

Lab 2 (15 min)

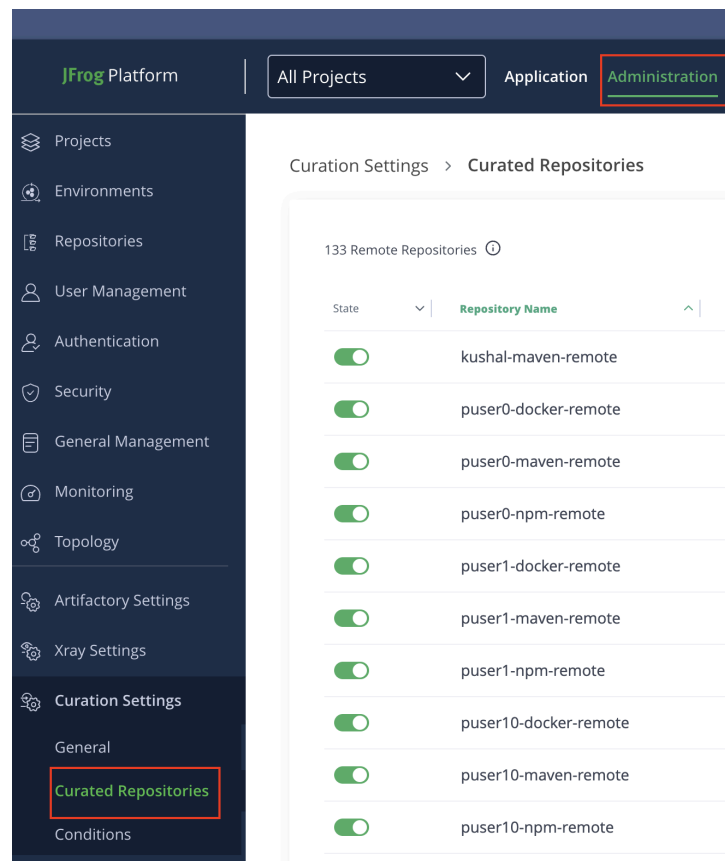
OVERVIEW: In this lab you will use JFrog Curation, configure policies with it and test it with a maven install command.

EXPECTED OUTCOME: Upon successful completion of this lab you will gain knowledge of how to curate open-source dependencies with the JFrog Platform.

Step by step instructions

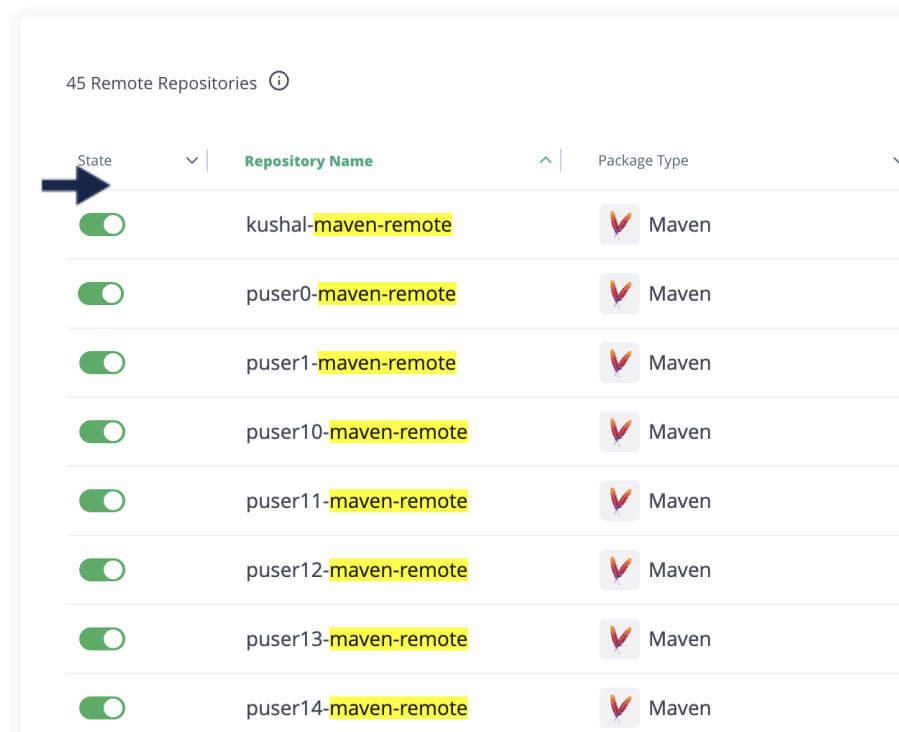
Phase #1 - Selecting a Repository to curate









1. Click on 'Administration' at the top pane and then Curation Settings -> Curated Repositories on the left pane.



2. Make sure Curation is Turned On for your respective 'puserX-maven-remote' repository. This will enable you to enforce curation policies on this repository.

