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.

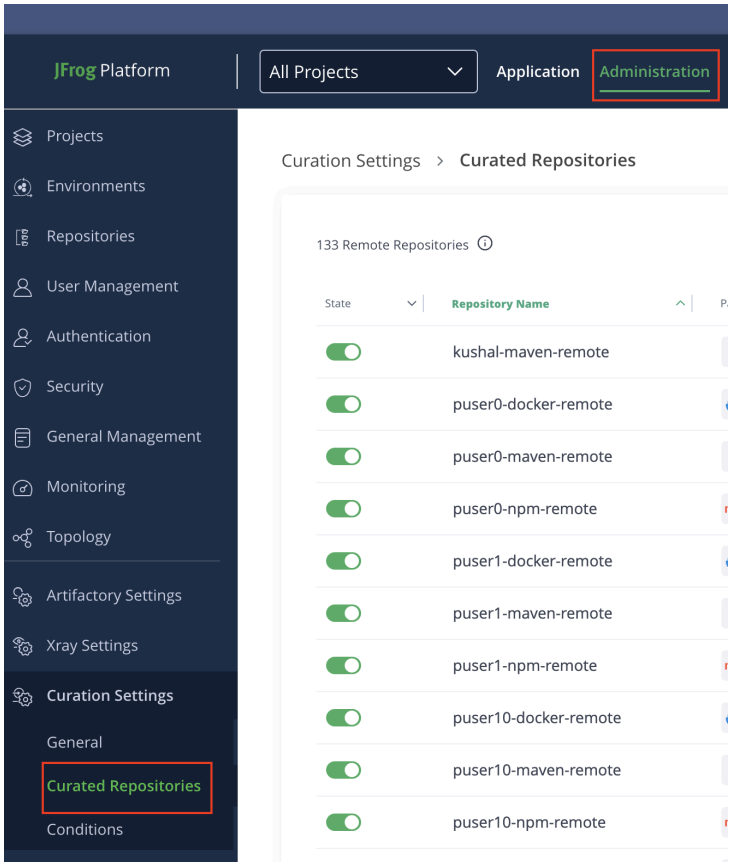
Step by step instructions

Note :

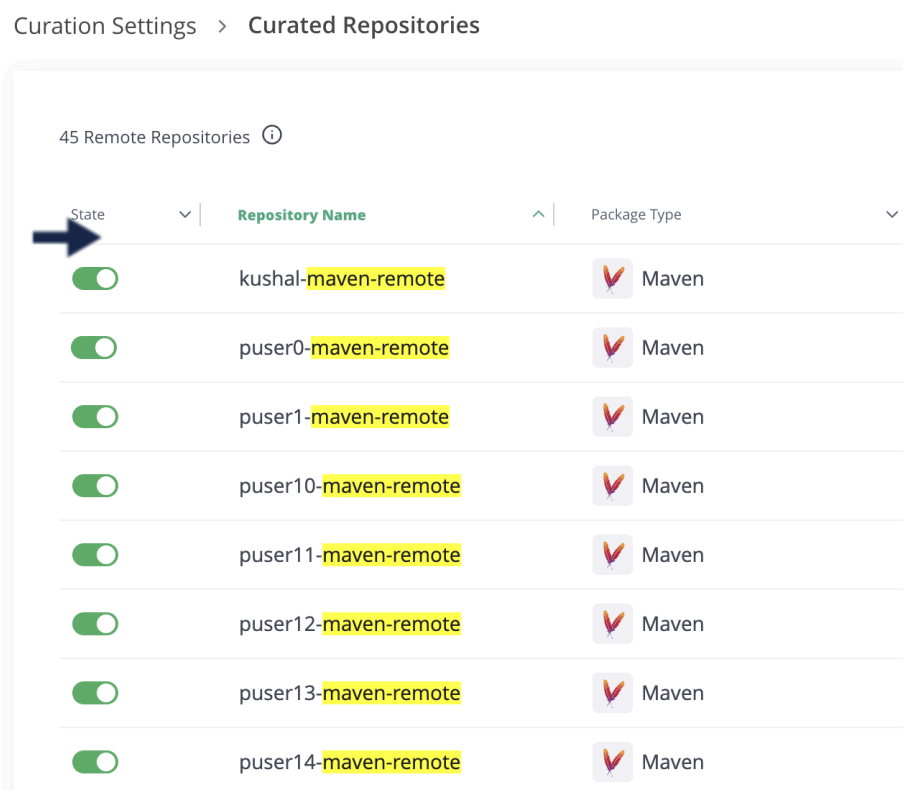
As phase #1 requires admin rights, this has already been done in the training lab environment.
This will be demonstrated by your lab instructor.
As part of the training, we recommend you read the instructions below, as it will teach you the exact process and steps required to control your 3rd parties dependencies as a JFrog platform's administrator.

