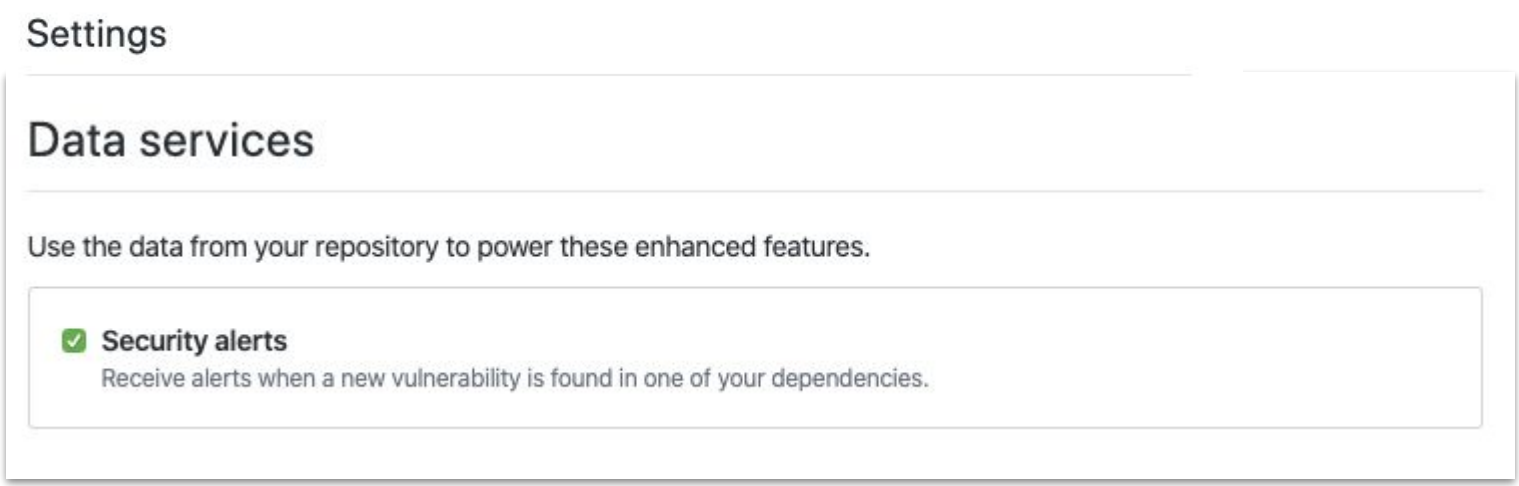
Vulnerable versions: `<= 2.19.1`
Patched version: `2.20.0`

The Requests package through 2.19.1 before 2018-09-14 for Python sends an HTTP Authorization header to an http URI upon receiving a same-hostname https-to-http redirect, which makes it easier for remote attackers to discover credentials by sniffing the network.

