ISEC5000 **Assignment 1** **Due: Mar 18th**

Software Scanning and CVE

App Security Scanning

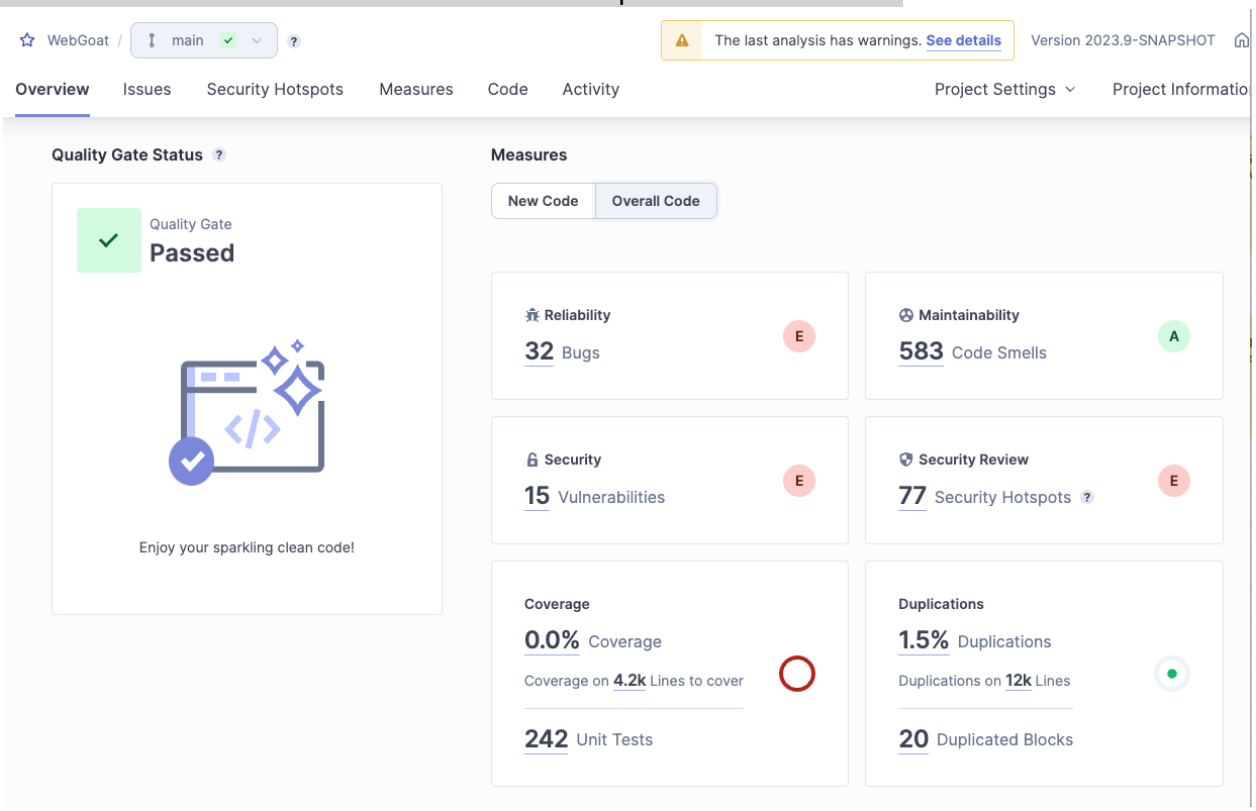
As discussed in class you will be picking a project from a past course at NSCC that is based in C#, JavaScript, or Java. You will need access to the source code as well as the application. Complete the following sections.

1) Main Purpose of the Application

<In 2-3 paragraphs describe the main purpose of the application, this is so I understand roughly what the application is – max one page>

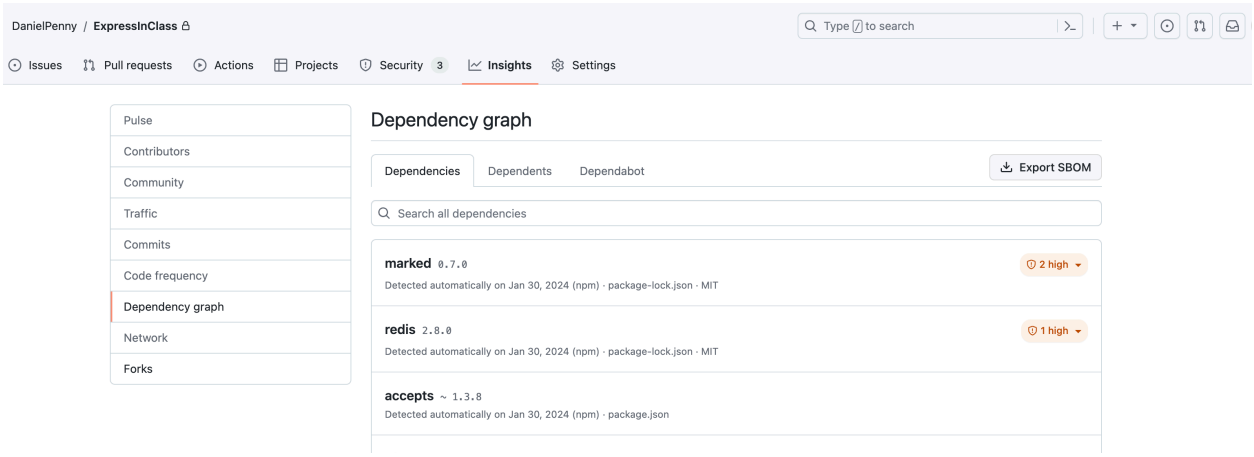
2) Setup and scan the Application using SonarCube

<Screenshot the results of the scan like the sample scan of WebGoat>



3) SCA Scan

- Include a SCA (Static Component Analysis) scan that finds outdated components, can use GitHub (Recommend Github) or a dependency analysis tool from OWASP. Most new projects will not have many outdated components – Include a summary screenshot of this showing no vulnerabilities and the SBOM (Software Bill of Materials)
-



4) Identify the top 3 issues from the above scans, from the above 2 scans. Security issues must be included first but if there are NO security issues, then use other issues within the scan. If there are not enough of them, please contact the instructor.

<u>For Each Issue Discovered Describe (in max 2 pages per CVE – likely one page or less)</u>

For all 3 of the Issues identified

- Investigate in SonarCube or SCA (CVE)
- Understand & describe the issue.
    - Investigate via web and LMM if needed.
- Describe in your own words how this vulnerability could be exploited, or why the issue could lead to a vulnerability.
- Note: if it's one of the OWASP top 10, which one
- Understand what is needed to fix it.
- In your own words (not a cut and paste of the vulnerability remediation text) describe the cause, and how you might fix it.
- If there are multiple options, you can describe them both).

Upload the file to Brightspace drobox "Assignment 1 - App Security Scanning."
Folder location "Assignment 1 - App Security Scanning"

Due Mar 18 @ midnight