From DevOps to DevSecOps:
A JFrog Security Workshop

Hands-on for 30 minutes

Introduction

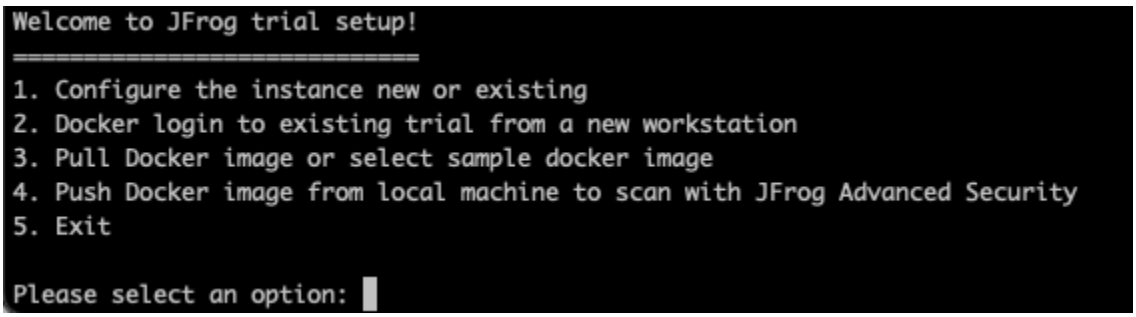
The JFrog Advanced Security trial provides a fully-functional version of the JFrog Platform (including Artifactory and Distribution).
The trial is pre-populated with artifacts (container and Terraform file) so you can immediately go through the security scan results and see the value of the output, as well as the flow and the experience.

If you want to scan your own artifacts, we recommend creation of new local/remote repositories in Artifactory, and pull/push artifacts (such as Docker containers) for security scanning and observation or examination of the results.

The provided script utility simplifies the onboarding process and will help you set up your instance.

The utility will help you do the following:

- Setup/Configure a new or existing JFrog Platform trial instance
- Configure 'local' and 'remote' Docker repositories with advanced security scanning
- Assist you with loading Docker images from your local workstation or from Dockerhub (including recommended samples)



How to use JFrog Advanced Security

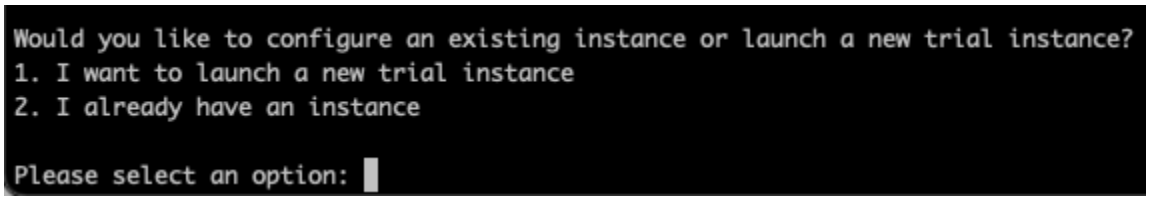
Script will be found under 'guided_trial.zip'

Windows	Linux or Mac
1. Extract the batch (.bat) script 2. Open *cmd.exe* 3. *cd script directory* 4. *windows_guided_trial.bat*	1. Extract the bash (.sh) script 2. Open terminal 3. *cd script directory* 4. *chmod +x linux_guided_trial.sh* 5. *./linux_guided_trial.sh*

