Lab 4 (15 min)

OVERVIEW: In this lab you will experience JFrog Advanced Security value with actual docker images scanning.

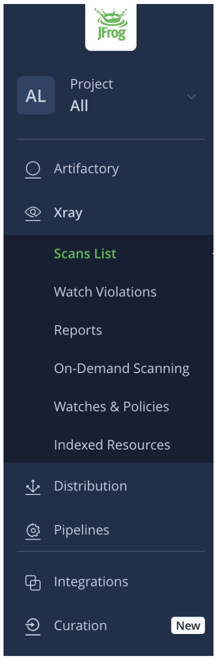
EXPECTED OUTCOME: Upon successful completion of this lab you will gain knowledge of how to use the Security issues page and extract relevant value from it

<u>Step by step instructions</u>

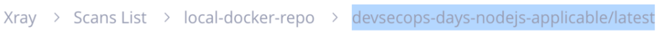
<u>Phase #1 - Inspecting the NodeJS project</u>

Note: The project we are working with has its own ‘Dockerfile’, and we have pre-built the container and pushed it to the ‘docker-local’ repository. We have done so to save time, but in a real life scenario we would of course expect the container to be one that your CI process built.

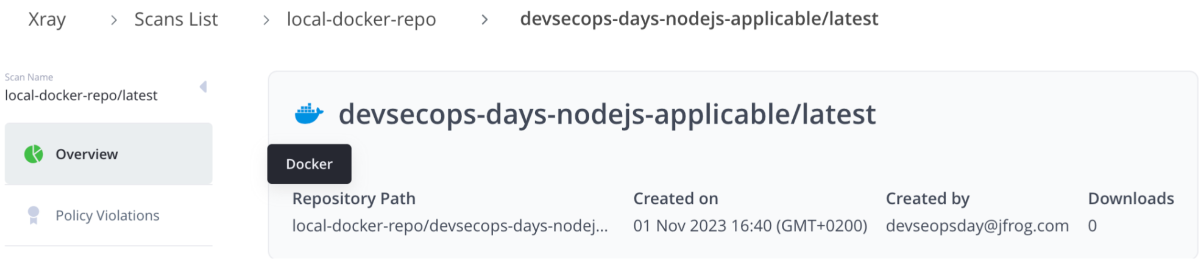
1. Open your browser and navigate to your JPD. Choose ‘Xray’ -> ‘Scans list’.