GitHub Vulnerability Detection

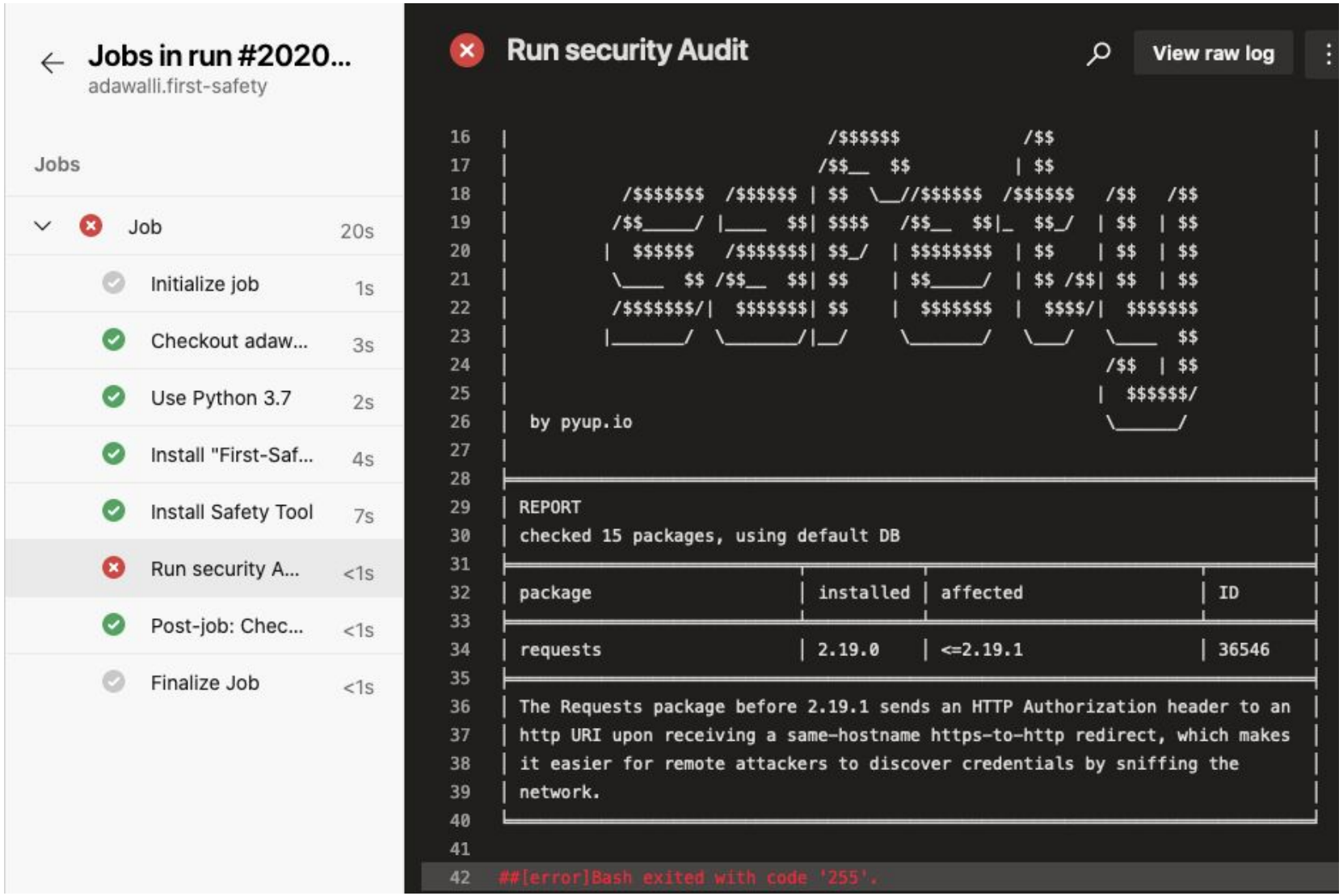
How to Enable






DEMO 2
Pipeline vulnerability
detection using *Safety*

Github + Azure Pipelines + Python Safety



Add Security Check to Azure Pipeline

Create Azure Pipeline

15 ■■■■■ azure-pipelines.yml

```
@@ -0,0 +1,15 @@
+ trigger:
+ - master
+
+ pool:
+   vmImage: 'ubuntu-latest'
+
+ steps:
+ - task: UsePythonVersion@0
+   inputs:
+     versionSpec: '3.7'
+   displayName: 'Use Python 3.7'
+
+ - script: |
+     python setup.py install
+   displayName: 'Install "First-Safety" Package'
```