Step #1 - Set up and configure a trial instance

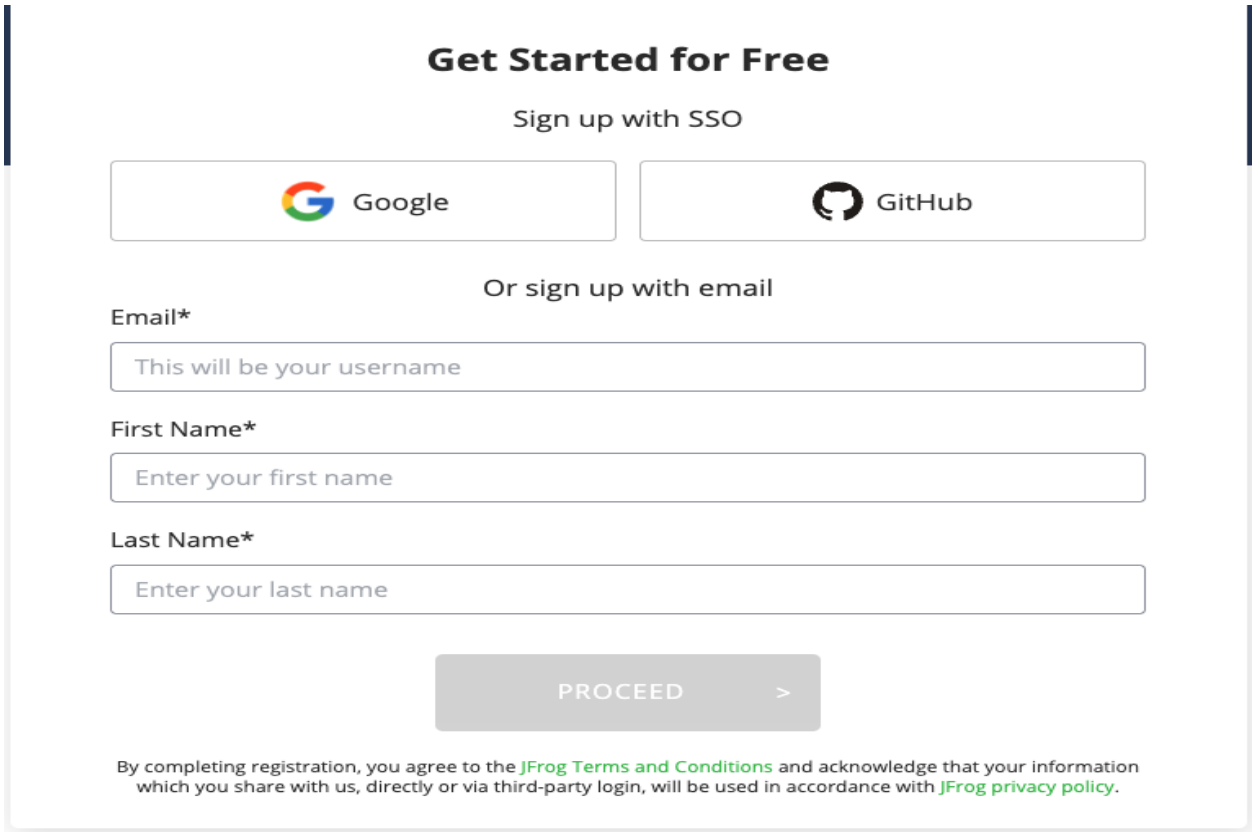
Select the option "1".

Then select "1. I want to launch a new trial instance"

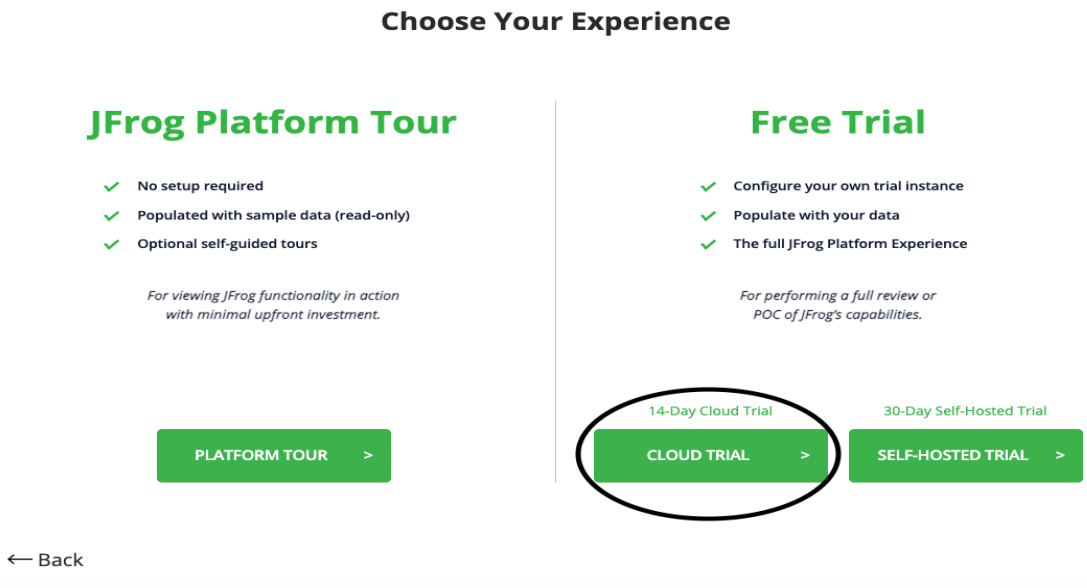


Note: If you **already signed up for a JFrog trial instance**, then select "2. I already have an instance", and continue to Step 1.1. The script will open the browser to launch the instance.

