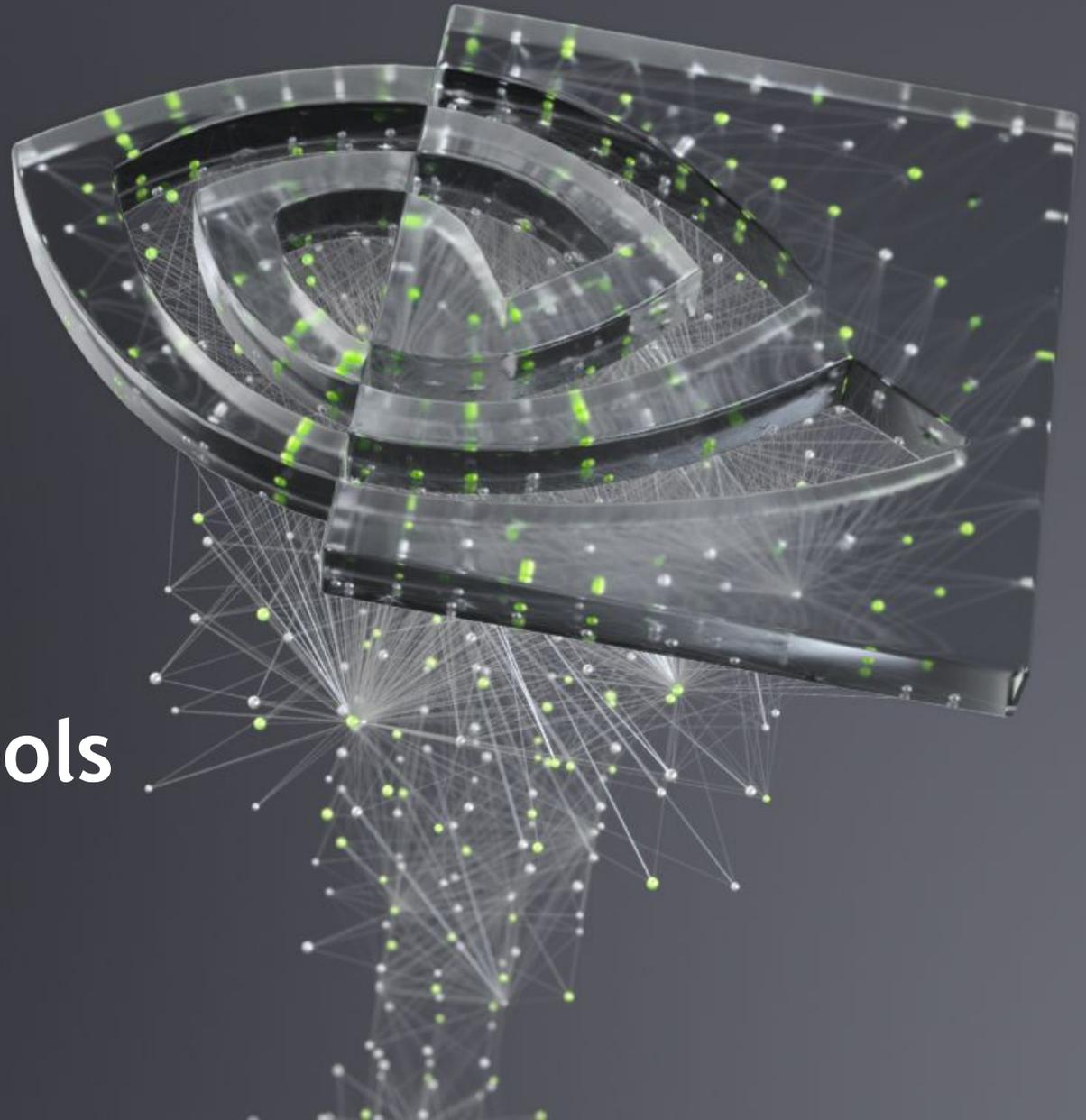




Product Security Tools Friend or Foe

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*

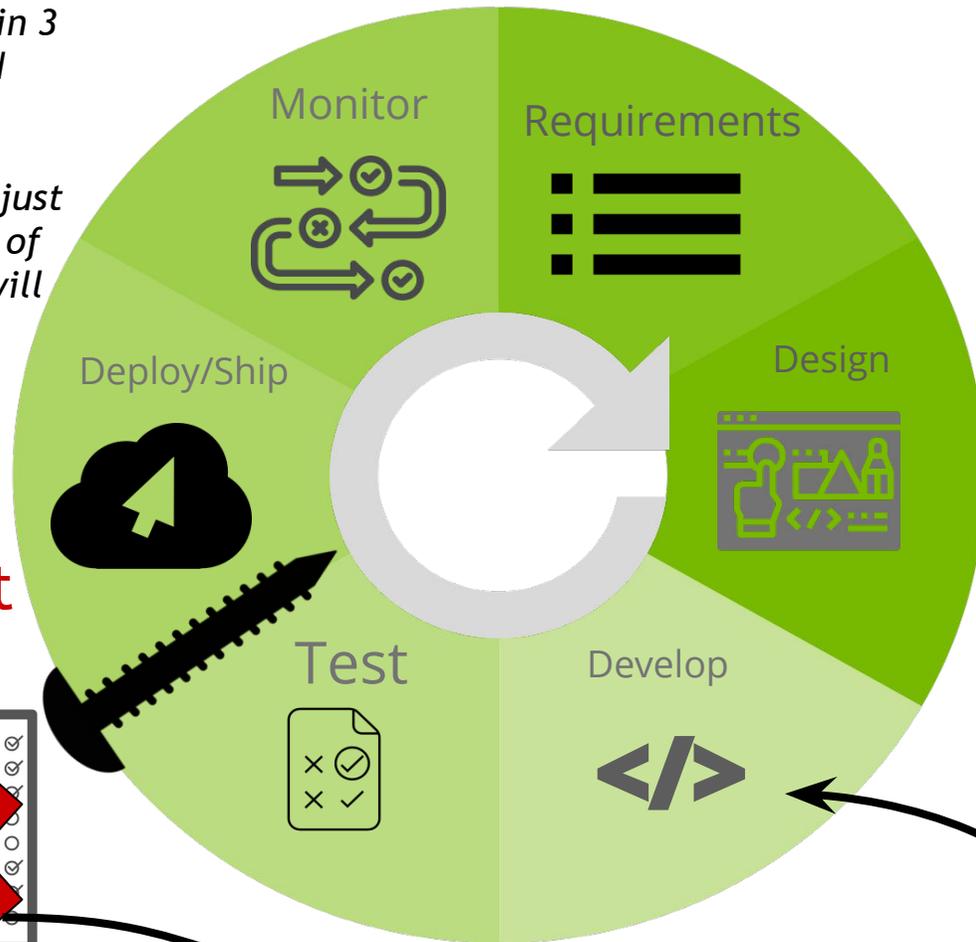
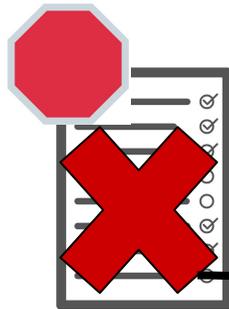
DEMO 4 - integrating external scanning tools like *WhiteSource BOLT*

Security's Bad Rep

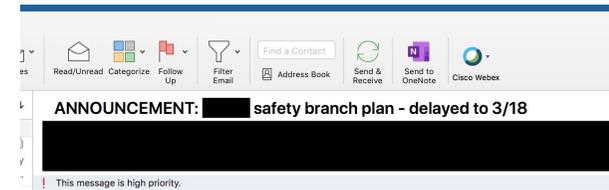
Developer: 'Release is scheduled in 3 days. Can you drop everything and help me now?!'