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.

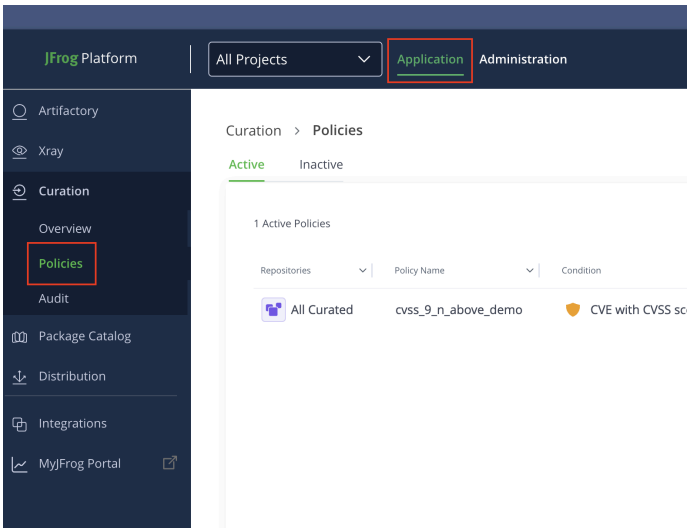


2. Make sure Curation is Turned On for your respective ‘puserX-maven-remote’ repository. This will enable you to enforce curation policies on this repository.



