

Lab 3 (15 min)

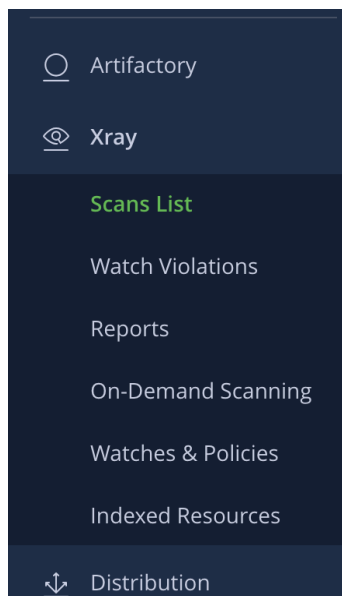
OVERVIEW: In this lab you will experience JFrog Advanced Security value with actual docker images scanning.

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

JFrog Platform | puser23 | Application Administration

Artifactory Xray Scans List Watch Violations Reports On-Demand Scanning

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

Scan Name: puser23-docker-local/latest

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.

demo-jas/latest

Repository Path: puser23-docker-local/demo-jas/latest/manifest.json | Created by: user43 | Downloads: 0 | Last Scan: 05 Sep 2024 11:19 (GMT-0500)

1 Malicious packages detected
ecopower | 1.3

Vulnerabilities (View All)

by Severity

Critical	43
High	94
Medium	55
Low	5
Unknown	10

207

Critical & High vulnerabilities by Applicability
93% of CVEs are covered by contextual analysis

Applicable	79
Not Applicable	45

10 Others

Exposures (View All)

Secrets Services Applications

Critical	0
High	3
Medium	2
Low	0
Unknown	0

5

Policy Violations (View All)

by Severity

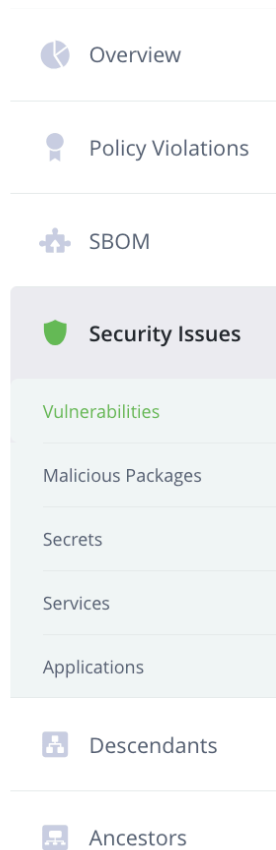
Critical	27
High	117
Medium	0
Low	0
Unknown	0

144

by Type

Security	27
License	1
Operational	116


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



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

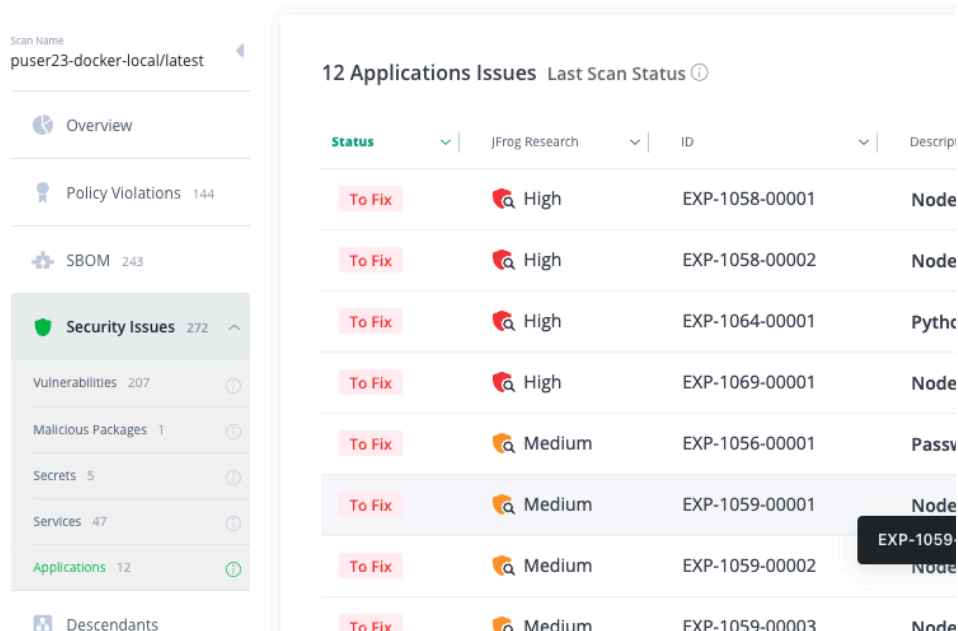
Hint: use the Filter  icon to refine the data.

8. How many NOT APPLICABLE Violations were detected by the system?

Hint: click  Policy Violations 144 to review the data.

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

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

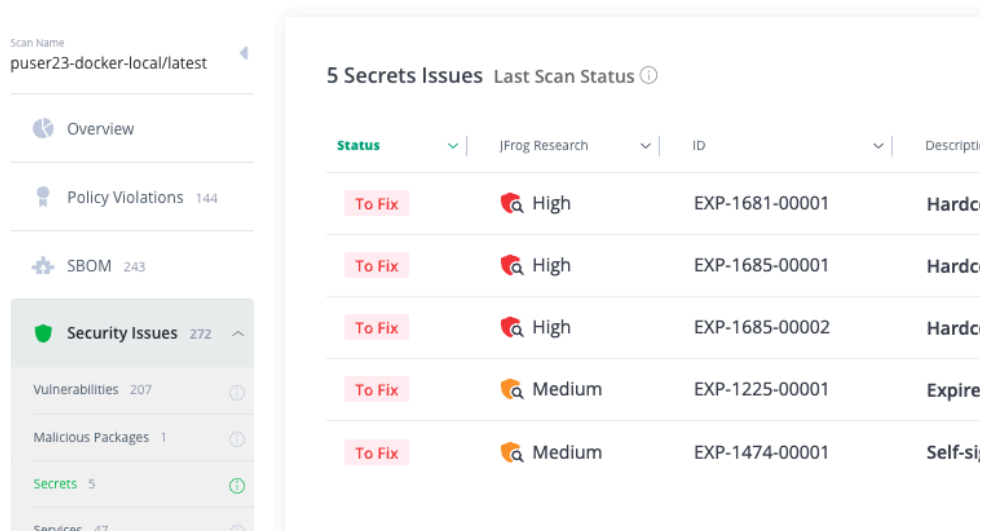


The screenshot shows the Xray interface for the scan 'puser23-docker-local/latest'. The left sidebar lists various security categories: Overview, Policy Violations (144), SBOM (243), Security Issues (272), Vulnerabilities (207), Malicious Packages (1), Secrets (5), Services (47), Applications (12), and Descendants. The 'Applications' category is selected, showing 12 issues. The main panel displays a table of these issues, all marked 'To Fix'. The issues are categorized by severity: High (4 issues) and Medium (8 issues). The table columns are Status, JFrog Research, ID, and Description. A tooltip for issue EXP-1059-00001 is visible, showing the description 'Node'.

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

10. Does your selected image have any secrets detected?

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



The screenshot shows the Xray interface for the scan 'puser23-docker-local/latest'. The left sidebar is the same as in the previous screenshot. The 'Secrets' category is selected, showing 5 issues. The main panel displays a table of these issues, all marked 'To Fix'. The issues are categorized by severity: High (3 issues) and Medium (2 issues). The table columns are Status, JFrog Research, ID, and Description. A tooltip for issue EXP-1225-00001 is visible, showing the description 'Expire'.

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