2. Choose the ‘docker-local’ repository, and the ‘devsecops-days-nodejs-applicable/latest’ container.



Xray > Scans List > local-docker-repo > devsecops-days-nodejs-applicable/latest



Xray > Scans List > local-docker-repo > devsecops-days-nodejs-applicable/latest

Scan Name
local-docker-repo/latest

Overview

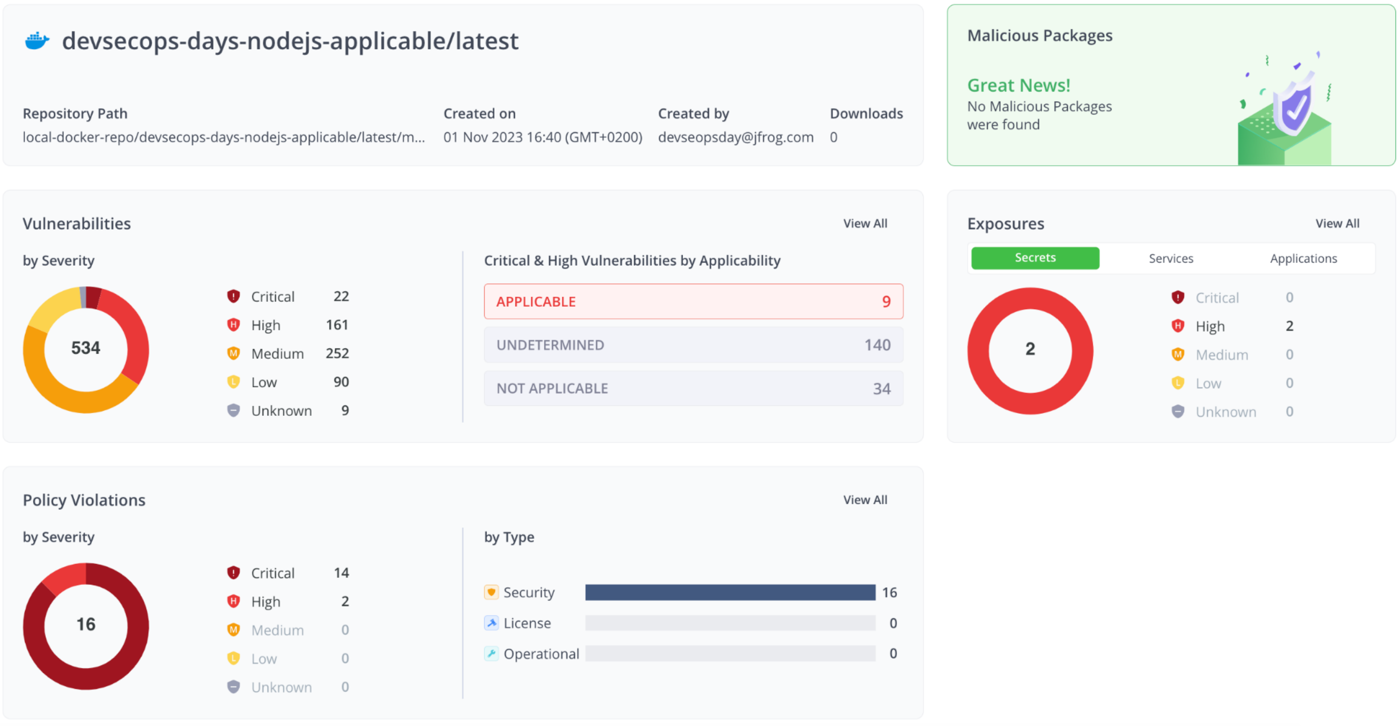
Policy Violations

devsecops-days-nodejs-applicable/latest

Docker

Repository Path	Created on	Created by	Downloads
local-docker-repo/devsecops-days-nodej...	01 Nov 2023 16:40 (GMT+0200)	devseopsday@jfrog.com	0

3. Inspect the ‘Overview’ page, which provides a summary of the components and issues of the Container.



devsecops-days-nodejs-applicable/latest

Repository Path	Created on	Created by	Downloads
local-docker-repo/devsecops-days-nodejs-applicable/latest/m...	01 Nov 2023 16:40 (GMT+0200)	devseopsday@jfrog.com	0