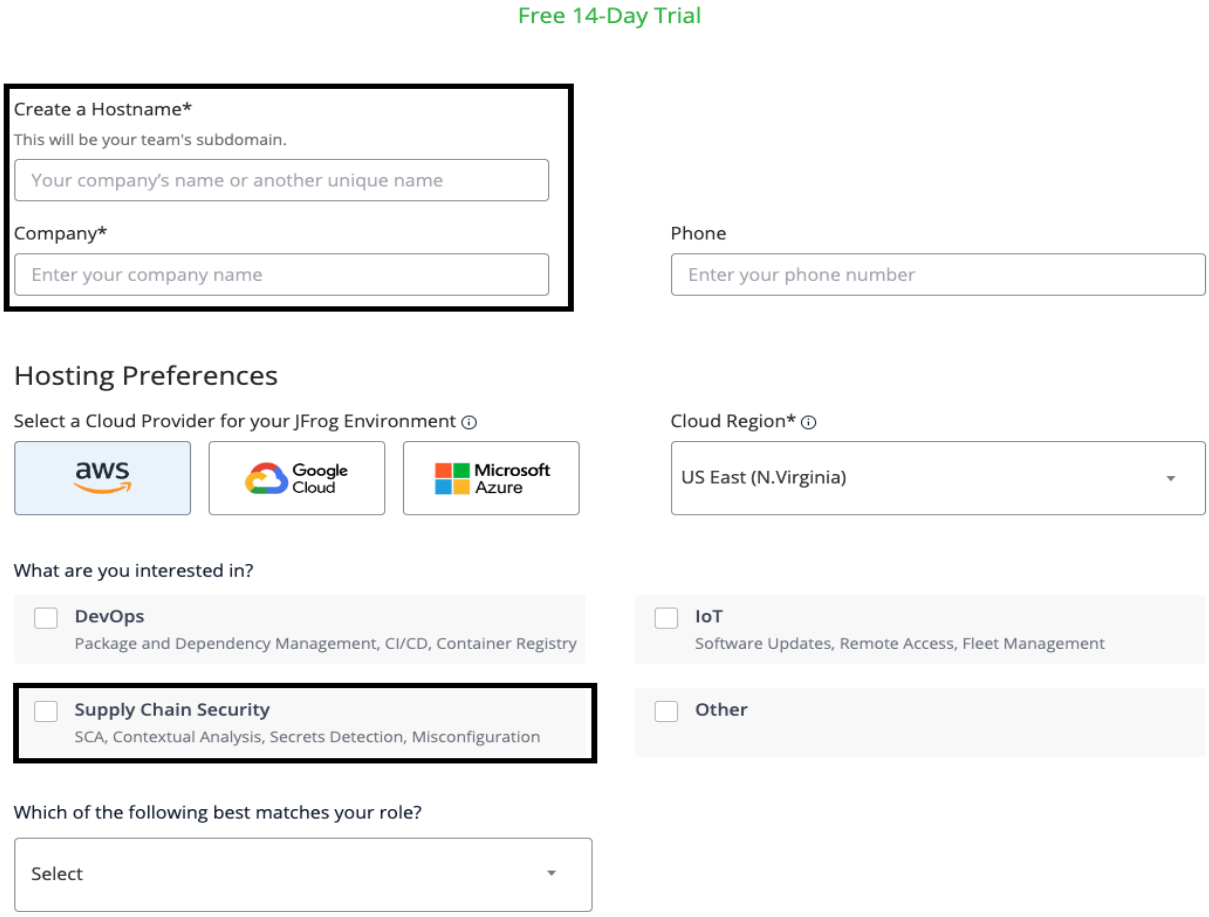
Otherwise, continue with the registration process - the script will open the browser for registration:



Provide the information requested and click “Proceed”



Select “Cloud trial”



You will be to provide a hostname, company, hosting preferences and the interest of this workshop as well as your role.

Step #1.1 - Connecting the instance locall

Once the instance is up, paste the instance name and credentials into the terminal.

Follow the script, which will open the browser and guide you through the process.