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>

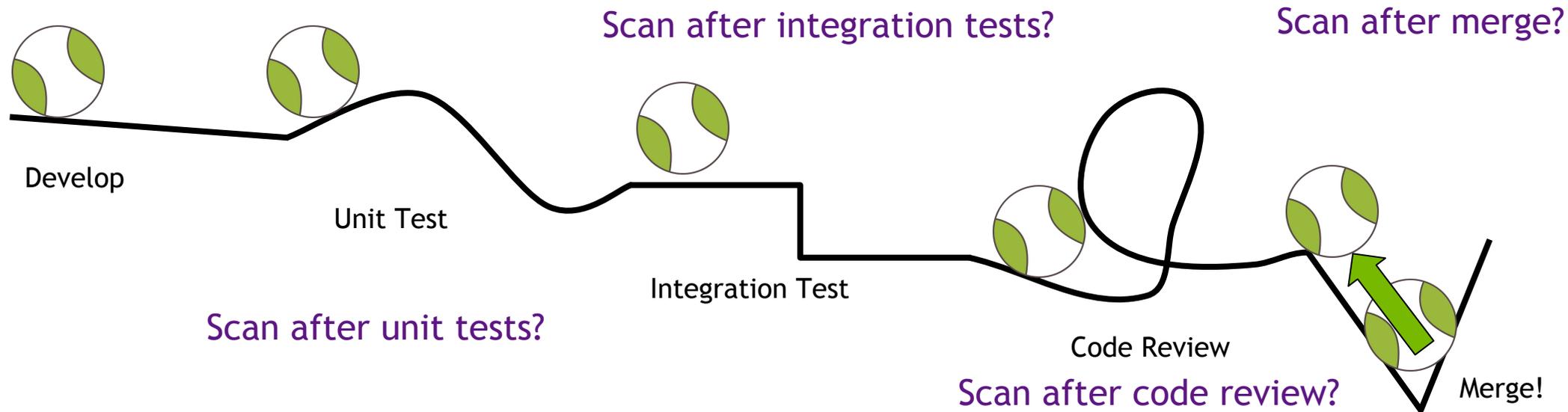


Tools Developers Need ... & WANT!

	Findings	examples
Open Source Security	Vulnerable Open Source Software (OSS) Dependencies	   
Static Analysis (SAST)	source code defects	 
Sensitive Material Detection	detect passwords, profanity, porn	
Dynamic Analysis (DAST)	input/output and configuration issues, unused ports	 
Container Scanning	detect vulnerabilities in image	   

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

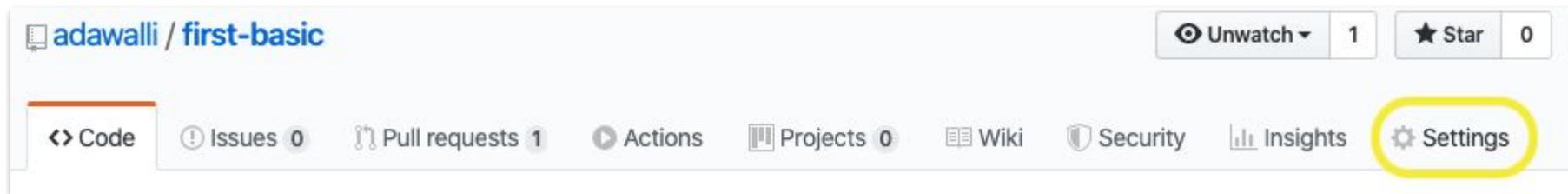
Vulnerable versions: <= 2.19.1

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



Settings

Data services

Use the data from your repository to power these enhanced features.

- Security alerts**
Receive alerts when a new vulnerability is found in one of your dependencies.



DEMO 2
Pipeline vulnerability
detection using *Safety*

Github + Azure Pipelines + Python Safety

The image shows a screenshot of the Azure Pipelines interface. On the left, a list of jobs is shown for a run titled 'Jobs in run #2020...' by 'adawalli.first-safety'. The jobs are:

- Initialize job (1s)
- Checkout adaw... (3s)
- Use Python 3.7 (2s)
- Install "First-Saf..." (4s)
- Install Safety Tool (7s)
- Run security A... (<1s) - This job is marked as failed with a red 'x' icon.
- Post-job: Chec... (<1s)
- Finalize Job (<1s)

The right side of the image shows the raw log for the failed 'Run security Audit' step. The log content is as follows:

```
16 | /$$$$$ /$$
17 | /$$_ $$ | $$
18 | /$$$$$ /$$$$$ | $$ \_//$$$$$ /$$$$$ /$$ /$$
19 | /$$___/ |___ $$| $$$ /$$_ $$|_ $$/ | $$ | $$
20 | $$$$$ /$$$$$| $$/ | $$$$$$ | $$ | $$ | $$
21 | \_ $$ /$$_ $$| $$ | $$___/ | $$ /$$| $$ | $$
22 | /$$$$$/| $$$$$$| $$ | $$$$$$ | $$$$/| $$$$$$
23 | _____/ \_____/|/ \_____/ \_____/ \_____ $$
24 | /$$ | $$
25 | | $$$$$/
26 | by pyup.io
27 |
28 |
29 | REPORT
30 | checked 15 packages, using default DB
31 |
32 | package | installed | affected | ID
33 |
34 | requests | 2.19.0 | <=2.19.1 | 36546
35 |
36 | The Requests package before 2.19.1 sends an HTTP Authorization header to an
37 | http URI upon receiving a same-hostname https-to-http redirect, which makes
38 | it easier for remote attackers to discover credentials by sniffing the
39 | network.
40 |
41 |
42 | ##[error]Bash exited with code '255'.
```