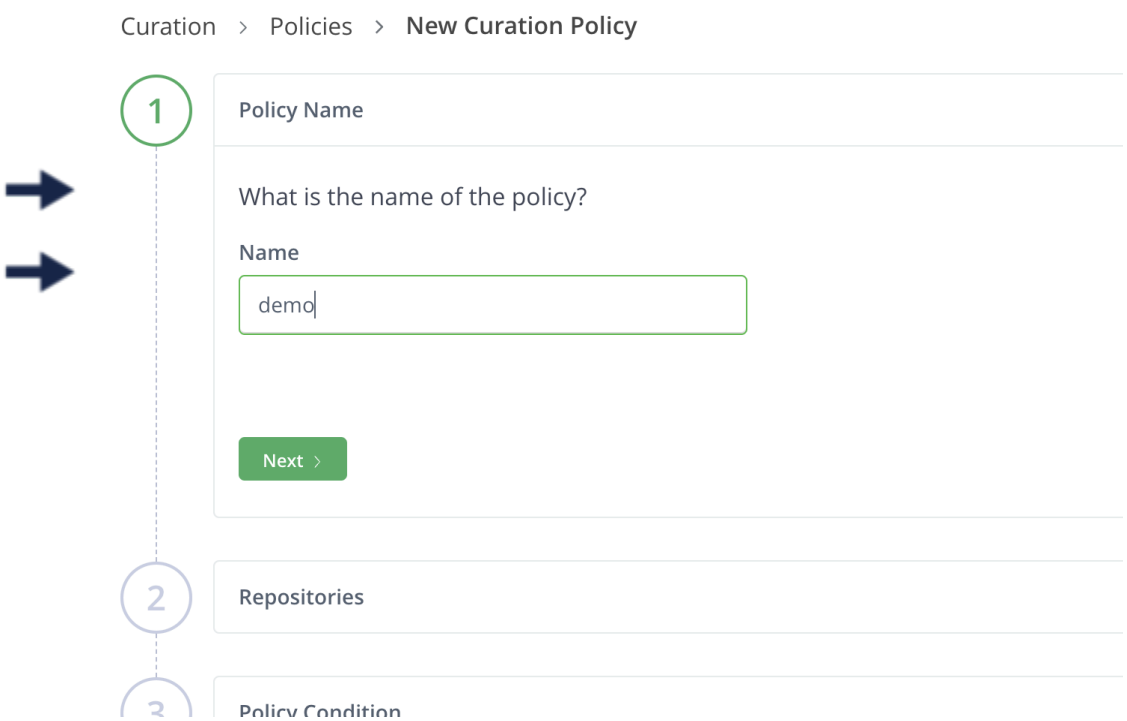
Phase #2 - Creating a Curation policy

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

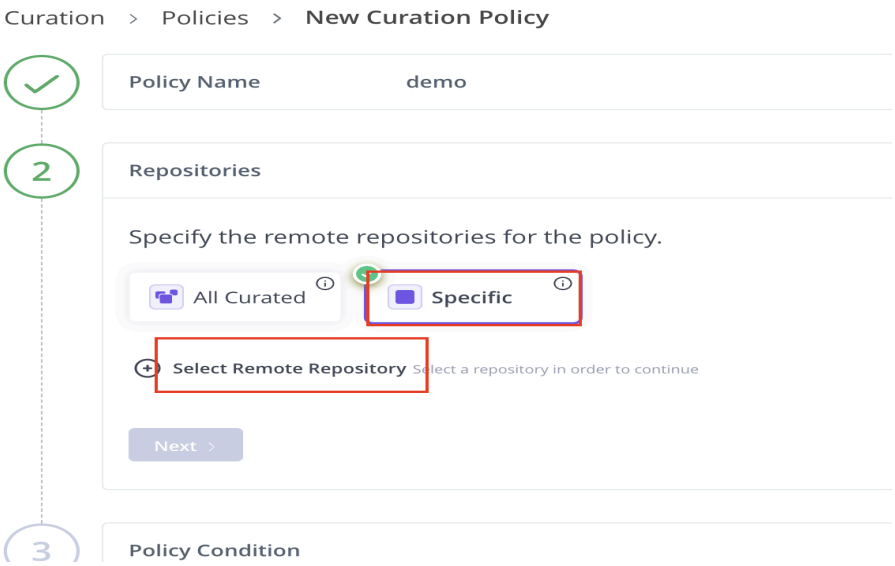


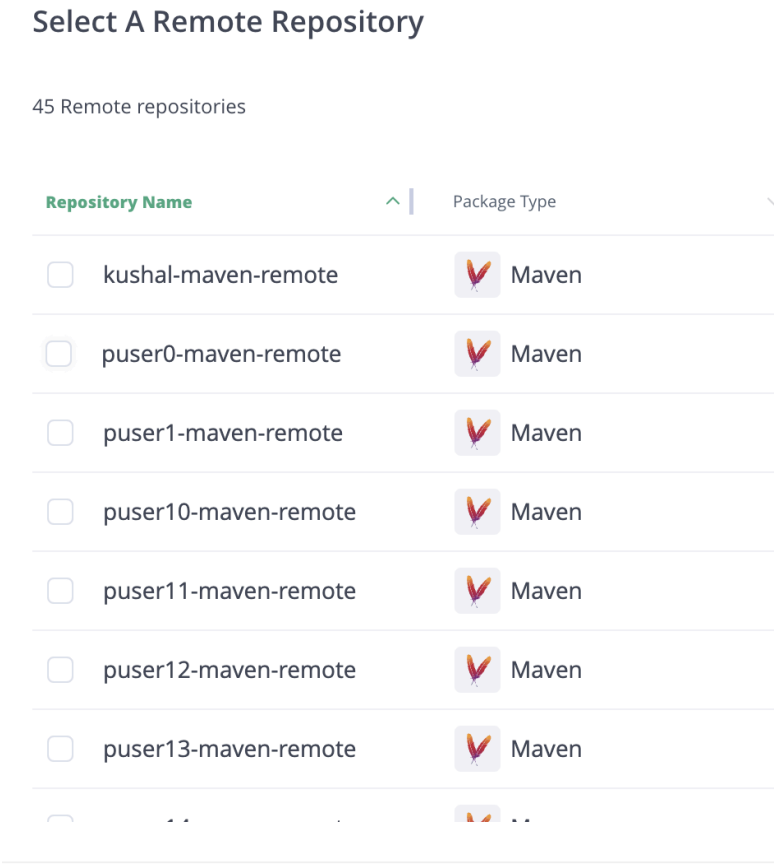
4. Click on 'Create Policy'