Once the script receives your credentials, it will:

- Create a new remote repository, ‘docker-hub-remote-repo’ for DockerHub, with advanced security scanning.
- Create a new remote repository ‘local-docker-repo’ for DockerHub, with advanced security scanning.
- Configure an Xray policy. The policy rules are:
    - Create violation for CVEs with Critical CVSS Score
    - Create violation for Exposures with High impact severity
    - Create violation and block download of malicious packages
- Configure an Xray Watch on all repositories.
- Execute “docker login” so you can work with the trial instance.

Step #2 - Docker login to existing trial from a new workstation

Run this step only on a new workstation.

The script will request the instance name and credentials (as asked in step #1) to configure the Docker client to work with an already-existing trial instance.

Step #3 - upload Docker to your repository

Option A - pull your proprietary Docker image or select the sample docker image

The script will assist you with pulling images from DockerHub to 'docker-hub-remote-repo' repository.

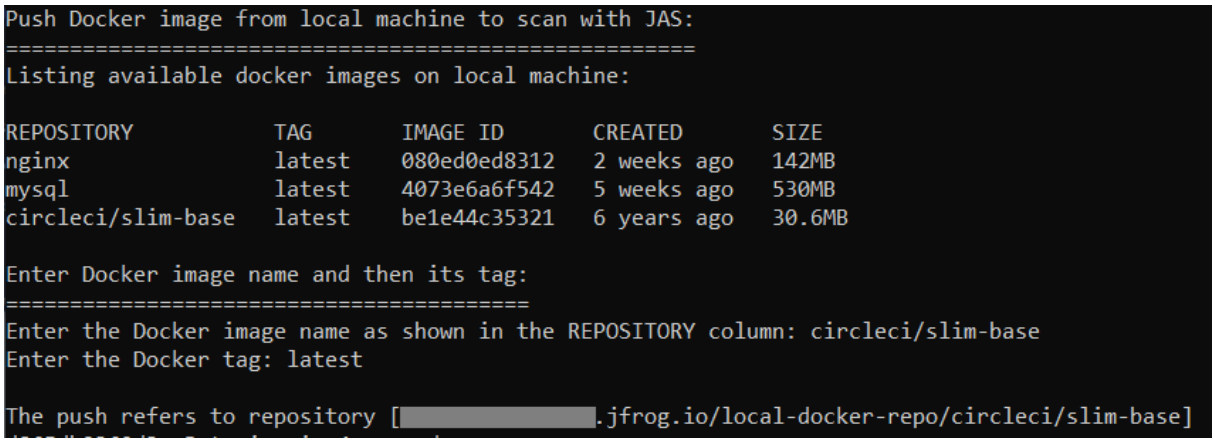
Options #1 and #2 offer a sample of known images with vulnerabilities.

```
Pull Docker image or select sample docker image:
================================================
1. Pull OWASP WebGoat - Good example of Contextual Analysis value
2. Pull netdata:1.13.0 - Good example of a Docker with 100M+ downloads with an embedded secret
3. Pull juice-shop:latest - Good example of Application and Secret Exposures
4. Pull hello:latest- Good example of ServiceExposures (nginx)
5. Pull custom image from DockerHub via Artifactory to scan with JFrog Advanced Security
```

When the pull process has completed, you will be automatically redirected to the Scans List screen in the platform (in your browser) to review the results. See Appendix A to learn about the Scans List, the security navigation bar and types of findings you can review. If you are working with sample images (WebGoat or Netdata), please see Appendix B.

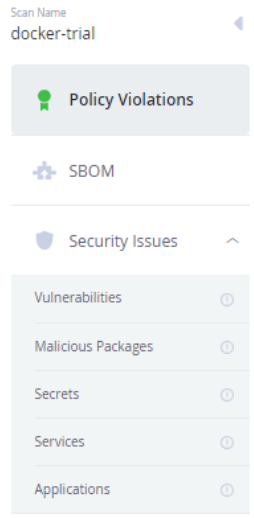
Option B - Push Docker image from local machine to scan with JFrog

The script will assist you with pushing images from your local machine to the 'local-docker-repo' repository.



Appendix A - Scan result structure

The JFrog scan reports are available under the “Security Issues” screen and contain comprehensive information about the broad set of scan results.