Malicious Packages

Great News!
No Malicious Packages were found

Vulnerabilities — View All

by Severity: 534

Severity	Count
Critical	22
High	161
Medium	252
Low	90
Unknown	9

Critical & High Vulnerabilities by Applicability

Applicability	Count
APPLICABLE	9
UNDETERMINED	140
NOT APPLICABLE	34

Exposures — View All

Secrets | Services | Applications

2

Severity	Count
Critical	0
High	2
Medium	0
Low	0
Unknown	0

Policy Violations — View All

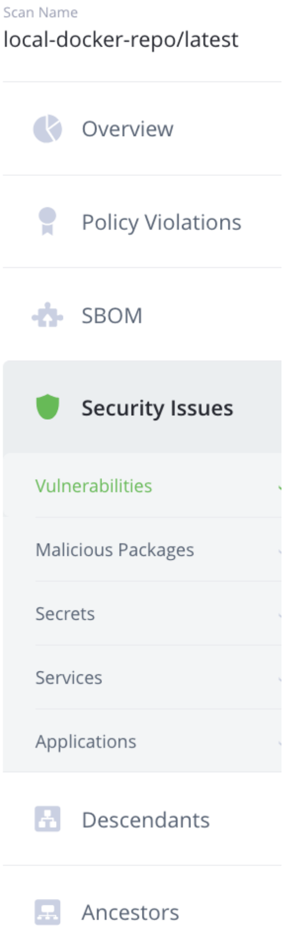
by Severity: 16

Severity	Count
Critical	14
High	2
Medium	0
Low	0
Unknown	0

by Type

Type	Count
Security	16
License	0
Operational	0

4. From the inner left bar, click on ‘Security Issues’ -> ‘Vulnerabilities’.



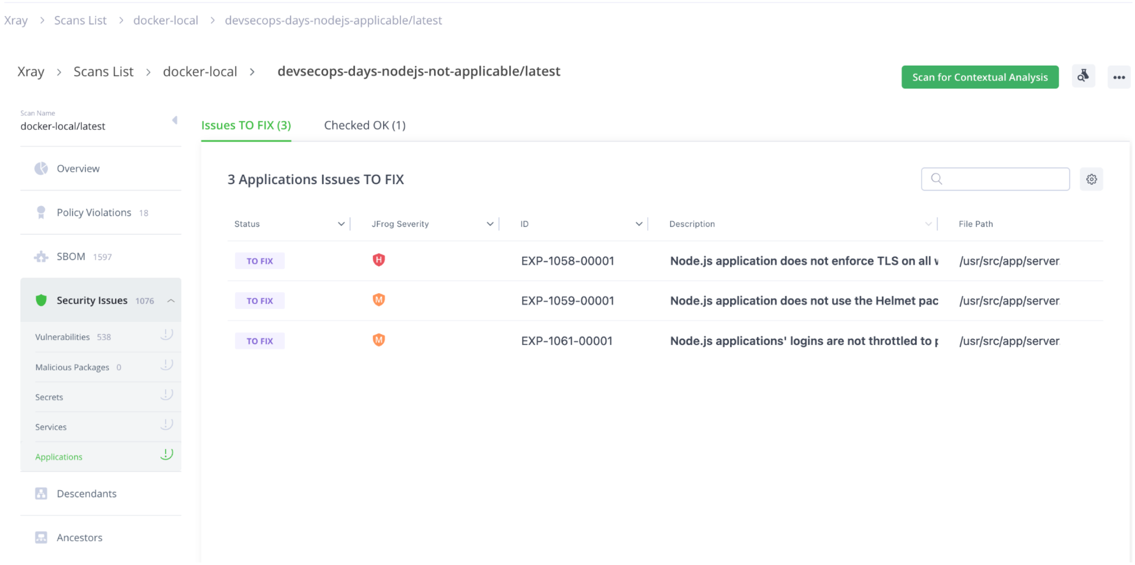
Scan Name
local-docker-repo/latest

5. Look at “*CVE-2022-29078*”
    a. Is it applicable to this docker image?
    b. What is the risk?
    c. What is the remediation process?
6. Now look at “*CVE-2020-11656*”
    a. Note the CVSS score of 9.8!
    b. Why is it not applicable to this docker image?
7. How many Critical, yet NOT APPLICABLE vulnerabilities were detected by the system?

Phase #2 - Rebuilding CVE-2022-29078

Note: We've pre-built a version of the same container, this time with the fix suggested for CVE-2022-29078