5. Choose a name for the policy and click ‘Next’

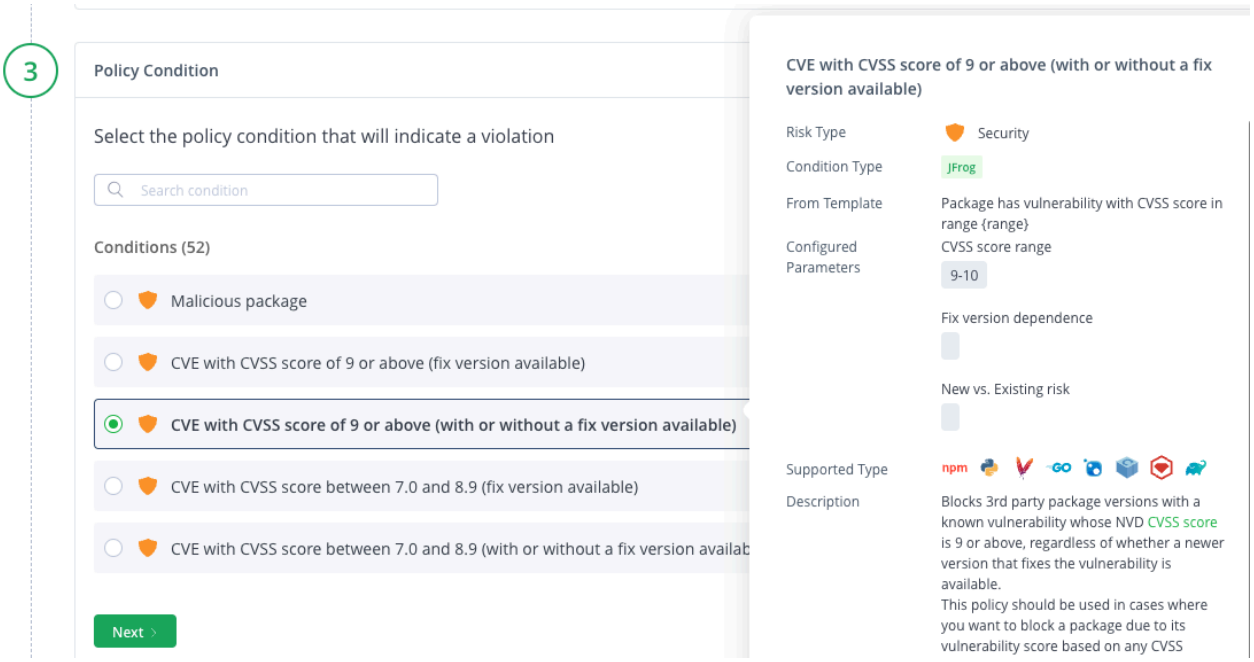


6. Choose your specific ‘puserX-maven-remote” repository. This means the policy will be enforced only on this repository. Click ‘Next’.

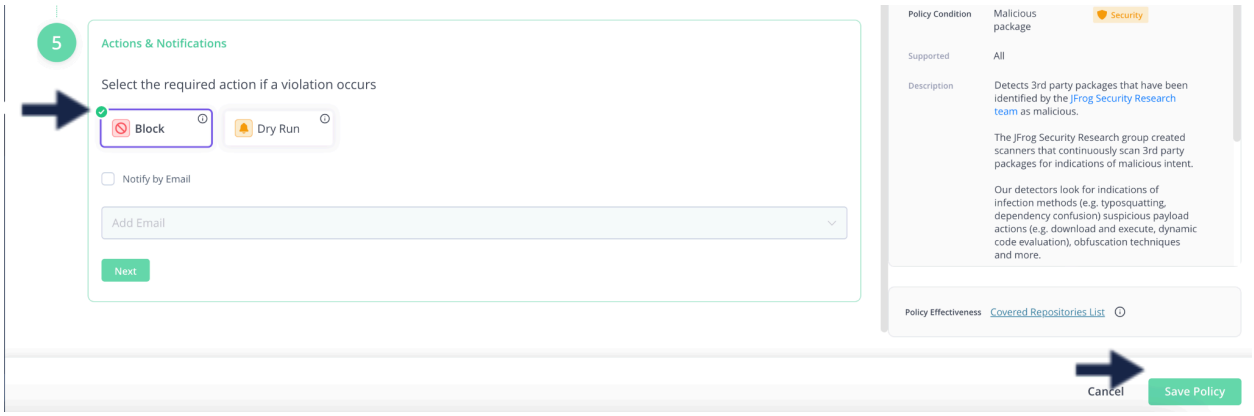




7. Now it's time to choose a condition for the policy. Take a look at the different options, some are security related, some are license related and some are operational.
   Curation enables you to pick the right OSS dependency based on different types of criterias. For this lab, let's choose 'CVE with CVSS score 9 or above (with or without a fix version available)' as the condition. Click '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.