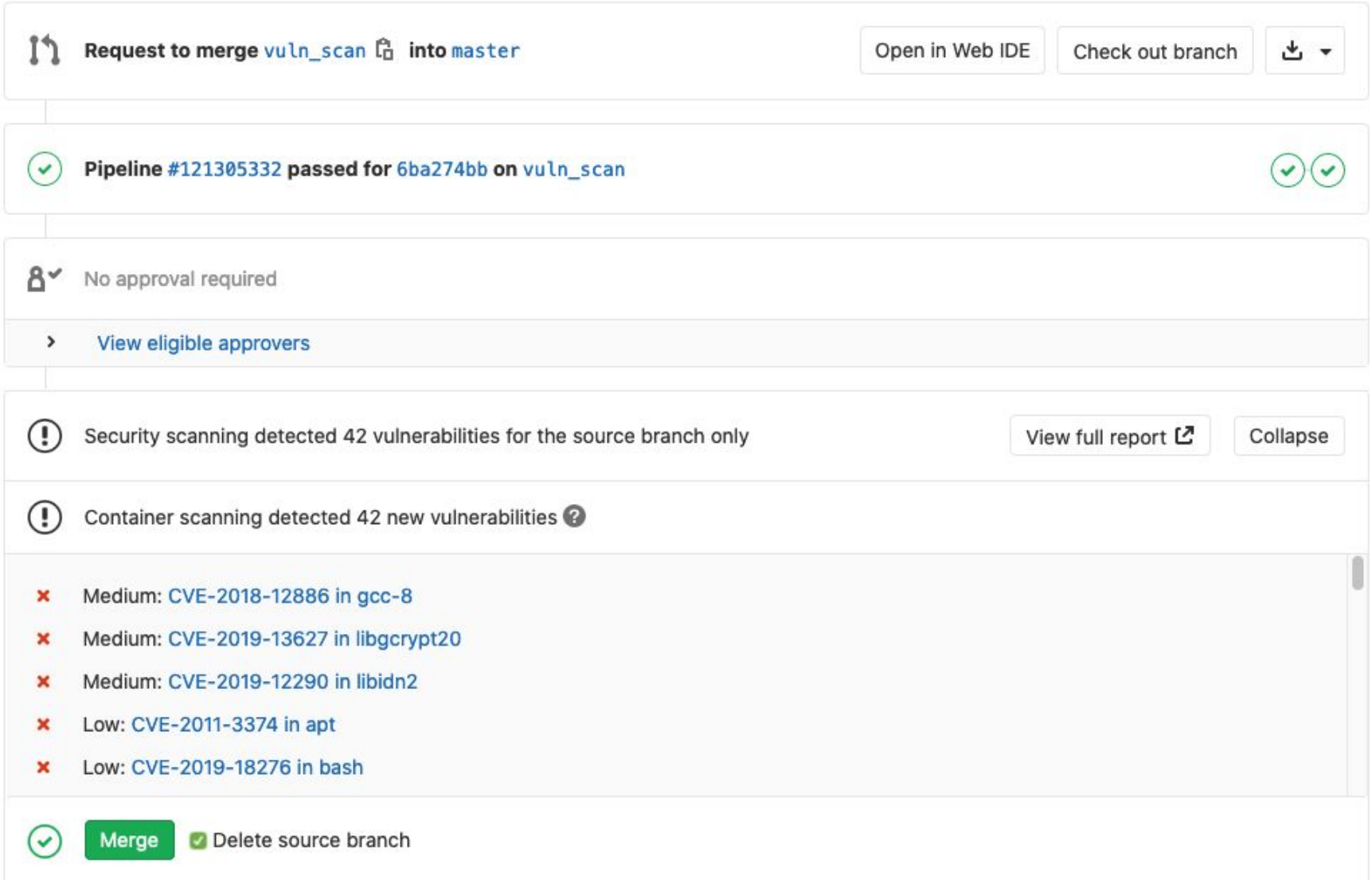
Add Vulnerability Check

8 ■■■■■ azure-pipelines.yml

```
@@ -13,3 +13,11 @@ steps:
  - script: |
      python setup.py install
    displayName: 'Install "First-Safety" Package'
+
+ - script: |
+     pip install safety
+   displayName: 'Install Safety Tool'
+
+ - script: |
+     safety check --full-report
+   displayName: 'Run security Audit'
```