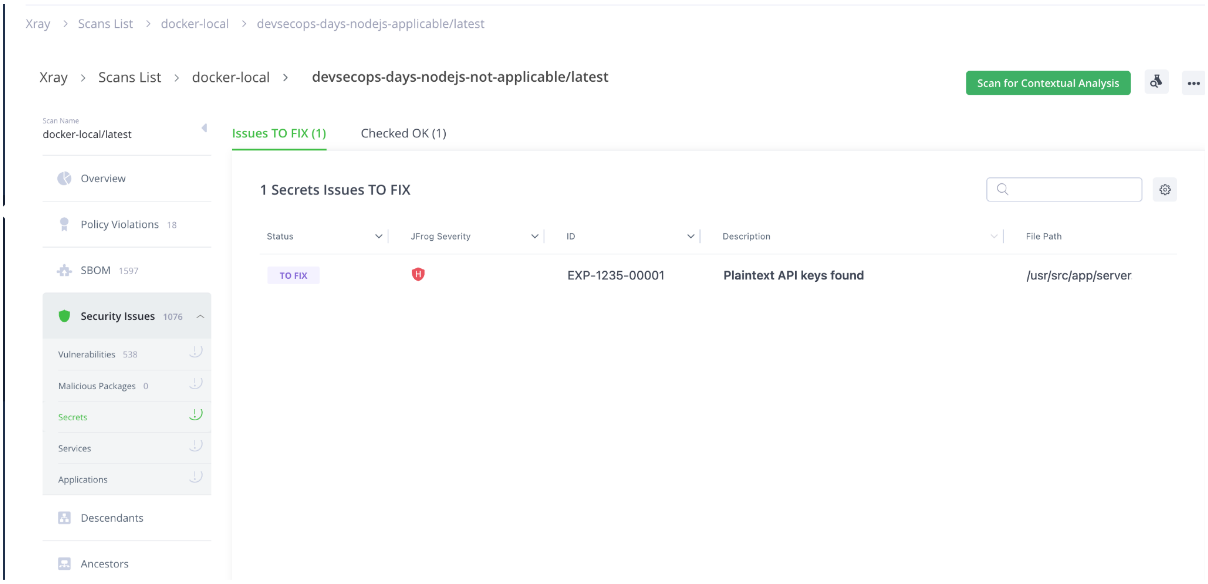
8. Go back to step 2, and this time choose 'devsecops-days-nodejs-not-applicable/latest' as your container.
    a. Is CVE-2022-29078 still marked as applicable?
9. Let's look at other data. Does your selected image have any application exposures?



3 Applications Issues TO FIX

Status	JFrog Severity	ID	Description	File Path
TO FIX	H	EXP-1058-00001	**Node.js application does not enforce TLS on all v**	/usr/src/app/server
TO FIX	M	EXP-1059-00001	**Node.js application does not use the Helmet pac**	/usr/src/app/server
TO FIX	M	EXP-1061-00001	**Node.js applications' logins are not throttled to p**	/usr/src/app/server

10. Does your selected image have any secrets detected?

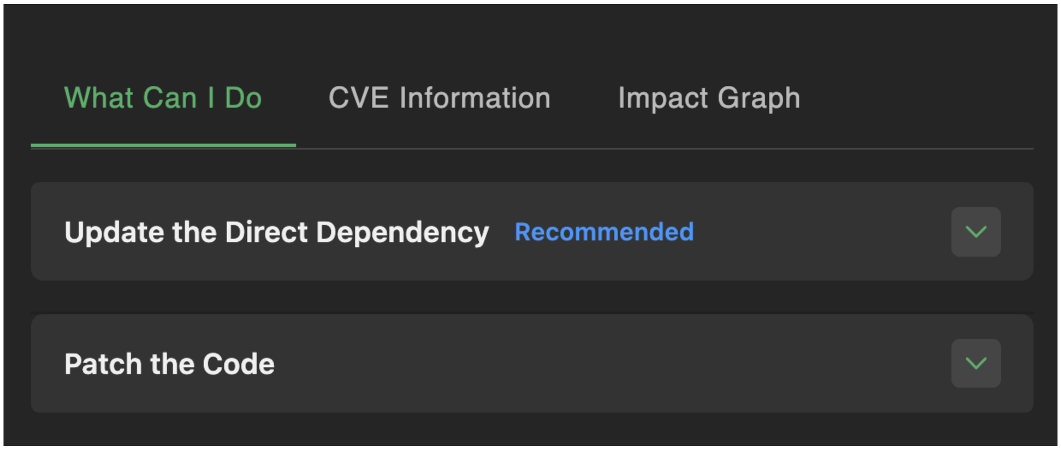


1 Secrets Issues TO FIX

Status	JFrog Severity	ID	Description	File Path
TO FIX	H	EXP-1235-00001	**Plaintext API keys found**	/usr/src/app/server

Phase #3 - Fixing CVE-2022-29078

11. Go back to your IDE with the NodeJS project opened
    a. Scan the application and locate CVE-2022-29078
    b. Try to fix it, following the remediation suggested by the JFrog plugin.



    c. Run the IDE scan once again.
        i. Is the CVE still marked as applicable?

Congratulations! You have completed Lab 4