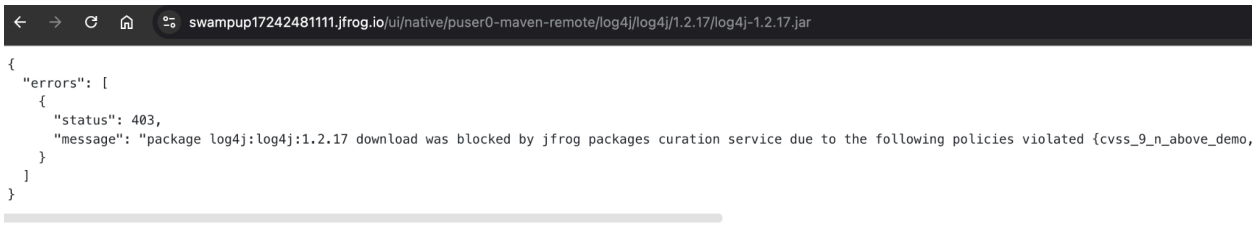
Congratulations, you've created your first curation policy!

Phase #3 - Testing your Curation policy

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

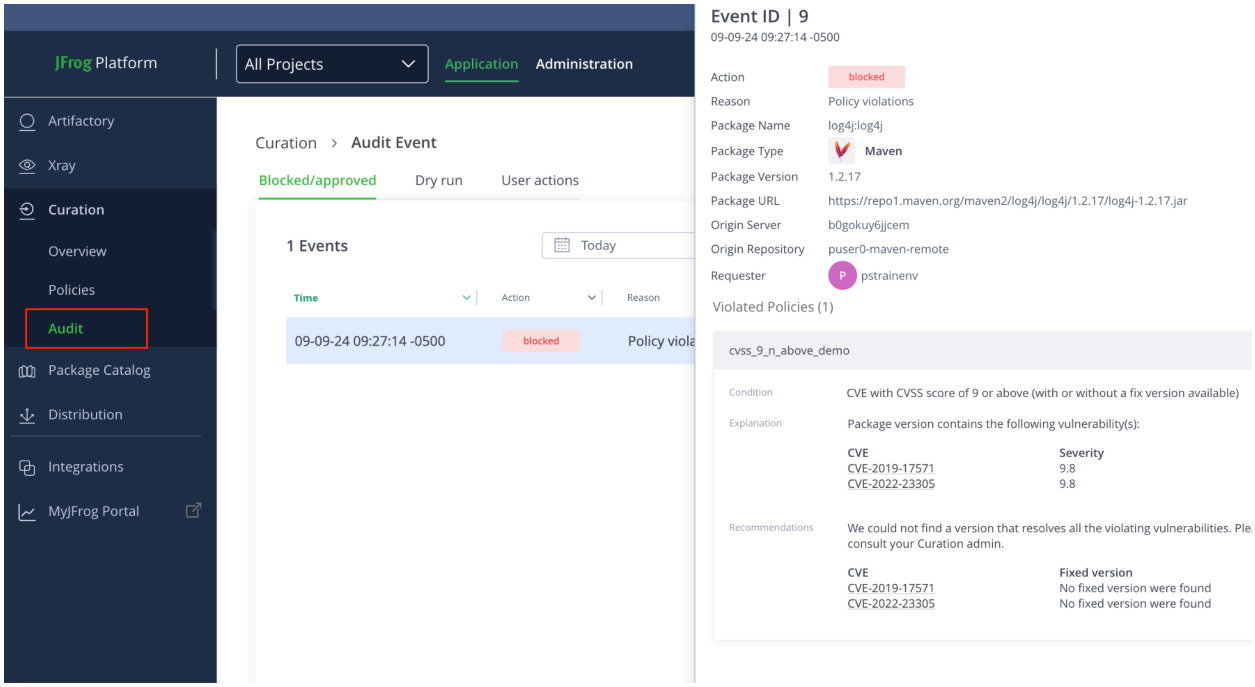
https://dsodsec.jfrog.io/artifactory/puserX-maven-remote/log4j/log4j/1.2.17/log4j-1.2.17.jar