The report contains the following sections:

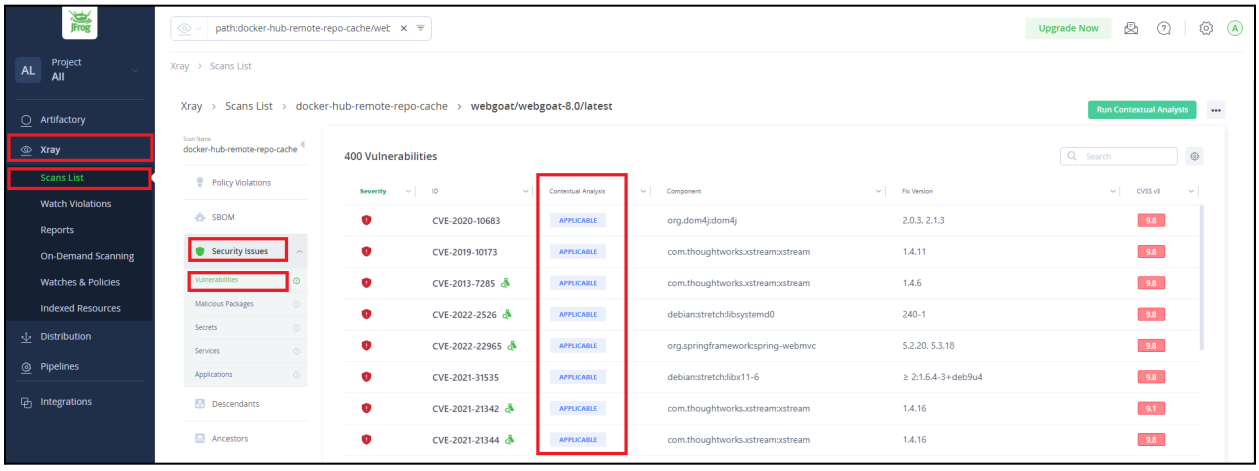
- **Policy Violations:**
  - An aggregation of security issues that cause a violation of the policy. In step 1 we have configured the following policy:
    - Trigger a violation upon Critical CVSS Score
    - Trigger a violation upon High impact exposure (of Secrets, Application, Services)
    - Trigger a violation upon detection of a malicious package
- **SBOM**
  - Lists all of the detected open source software components that were detected in the artifact, including the option to export the results in SPDX and CyclonDX formats
- **Security Issues → Vulnerabilities:**
  - Lists all of the CVEs that were found. For Docker containers, you can see the results of “Contextual Analysis” scanning that allows you to prioritize the open source software vulnerabilities that are actually exploitable (applicable or not) in your application.
- **Security Issues → Malicious Packages:**
  - Discover and eliminate unwanted or unexpected malicious packages, using JFrog’s unique database of malicious packages.
- **Security Issues → Secrets:**
  - Detect secrets left exposed in any containers stored in JFrog Artifactory to prevent any accidental leak of passwords, API keys, internal tokens, or credentials.
- **Security Issues → Services:**
  - Discover whether common services (such as Nginx, envoy, Prometheus, Apache, and more) are configured insecurely, creating attack risks.
- **Security Issues → Applications:**
  - Discover if your developers are using OSS libraries insecurely, causing possible exposure.