Add Security Check to Azure Pipeline

Create Azure Pipeline

```
▼ 15 █████ azure-pipelines.yml 📄
...  ...  @@ -0,0 +1,15 @@
1  + trigger:
2  + - master
3  +
4  + pool:
5  +   vmImage: 'ubuntu-latest'
6  +
7  + steps:
8  + - task: UsePythonVersion@0
9  +   inputs:
10 +     versionSpec: '3.7'
11 +     displayName: 'Use Python 3.7'
12 +
13 + - script: |
14 +   python setup.py install
15 +   displayName: 'Install "First-Safety" Package'
```

Add Vulnerability Check

```
▼ 8 █████ azure-pipelines.yml 📄
...  ...  @@ -13,3 +13,11 @@ steps:
13  13  - script: |
14  14      python setup.py install
15  15      displayName: 'Install "First-Safety" Package'
16  +
17  + - script: |
18  +   pip install safety
19  +   displayName: 'Install Safety Tool'
20  +
21  + - script: |
22  +   safety check --full-report
23  +   displayName: 'Run security Audit'
```



DEMO 3
GitLab container scanning
with *Clair*

Container Scanning with Gitlab

 Request to merge `vuln_scan` into `master` Open in Web IDE Check out branch  ▾

 Pipeline #121305332 passed for 6ba274bb on vuln_scan  

 No approval required

[View eligible approvers](#)

 Security scanning detected 42 vulnerabilities for the source branch only View full report  Collapse

 Container scanning detected 42 new vulnerabilities 

-  Medium: [CVE-2018-12886](#) in `gcc-8`
-  Medium: [CVE-2019-13627](#) in `libgcrypt20`
-  Medium: [CVE-2019-12290](#) in `libidn2`
-  Low: [CVE-2011-3374](#) in `apt`
-  Low: [CVE-2019-18276](#) in `bash`