DEMO 3
GitLab container scanning
with *Clair*

Container Scanning with Gitlab



Add Container Scanning to Gitlab Pipeline

Create Gitlab Pipeline

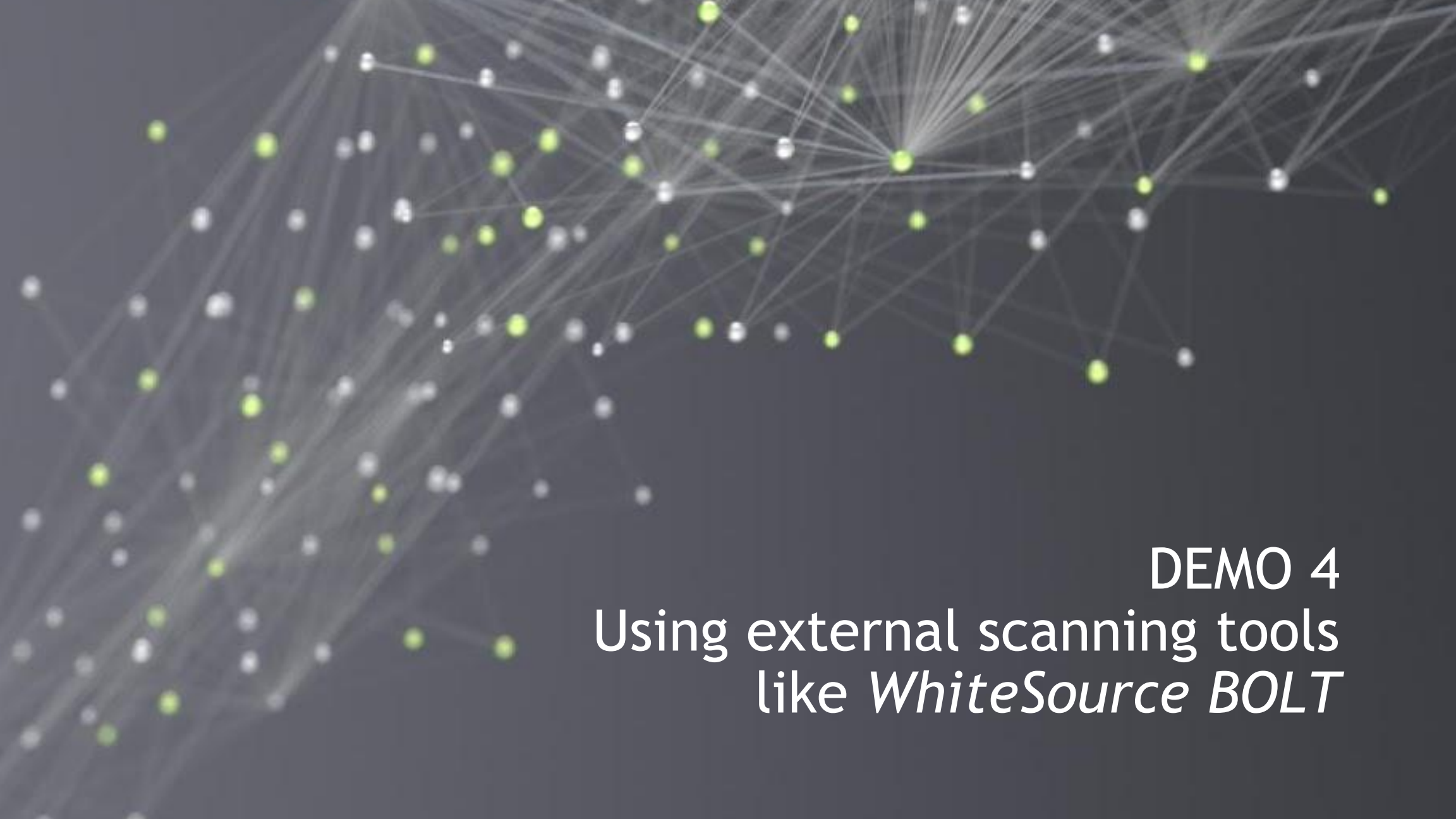
.gitlab-ci.yml 0 → 100644 — View file @ a14b2686

```
+ variables:
+   DOCKER_DRIVER: overlay2
+
+ services:
+   - docker:stable-dind
+
+ build:
+   image: docker:stable
+   tags:
+     - docker
+   stage: build
+   variables:
+     IMAGE_TAG: $CI_REGISTRY_IMAGE/$CI_COMMIT_REF_SLUG:$CI_COMMIT_SHA
+   before_script:
+     - |
+       docker login -u $CI_REGISTRY_USER \
+                    -p $CI_REGISTRY_PASSWORD $CI_REGISTRY
+   script:
+     - docker build -t "${IMAGE_TAG}" .
+     - docker push "${IMAGE_TAG}"
```

