Lab 3 - VS Code (30 min)

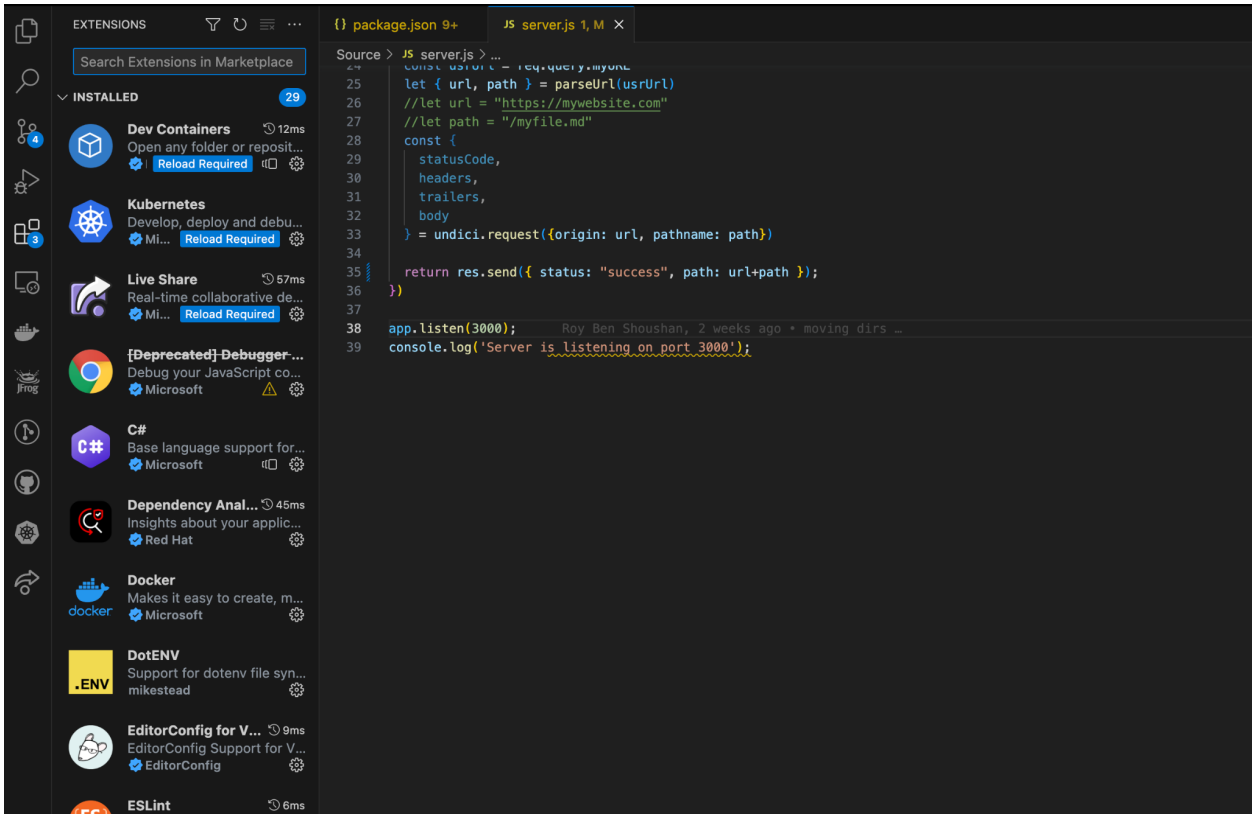
In this lab you will experience JFrog Advanced Security value when developing code in the IDE..

Upon successful completion of this lab you will gain knowledge of how to use the JFrog Xray plugin within your IDE, in order to mediate any 3rd party vulnerabilities, before committing your code.