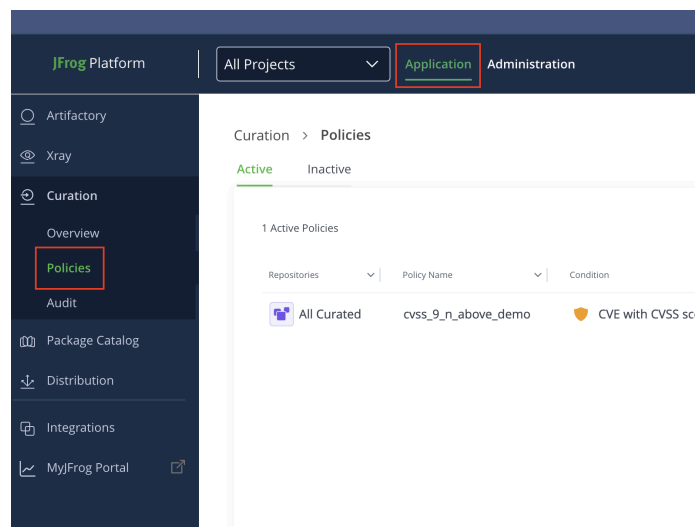
Curation Settings > Curated Repositories



State	Repository Name	Package Type
	kushal-maven-remote	Maven
	puser0-maven-remote	Maven
	puser1-maven-remote	Maven
	puser10-maven-remote	Maven
	puser11-maven-remote	Maven
	puser12-maven-remote	Maven
	puser13-maven-remote	Maven
	puser14-maven-remote	Maven

Phase #2 - Creating a Curation policy

3. Click on 'Application' at the top pane and then on 'Curation' -> 'Policies' from the left pane.



4. Click on 'Create Policy'

5. Choose a name for the policy and click 'Next'

Curation > Policies > New Curation Policy

1

Policy Name

What is the name of the policy?

Name

Next >

2

Repositories

3

Policy Condition

6. Choose your specific 'puserX-maven-remote' repository. This means the policy will be enforced only on this repository. Click 'Next'.

Curation > Policies > New Curation Policy

✓

Policy Name

demo

2

Repositories

Specify the remote repositories for the policy.

☐ All Curated ⓘ

☒ Specific ⓘ

+

Select Remote Repository

Select a repository in order to continue









Next >

3

Policy Condition

Select A Remote Repository

45 Remote repositories

Repository Name	Package Type
<input type="checkbox"/> kushal-maven-remote	 Maven
<input type="checkbox"/> puser0-maven-remote	 Maven
<input type="checkbox"/> puser1-maven-remote	 Maven
<input type="checkbox"/> puser10-maven-remote	 Maven
<input type="checkbox"/> puser11-maven-remote	 Maven
<input type="checkbox"/> puser12-maven-remote	 Maven
<input type="checkbox"/> puser13-maven-remote	 Maven
<input type="checkbox"/> ...	 Maven

- Now it's time to choose a condition for the policy. Take a look at the different options, some are security related, some are license related and some are operational. Curation enables you to pick the right OSS dependency based on different types of criterias. For this lab, let's choose 'Malicious Package' as the condition. Click 'Next'.

3

Policy Condition

Select the policy condition that will indicate a violation

Malicious package

CVE with CVSS score of 9 or above (fix version available)

CVE with CVSS score of 9 or above (with or without a fi...

CVE with CVSS score between 7.0 and 8.9 (fix version a...

CVE with CVSS score between 7.0 and 8.9 (with or with...

CVE with CVSS score between 7.0 and 8.9 (with or with...

Malicious package

Security

Supported

All

Description

Detects 3rd party packages that have been identified by the [JFrog Security Research team](#) as malicious.

The JFrog Security Research group created scanners that continuously scan 3rd party packages for indications of malicious intent.