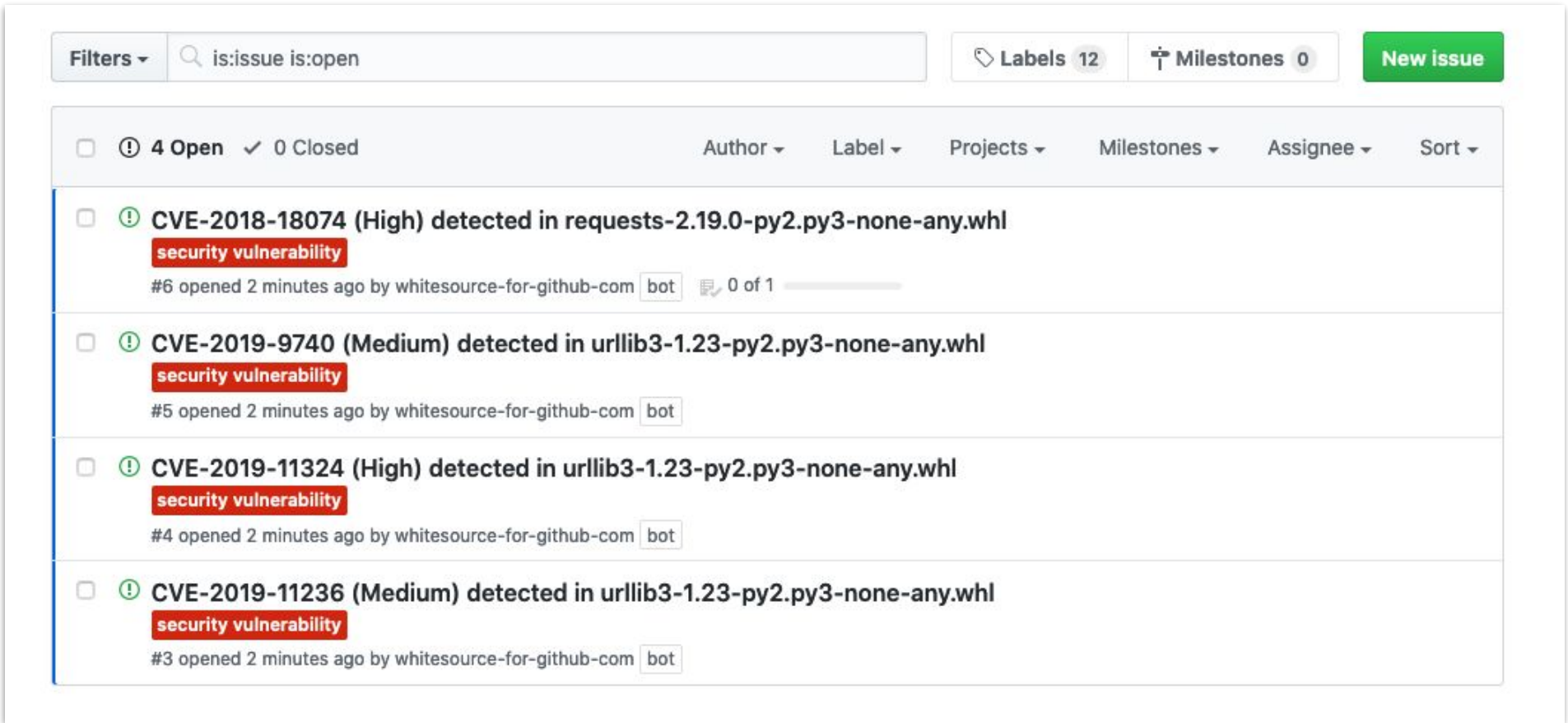
Add Security Scanning

.gitlab-ci.yml — View file @ 6ba274bb

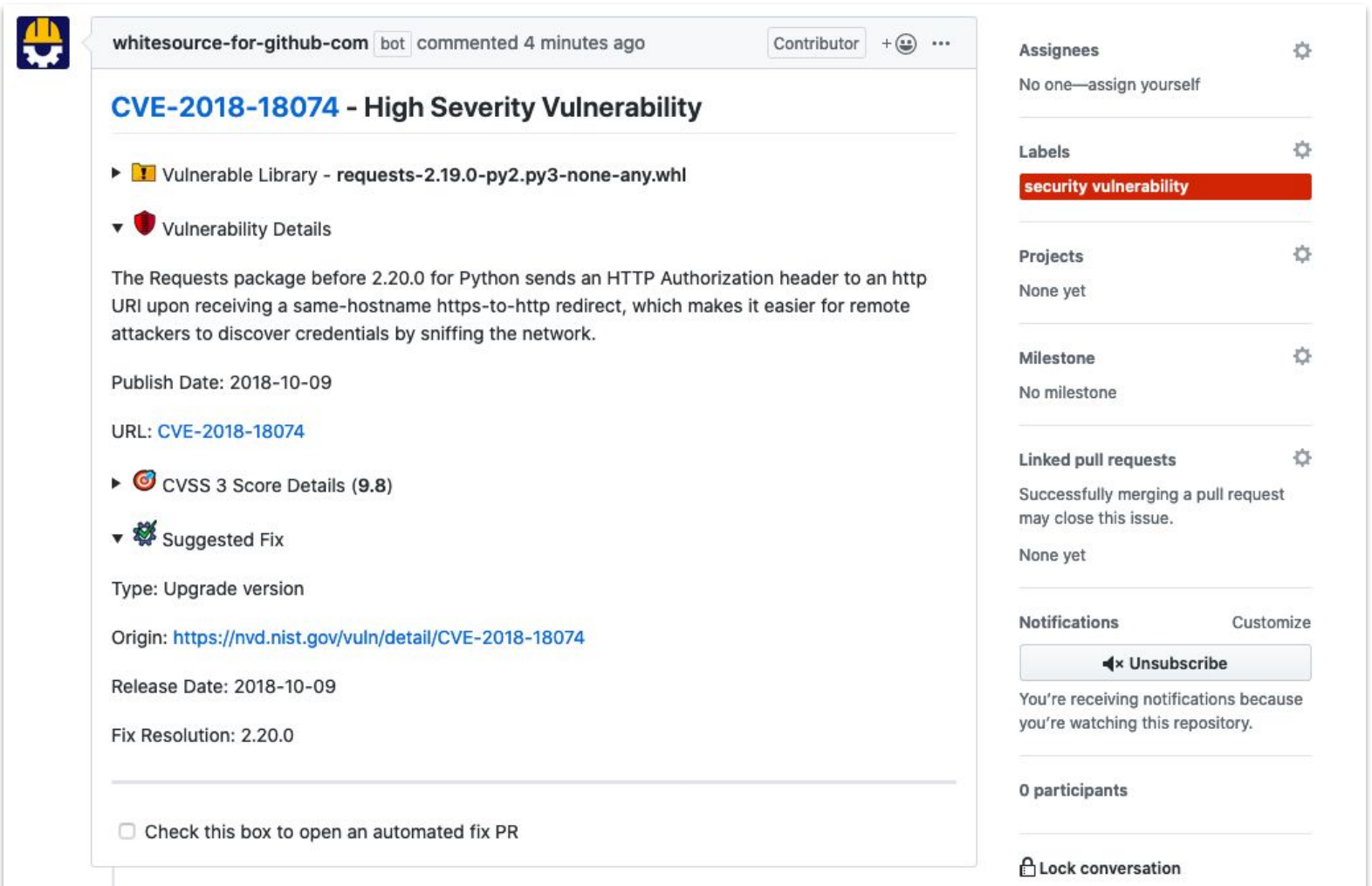
```
@@ -4,6 +4,9 @@ variables:
 services:
   - docker:stable-dind

+ include:
+   - template: Container-Scanning.gitlab-ci.yml
+
 build:
   image: docker:stable
   tags:
```


