

Lab 3 (15 min)

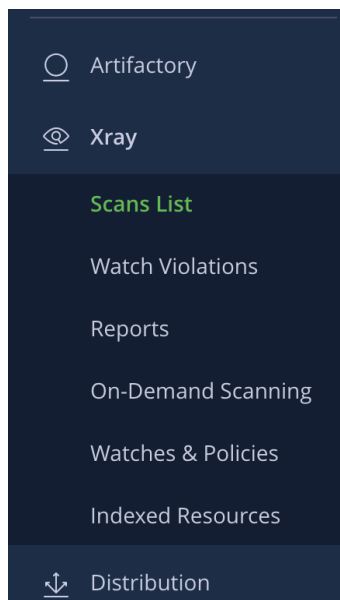
OVERVIEW: In this lab you will experience JFrog Advanced Security value with actual docker images scanning.

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

Step by step instructions

Note: The project we are working with has its own 'Dockerfile', and we have pre-built the container and pushed it to the 'puserXX-docker-local' repository in your respective Projects. 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'.



- Choose the 'puserXX-docker-local' repository, and the 'demo-jas/latest' container.

The screenshot shows the JFrog Platform interface. The top navigation bar includes 'JFrog Platform', a dropdown menu with 'puser23', and tabs for 'Application' and 'Administration'. The left sidebar contains links for 'Artifactory', 'Xray', 'Scans List' (highlighted), 'Watch Violations', 'Reports', and 'On-Demand Scanning'. The main content area displays the breadcrumb 'Xray > Scans List > puser23-docker-local > demo-jas/latest'. Below this, there's a 'Scan Name' field with 'puser23-docker-local/latest' and an 'Overview' button. A table shows repository details for 'demo-jas/latest':

Repository Path	Created by	Downloads
puser23-docker-local/demo-jas/latest/manifest.json	user43	0

- Inspect the 'Overview' page, which provides a summary of the components and issues of the Container.

The screenshot displays the 'demo-jas/latest' Overview page. It includes a header with the repository path, creation details, and last scan date. A red alert box indicates '1 Malicious packages detected' with the package 'ecopower | 1.3'. The page is divided into three main sections: Vulnerabilities, Exposures, and Policy Violations.

Vulnerabilities

by Severity

Severity	Count
Critical	43
High	93
Medium	57
Low	5
Unknown	14

Total: 212

Critical & High vulnerabilities by Applicability: 96% of CVEs are covered by contextual analysis

Applicability	Count
Applicable	77
Not Applicable	49

6 Others

Exposures

by Severity

Severity	Count
Critical	0
High	3
Medium	2
Low	0
Unknown	0

Total: 5

Policy Violations

by Severity

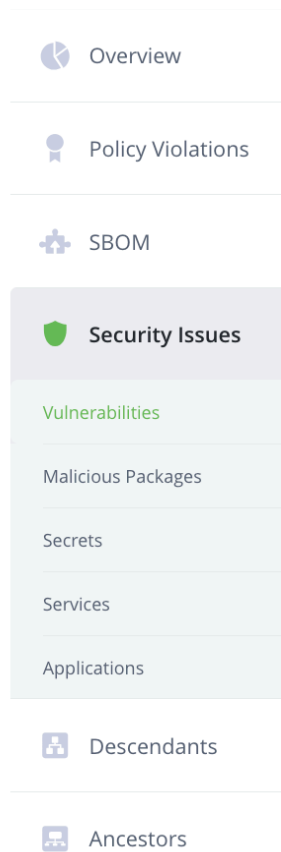
Severity	Count
Critical	27
High	38
Medium	0
Low	0
Unknown	0

Total: 65


by Type

Type	Count
Security	65
License	0
Operational	0

- From the inner left bar, click on 'Security Issues' -> 'Vulnerabilities'.



5. Look at “CVE-2020-14343”
 - a. Is it applicable to this docker image?
 - b. What is the risk?
 - c. What is the remediation process?
6. Now look at “CVE-2023-32314”
 - a. Note the CVSS score of 10!
 - b. Why is it not applicable to this docker image?
7. How many Critical, yet NOT APPLICABLE vulnerabilities were detected by the system?

Hint: use the Filter  icon to refine the data.
8. How many NOT APPLICABLE Violations were detected by the system?

Hint: click  to review the data.

9. You shouldn't see any due to a setting in the XRay policy to 'Skip Not Applicable' CVEs from raising a violation.

Rule Name

critical

If The following condition is met


Rule type

CVEs

Rule category

☒ Minimal Severity ☐ CVSS Score ☐ CVE IDs

Select minimal severity

 Critical

Recommended severity - High

☐ Except if a Fix Version is not available ⓘ

☒ Skip not applicable CVEs ⓘ

10. Let's look at other data. Does your selected image have any application exposures?

Xray > Scans List > puser23-docker-local > demo-jas/latest

Scan Name
puser23-docker-local/latest

Overview

Policy Violations 144

SBOM 243

Security Issues 272

- Vulnerabilities 207
- Malicious Packages 1
- Secrets 5
- Services 47
- Applications 12**

Descendants

12 Applications Issues Last Scan Status ⓘ

Status	JFrog Research	ID	Description
To Fix	High	EXP-1058-00001	Node
To Fix	High	EXP-1058-00002	Node
To Fix	High	EXP-1064-00001	Python
To Fix	High	EXP-1069-00001	Node
To Fix	Medium	EXP-1056-00001	Passv
To Fix	Medium	EXP-1059-00001	Node
To Fix	Medium	EXP-1059-00002	Node
To Fix	Medium	EXP-1059-00003	Node

11. Does your selected image have any secrets detected?

Xray > Scans List > puser23-docker-local > demo-jas/latest

Scan Name
puser23-docker-local/latest

Overview

Policy Violations 144

SBOM 243

Security Issues 272

- Vulnerabilities 207
- Malicious Packages 1
- Secrets 5**
- Services 47

5 Secrets Issues Last Scan Status ⓘ

Status	JFrog Research	ID	Description
To Fix	High	EXP-1681-00001	Hardc
To Fix	High	EXP-1685-00001	Hardc
To Fix	High	EXP-1685-00002	Hardc
To Fix	Medium	EXP-1225-00001	Expire
To Fix	Medium	EXP-1474-00001	Self-si

Congratulations! You have completed Lab 3