**GitHub Flow for Security and Vulnerability Checks with Snyk**

This document outlines the GitHub workflow for identifying and mitigating vulnerabilities in a repository using Snyk.

**Prerequisites**

1. **Set up Snyk**:
   * Install the Snyk CLI***: npm install -g snyk.***
   * Authenticate with Snyk: ***snyk auth.***
2. **Repository Setup**:
   * Ensure the repository is cloned locally***: git clone <repository-url>.***
   * Navigate to the project directory: ***cd <repository-folder>.***

**Workflow**

**1. Create a New Branch**

* Use feature branches for security assessments.
* Command:  
  “***git checkout -b snyk-fix***”

**2. Install Dependencies**

* Ensure all dependencies are installed for accurate analysis.

Command:  
“***npm install***”

**3.Run Snyk Security Checks**

* Use Snyk CLI to scan for vulnerabilities:  
  “***snyk test***”
* monitor the repository for future vulnerabilities:  
  “***snyk monitor***”

**4.Using the Snyk Desktop resolving the Vulnerabilities**

* by opening multiple fix PR’s and upgrading patches helped resolve most of the errors.
* Upgrading certain version of libraries helped resolved critical issues.

**5. Analyze Results**

* Review the output for:
  + Severity of vulnerabilities (low, medium, high, critical).
  + Suggested fixes or updates.

**6. Apply Fixes**

* Automatically fix issues when possible:  
  “***snyk fix***”
* Manually update dependencies as suggested by Snyk via the snyk desktop

**7. Commit and Push Changes**

* Commit the fixes to the branch:  
  “***git add .***   
  ***git commit -m "Fix vulnerabilities detected by Snyk***"
* Push the changes to GitHub:  
  “***git push origin snyk-security-checks***”

**8. Create a Pull Request**

* Open a pull request (PR) to merge changes into the main branch.
* Add a description detailing:
  + Vulnerabilities detected.
  + Fixes applied.

**9. Review and Merge**

* Collaborate with team members to review the PR.
* Ensure all tests pass.
* Merge the PR into the main branch.

**10. Maintain Security**

* Regularly run this command to ensure no new vulnerability arises as the code may have regular changes and updations in it  
  “***snyk test***”
* Monitor and address the vulnerabilities regularly.