Lab 3 - VS Code (20 min)

OVERVIEW: In this lab you will experience JFrog Security's shift left capabilities when developing code in 'VS Code' IDE.

EXPECTED OUTCOME: Upon successful completion of this lab you will gain knowledge of how to use the JFrog Xray plugin within your IDE, in order to mitigate different security exposures: 1st party vulnerabilities, 3rd party vulnerabilities, and secrets.

Step by step instructions

Phase #1 - Scanning the source code:

1. Clone the demo project repository found in: https://github.com/jfrog/DevSecOpsDayEMEA2023/tree/main/secure-your-software-supply-chain
   Note: The repository is cloned to your dev machine, however, it is important to clone it to your own computer, where your IDE is accessible
2. Open the project in your IDE, navigate to the "Source" folder, and run the "npm install" command in the terminal in the IDE.
3. Go to the JFrog tool tab, and start the scan (This may take several minutes).

Phase #2 - Reviewing the results:

4. After the scan is complete, review the scan results in the JFrog tool tab. The different issues will be found in multiple files, for example:
   a. Server.js, bootstrap.js: 1st party code issues (SAST), and applicable vulnerabilities (SCA)
   b. package.json: Vulnerabilities in 3rd party packages (SCA)
   c. token.txt: Leaked secrets
5. Expand server.js in the scan results, and read about the 'Template Object Injection' issue. We encourage you to fix this issue, according to the suggested fix and re-run the scan.

Congratulations! You have completed Lab 3