XRAY CHALLENGE STEPS

1. GET YOUR PLATFORM ENVIRONMENT

a. If you don't have a JFrog Platform environment - then **sign up for a Free Tier JFrog Cloud Subscription**, which includes JFrog Artifactory, JFrog Xray and JFrog Pipelines. Or alternatively **start a Self-Hosted Free 30 Day Trial** of JFrog Artifactory and JFrog Xray.
b. Login to your JFrog Platform instance. After you login you will see an overview screen in the UI that looks like a map.

2. CREATE A REPOSITORY

a. To start scanning for vulnerabilities with JFrog Xray you will need either a repository with some content (like packages and components) or a build or a release bundle. If you already have repositories with content you can immediately start using Xray.
b. If you don't know how to create a repository or how to use one - watch this video and it will show you how to set up a Maven Repository.

3. CREATE A POLICY, RULE AND A WATCH

a. To start scanning repositories for vulnerabilities you need to first define **Policies**, **Rules** and **Watches**.
b. A **Policy** is a composite of **Rule(s)**. A **Rule** is a stateless description of what should happen if you detect a vulnerability. A **Watch** is the connection between your policies and the actual resources or repositories you're scanning.
c. Select the Administration tab at the top of the left sidebar, and go down and click on **"Xray"** and select **"Watches & Policies"**.
d. To create a new policy click on **"New Policy"**, give it a name and optionally a description, then you need to choose **'Security'** as the policy type.
e. Now you have to add an action or a rule for the policy by clicking **"New Rule"** and then giving it a name. Then you need to decide what the minimum CVSS score is and the range you want to cover. The easy way is to choose from the preset severity groups in the drop down menu: All, Low, Medium, High or Critical.
f. Then you need to decide what action you need to happen if a security vulnerability match is found. Scroll down and select from the listed actions: notifications, trigger a webhook, block a download or release bundle and fail a build. Then click **'Save'**.
g. Now we have a policy associated with a rule, you can now **'Save'** the policy and we can start associating it with **'Watches'**
h. Select the **'Watches'** menu item at the top of the UI and go to **"New Watch"** and then give it a name and optionally a description.
i. You have to select which repositories (previously created) you want to scan by clicking the **"Add Repositories"** button and choose the repository from the list in the UI and click **'Save'**
j. Now the watch has a name, a repository(s) to scan and finally needs to be connected with a policy(s). To do this click **"Manage Policies"** and select the policies you want to connect to this watch and then click **"Create Watch"**
k. A watch will be activated to scan the repository by any of the following methods: triggered manually, the vulnerability database gets an update or the contents of the repository change.

4. VIEW THE RESULTS FROM YOUR WATCH

a. To use and view the result of the watch you need to click the Application tab at the top of the sidebar and scroll down and click **“Security & Compliance”** and select **“Watch Violations”** and then you can pick which watch you want to check and you will get an overview of all it’s violations
b. Choose the time period you desire to view the violations over in the **“Created”** drop down box and select a preset or define a custom range and press **“Search”**
c. You will then see the screen fill up with all of the vulnerabilities found by the watch according to the associated policy and rule. You can filter the view of vulnerabilities with the filter options at the top including - ‘Contains Text’, ‘Min. Severity’, ‘CVE ID’, and ‘Type’

5. TAKE THE SCREENSHOT

a. Click on one of the vulnerabilities in that window and you will get a new popup window which gives you an overview of the details of that vulnerability including type, provider, summary, severity etc. and a graphical view of the vulnerable component and where it is located.

Hint: The popup screen looks like a bullseye.