 Merge  Delete source branch

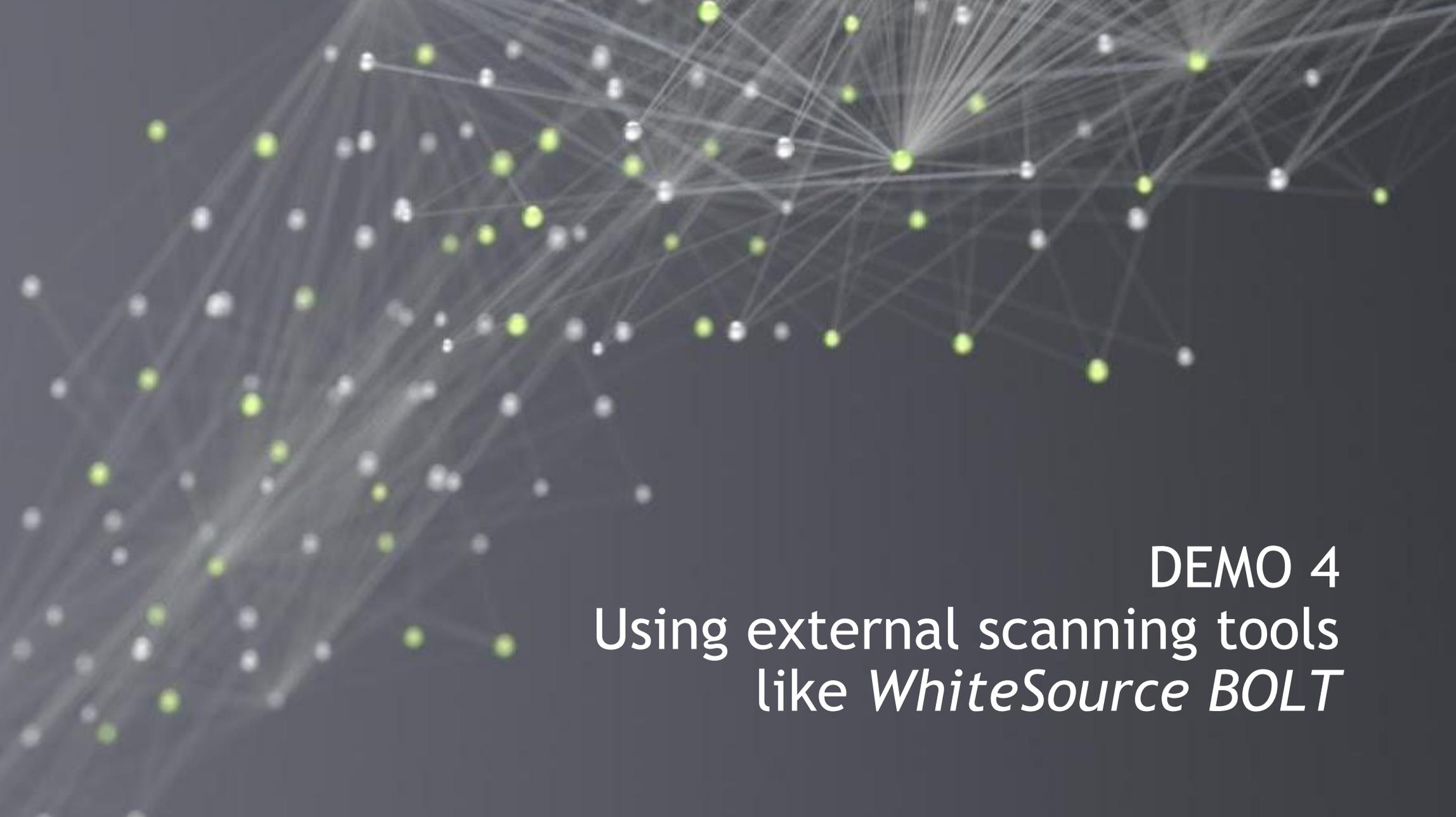
Add Container Scanning to Gitlab Pipeline

Create Gitlab Pipeline

```
▼ .gitlab-ci.yml 0 → 100644 📄 View file @ a14b2686
1 + variables:
2 +   DOCKER_DRIVER: overlay2
3 +
4 + services:
5 +   - docker:stable-dind
6 +
7 + build:
8 +   image: docker:stable
9 +   tags:
10 +     - docker
11 +   stage: build
12 +   variables:
13 +     IMAGE_TAG: $CI_REGISTRY_IMAGE/$CI_COMMIT_REF_SLUG:$CI_COMMIT_SHA
14 +   before_script:
15 +     - |
16 +       docker login -u $CI_REGISTRY_USER \
17 +         -p $CI_REGISTRY_PASSWORD $CI_REGISTRY
18 +   script:
19 +     - docker build -t "${IMAGE_TAG}" .
20 +     - docker push "${IMAGE_TAG}"
```

Add Security Scanning

```
▼ .gitlab-ci.yml 📄 View file @ 6ba274bb
...  ... @@ -4,6 +4,9 @@ variables:
4 4  services:
5 5  - docker:stable-dind
6 6
7 + include:
8 +   - template: Container-Scanning.gitlab-ci.yml
9 +
7 10  build:
8 11  image: docker:stable
9 12  tags:
```



DEMO 4
Using external scanning tools
like *WhiteSource BOLT*

Automated Issue Creation for Vulnerabilities

Filters Labels 12 Milestones 0 [New Issue](#)

4 Open 0 Closed Author Label Projects Milestones Assignee Sort

- CVE-2018-18074 (High) detected in requests-2.19.0-py2.py3-none-any.whl**
security vulnerability
#6 opened 2 minutes ago by whitesource-for-github-com bot 0 of 1
- CVE-2019-9740 (Medium) detected in urllib3-1.23-py2.py3-none-any.whl**
security vulnerability
#5 opened 2 minutes ago by whitesource-for-github-com bot
- CVE-2019-11324 (High) detected in urllib3-1.23-py2.py3-none-any.whl**
security vulnerability
#4 opened 2 minutes ago by whitesource-for-github-com bot
- CVE-2019-11236 (Medium) detected in urllib3-1.23-py2.py3-none-any.whl**
security vulnerability
#3 opened 2 minutes ago by whitesource-for-github-com bot

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](#)

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