Appendix B - Webgoat and netdata/1.13.0 examples

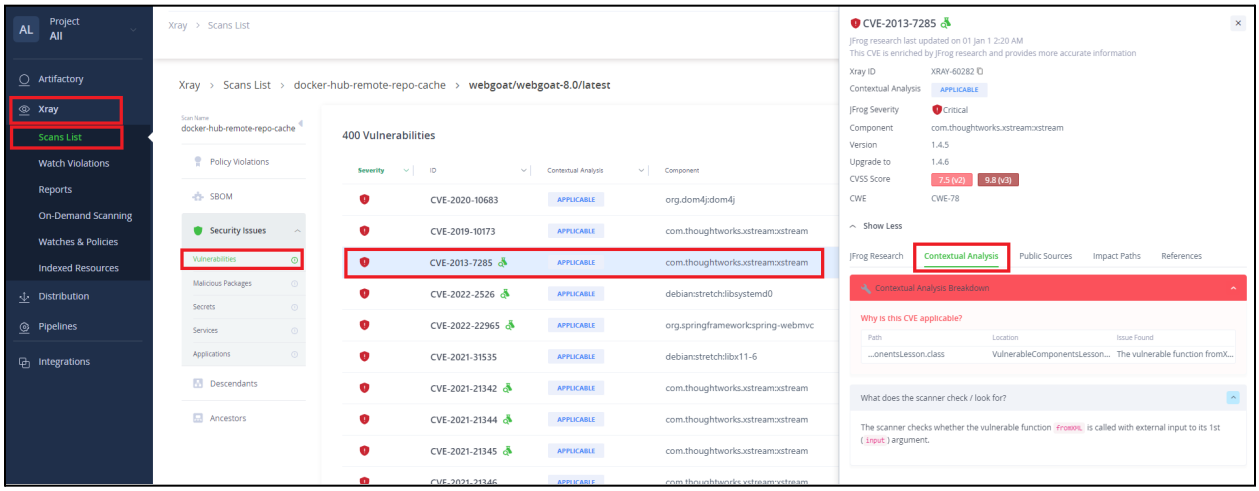
Example #1 | OWASP Webgoat

OWASP WebGoat is a deliberately insecure application that has vulnerabilities commonly found in Java-based applications that use common and popular open-source components.

This image contains many known vulnerabilities, so it is very useful for testing JFrog's Contextual Analysis capability, and to enjoy its value. For each identified vulnerability, the system will indicate if it's applicable or not in the specific context of the entire artifact (e.g., Docker container). When clicking on an applicable CVE or a not applicable one, you will be provided with proprietary CVE details, explaining and demonstrating how the applicability was determined. This will significantly reduce the noise that arises with not applicable CVEs, and allows you to focus on applicable CVEs, thus enabling your developers to save precious time while triaging vulnerabilities.



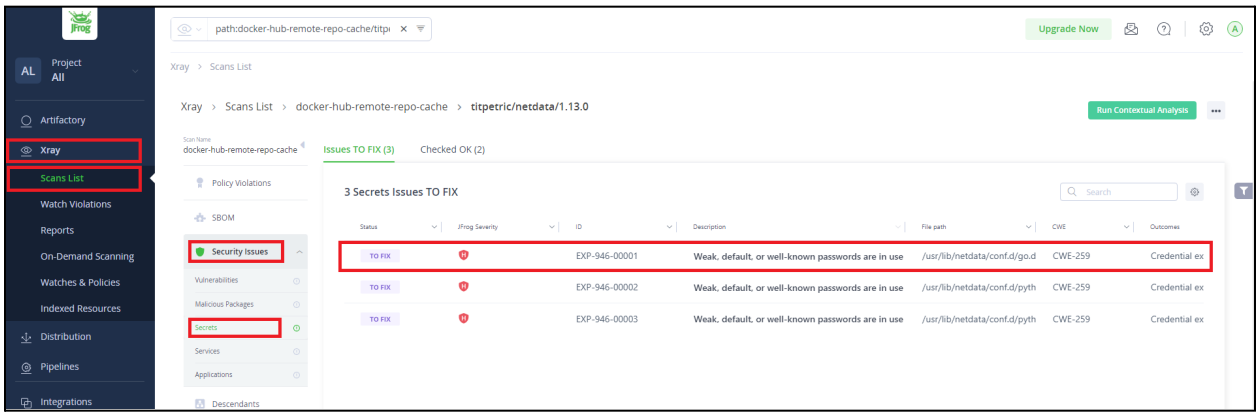
Under "Xray" > "Scans List" > "Security issues" > "Vulnerabilities" screen, you will find the complete list of identified CVEs. Please choose any of the "Applicable" or "Not Applicable" CVEs to reveal and review the additional information in the pane on the right of the screen. See the evidence that proves the CVE applicability and the following remediation steps to understand how the issue could be mitigated.



Example #2 | Netdata/1.13.0

Netdata provides distributed, real-time, performance and health monitoring for systems and applications. It is a highly-optimized monitoring agent you install on all your systems and containers. The Netdata Docker image has more than 100M+ downloads!

In the case of this specific version, the JFrog Secret Detection engine that scans for keys, credentials and API tokens, reveals a default weak password. When choosing one of the findings, you will be provided with information to point you accurately where the secret was found. It will also provide information about the risk, its implication, and remediation paths.



Under “Xray” > “Scans List” > “Security Issues“ > “Secrets” screen, you will find the complete list of revealed secrets. Please choose one of the findings to expand it and review the

additional information in the right pane. See the evidence that proves the secret is exposed and the following remediation steps to understand how the issue could be mitigated.