DEMO 4
Using external scanning tools
like *WhiteSource BOLT*

Automated Issue Creation for Vulnerabilities



Issue Detail with Optional Automated PR



whitesource-for-github-com bot commented 4 minutes ago Contributor

CVE-2018-18074 - High Severity Vulnerability

▶ Vulnerable Library - **requests-2.19.0-py2.py3-none-any.whl**

▼ Vulnerability Details

The Requests package before 2.20.0 for Python sends an HTTP Authorization header to an http URI upon receiving a same-hostname https-to-http redirect, which makes it easier for remote attackers to discover credentials by sniffing the network.

Publish Date: 2018-10-09

URL: CVE-2018-18074

▶ CVSS 3 Score Details (**9.8**)

▼ Suggested Fix

Type: Upgrade version

Origin: https://nvd.nist.gov/vuln/detail/CVE-2018-18074

Release Date: 2018-10-09

Fix Resolution: 2.20.0

☐ Check this box to open an automated fix PR

Assignees

No one—assign yourself

Labels

security vulnerability

Projects

None yet

Milestone

No milestone

Linked pull requests

Successfully merging a pull request may close this issue.

None yet

Notifications Customize

Unsubscribe

You're receiving notifications because you're watching this repository.

0 participants

Lock conversation

Summary

Shift your security left to move the ball forward!

- **Easily** enable Open Source vulnerability detection using GitHub & dependebot!
  - Github Built In security: https://github.com/adawalli/first-basic
- **Try Out** Safety for Python and **Add** it to an Azure DevOps pipeline
  - Github + Azure + Safety Package: https://github.com/adawalli/first-safety
- **Scanning containers** with Clair is as simple as adding a single line!
  - Gitlab + Clair Container Scanning: https://gitlab.com/adawalli/first-clair
- Transitive **dependency vulnerability detection** is delivered with WhiteSource Bolt
  - Github + Whitesource Bolt: https://github.com/adawalli/first-bolt

Technologies Used In Demo

- Whitesource Bolt
  - https://bolt.whitesourcesoftware.com/
- Whitesource Unified Agent
  - https://www.whitesourcesoftware.com/free-trial-request/
- Python Safety Package
  - https://github.com/pyupio/safety
- Azure Pipelines
  - https://azure.microsoft.com/en-us/services/devops/pipelines/
- Github Security
  - https://github.com/security
- Gitlab + Clair
  - https://docs.gitlab.com/ee/user/application_security/container_scanning/