Our detectors look for indications of infection methods (e.g. typosquatting, dependency confusion) suspicious payload actions (e.g.

Next

8. Here we can add a waiver that will exclude specific packages from the policy being created. A waiver can be added also after policy creation. Let's skip and click on 'Next'.
9. Currently, Curation has two different actions: 'Block', which will block the download request and return a proper error message, or 'Dry Run', which will only simulate the curation flow. Let's choose 'Block' and click on 'Save Policy' on the bottom right.

5

Actions & Notifications

Select the required action if a violation occurs

Block

Dry Run

Notify by Email

Add Email

Next

Policy Condition

Malicious package

Security

Supported

All

Description

Detects 3rd party packages that have been identified by the [JFrog Security Research team](#) as malicious.

The JFrog Security Research group created scanners that continuously scan 3rd party packages for indications of malicious intent.

Our detectors look for indications of infection methods (e.g. typosquatting, dependency confusion) suspicious payload actions (e.g. download and execute, dynamic code evaluation), obfuscation techniques and more.

Policy Effectiveness

Covered Repositories List

Save Policy

Congratulations, you've created your first curation policy!

Phase #3 - Testing your Curation policy

10. Open a new browser Tab and paste this URL for your respective 'puserX-maven-remote' repository.

<https://swampup17242481111.jfrog.io/artifactory/puserX-maven-remote/log4j/log4j/1.2.17/log4j-1.2.17.jar>

11. You should see a 403 Forbidden with a message explaining the Blocked download.

```

{
  "errors": [
    {
      "status": 403,
      "message": "package log4j:log4j:1.2.17 download was blocked by jfrog packages curation service due to the following policies violated {cvss_9_n_above_demo,
    }
  ]
}

```

Phase #4 - Inspecting the Curation event

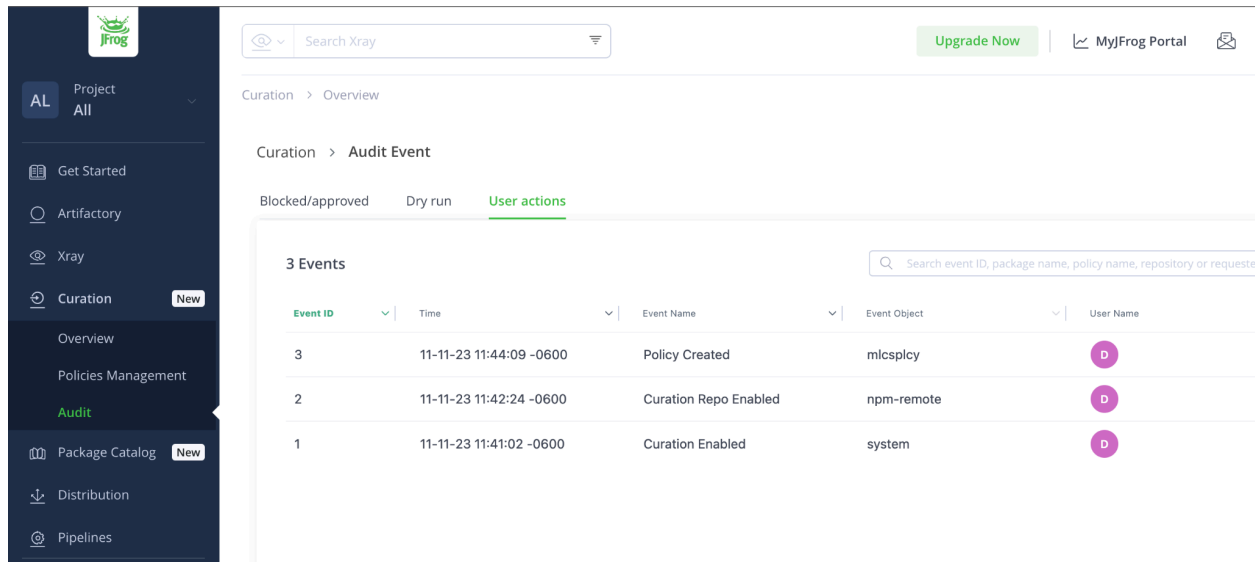
- Go back to the JPD UI, and click on 'Curation' -> 'Audit'. Here you should be able to see the last event, which is a rejection of your maven download request.