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



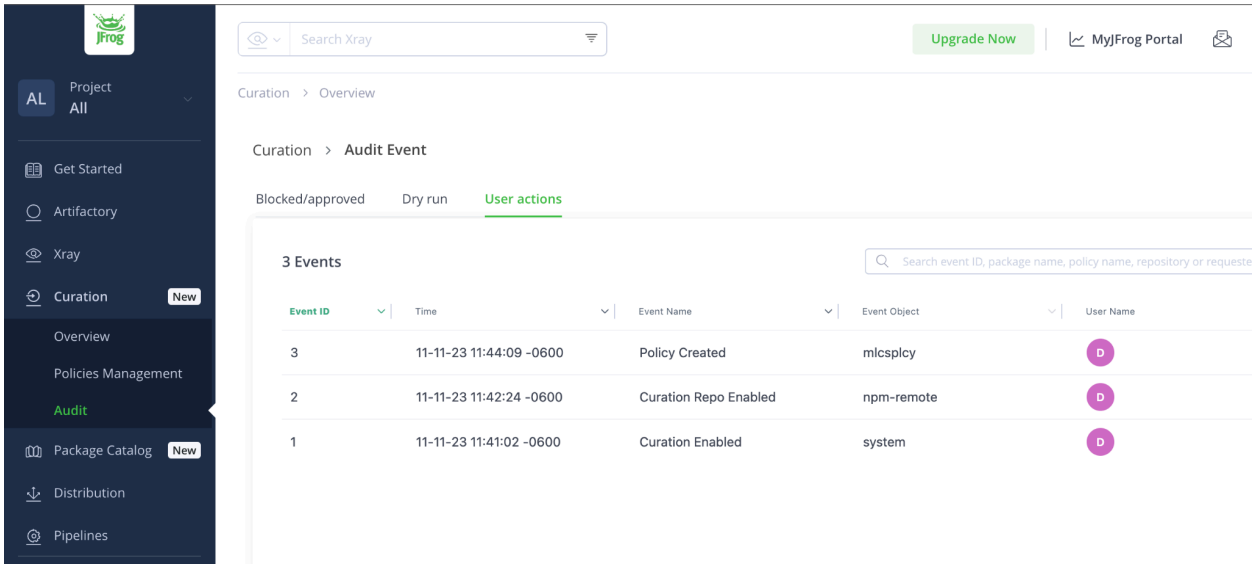
Phase #4 - Inspecting the Curation event

12. 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.



13. 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.

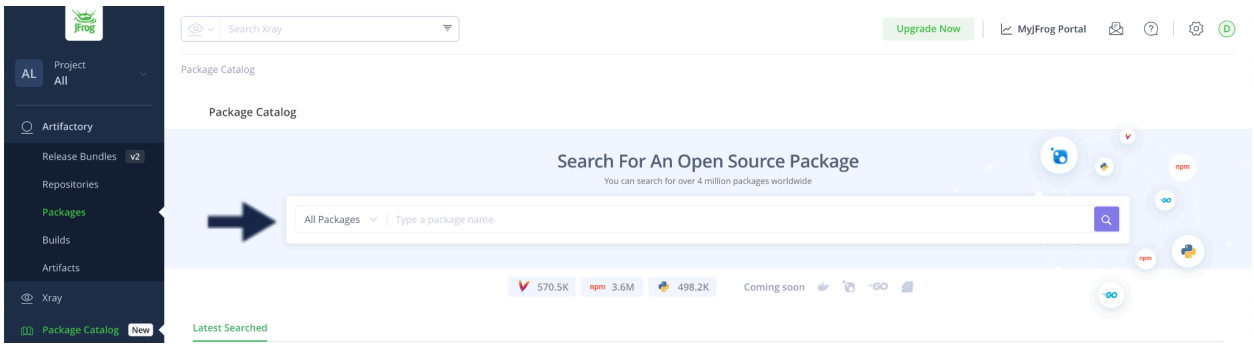
    Inspect the information provided on this action.



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.



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