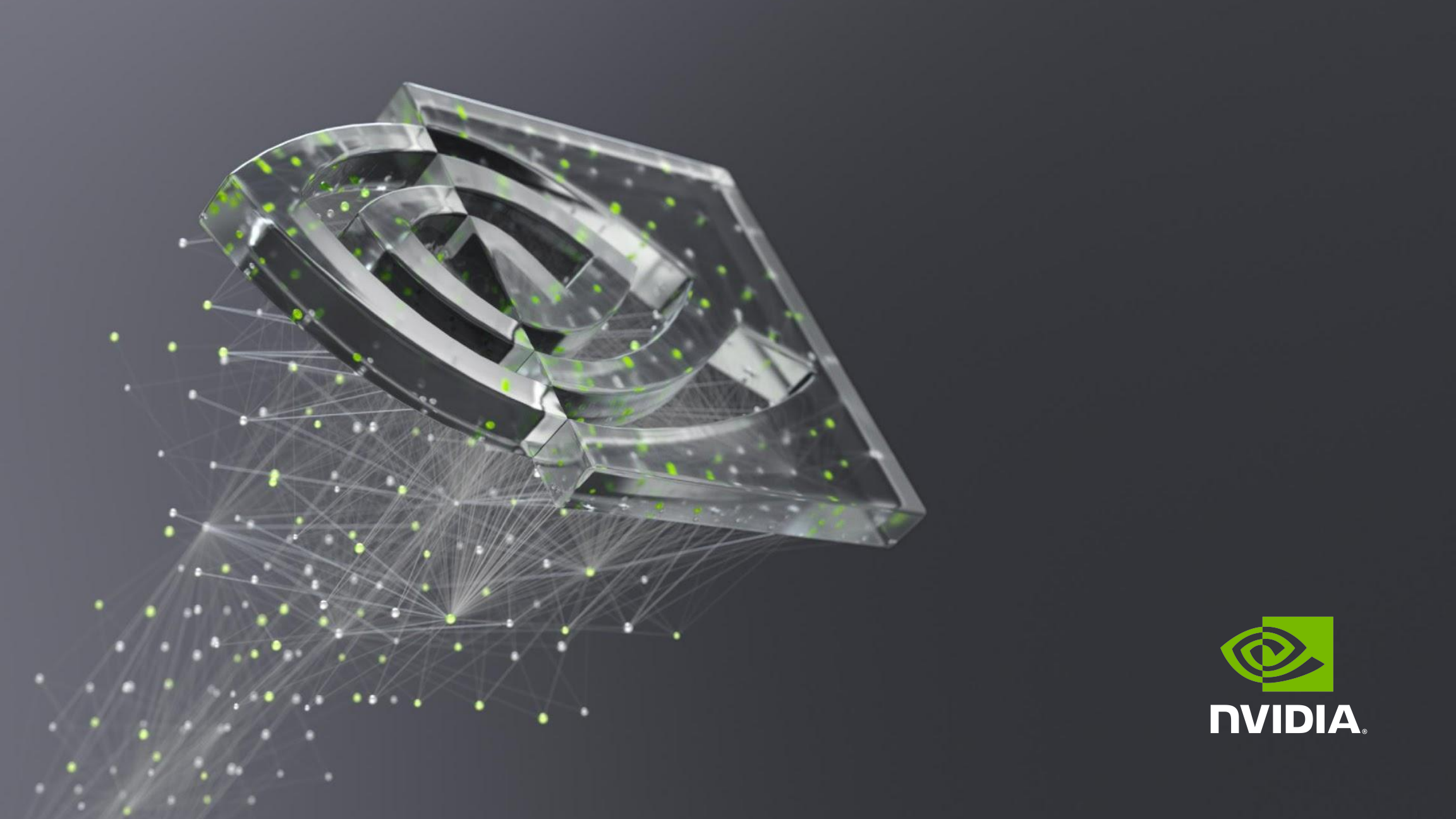
THANK YOU!

Comments, Questions, Follow-UP!

We love chatting with other Security Tools developers to knowledge share. Please contact us if you're interested in learning more or sharing!!

awallis@nvidia.com

jessicab@nvidia.com


NVIDIA