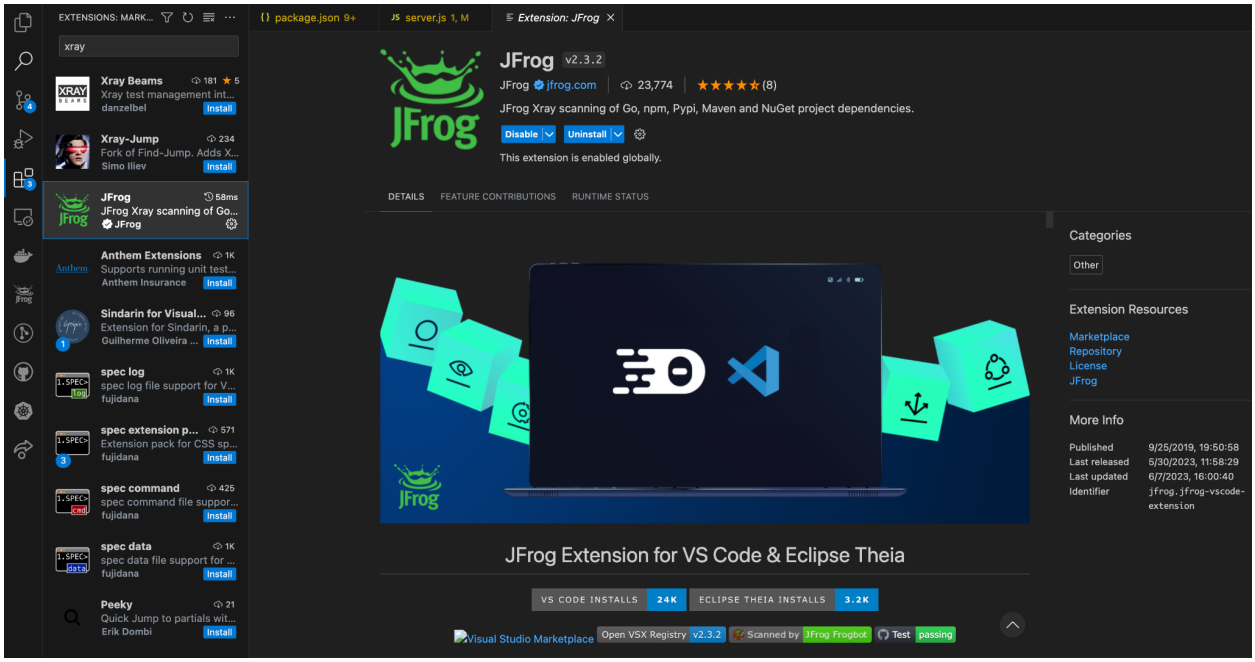
Step by step instructions

Phase #1 - installing the JFrog Xray IDE Plugin:

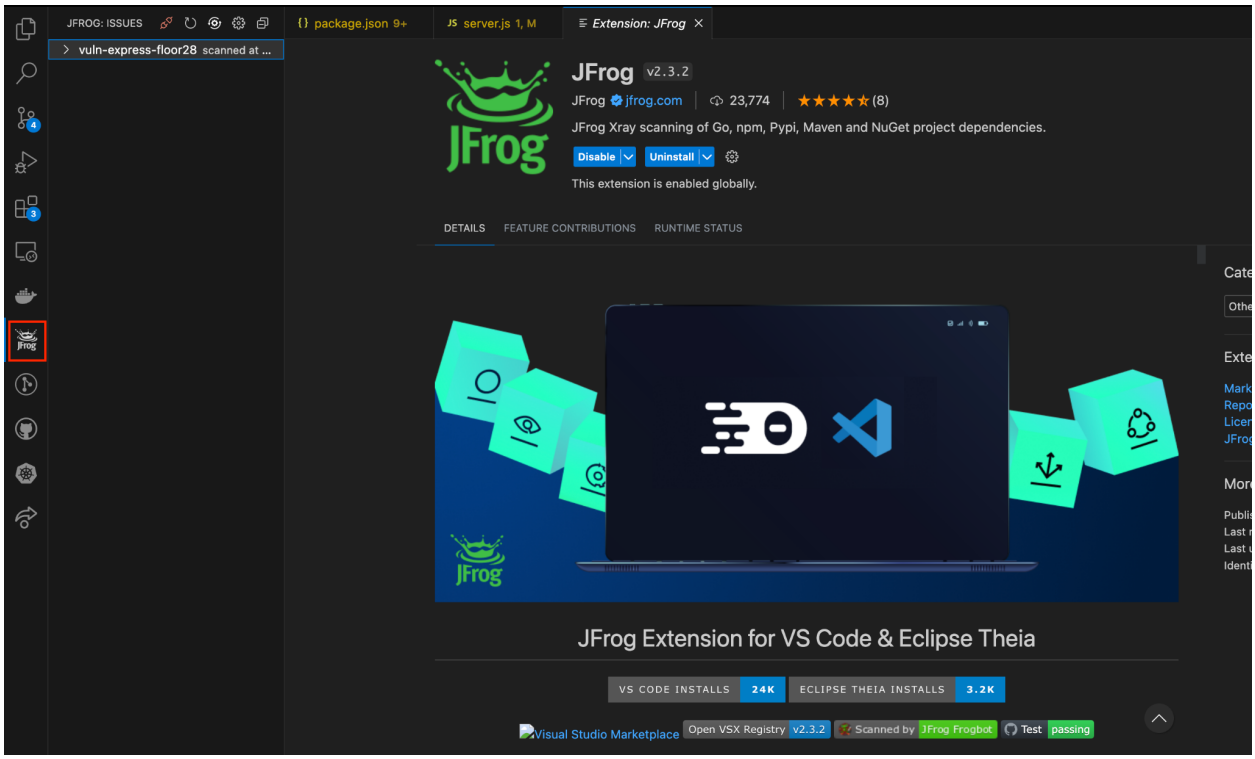
1. Click the Extensions icon in VS Code:



2. In the extension search bar search for “JFrog”, and then click install:



3. After the installation is complete, click the JFrog icon on the left toolbar:



4. Press the Enter your JFrog Platform connection details button, and update the URL, username and password (or API Token in case of SSO - this should be updated in the access token field) for

the trial created in Phase #1.

Phase #2 - Scanning the source code:

5. Clone the demo project repository found in: **https://gitlab.com/muldos/expressjs-appbundle-demo**
6. Open the project in your IDE, navigate to the “Source” folder, and run the “npm install” command in the terminal.
7. Go to the JFrog tool tab, and start the scan (This may take several minutes).

Phase #3 - Reviewing the results:

8. After the scan is complete, review the scan results in the JFrog tool tab. You should see to files in the scan results tab:
    a. package.json - This will have a list of vulnerable libraries referenced by the project.
    b. server.js - this file has references to the line of code that XRay concluded they have applicable vulnerabilities.
9. Expand the server.js in the scan results, and click on “CVE-2022-29078”. The vulnerability details should be presented in the details pane to the right, and the affected file should be opened in the editor, positioned on the vulnerable line in the code:
10. Fix the vulnerability based on the information on the details pane, and rerun the scan to check if the vulnerability has become inapplicable. The Vulnerability should be removed from the servers.js file, and when you click the vulnerable package in the package.json file, the CVE should no longer be reported.

Congratulations! You have completed the lab!