The screenshot displays the JFrog Platform UI. On the left, a sidebar contains navigation links: Artifactory, Xray, Curation (selected), Overview, Policies, Audit (highlighted with a red box), Package Catalog, Distribution, Integrations, and MyJFrog Portal. The main content area is titled 'Curation > Audit Event' and shows a table with 1 event. The event details on the right include:

- Event ID | 9**: 09-09-24 09:27:14 -0500
- Action**: blocked
- Reason**: Policy violations
- Package Name**: log4j:log4j
- Package Type**: Maven
- Package Version**: 1.2.17
- Package URL**: https://repo1.maven.org/maven2/log4j/log4j/1.2.17/log4j-1.2.17.jar
- Origin Server**: b0gokuy6jjcem
- Origin Repository**: puser0-maven-remote
- Requester**: pstrainenv
- Violated Policies (1)**:

Condition	Severity
CVE with CVSS score of 9 or above (with or without a fix version available)	9.8
Package version contains the following vulnerability(s):	9.8
CVE-2019-17571	9.8
CVE-2022-23305	9.8

- In addition, if you click on 'User Actions', you should be able to see the audit trail of the policy you created in Phase #2.
Inspect the information provided on this action.



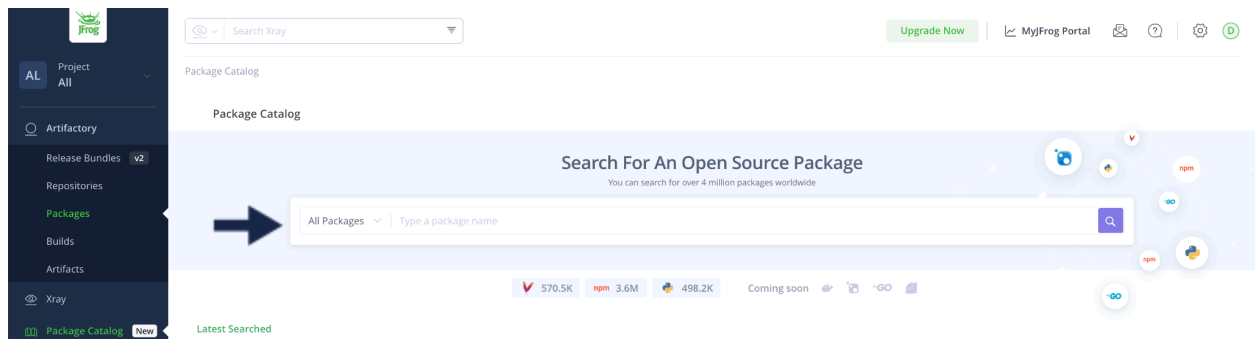
The screenshot shows the JFrog Xray interface. The left sidebar contains navigation links: Project All, Get Started, Artifactory, Xray, Curation (highlighted), Overview, Policies Management, Audit (highlighted), Package Catalog (New), Distribution, and Pipelines. The main content area is titled 'Curation > Audit Event'. Below this, there are tabs: 'Blocked/approved', 'Dry run', and 'User actions' (selected). A table titled '3 Events' displays the following data:

Event ID	Time	Event Name	Event Object	User Name
3	11-11-23 11:44:09 -0600	Policy Created	mlcsplcy	D
2	11-11-23 11:42:24 -0600	Curation Repo Enabled	npm-remote	D
1	11-11-23 11:41:02 -0600	Curation Enabled	system	D

Congratulations! You have completed Lab 2

Phase #5 - BONUS - Inspecting the package in JFrog Catalog

14. Go back to the UI, and click on 'Package Catalog'. Search for the 'cors.js' package.



The screenshot shows the JFrog Package Catalog interface. The left sidebar has navigation links: Project All, Artifactory, Release Bundles (v2), Repositories, Packages (highlighted), Builds, Artifacts, Xray, and Package Catalog (New). The main content area is titled 'Package Catalog'. A search bar is prominently displayed with the text 'Search For An Open Source Package' and 'You can search for over 4 million packages worldwide'. Below the search bar, there is a dropdown menu set to 'All Packages' and a text input field labeled 'Type a package name'. A blue arrow points to the search bar. At the bottom of the search bar, there are statistics: 570.5K, npm 3.6M, 498.2K, and 'Coming soon'.

15. What kind of information does the catalog provide on cors.js? What is the core issue and what is the remediation?