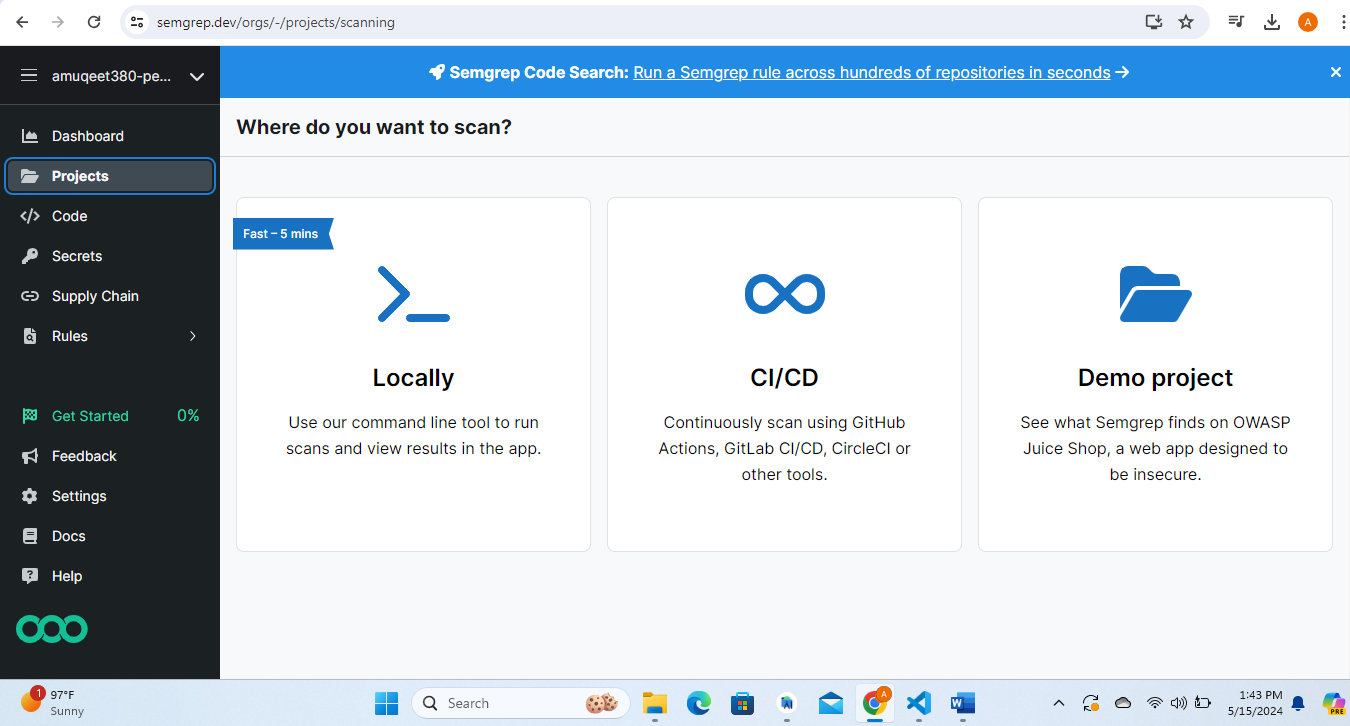
**Assignment no 3**

**Abdul Muqeet(4872)**

**1)Successfully install the Semgrep.dev**

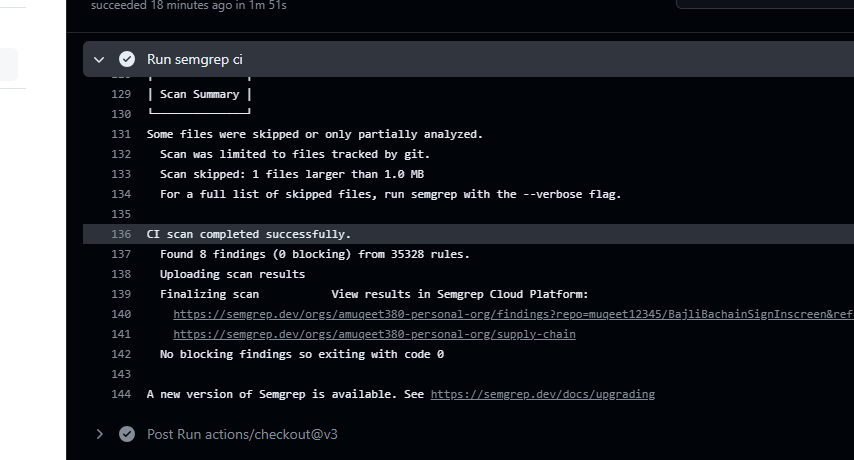


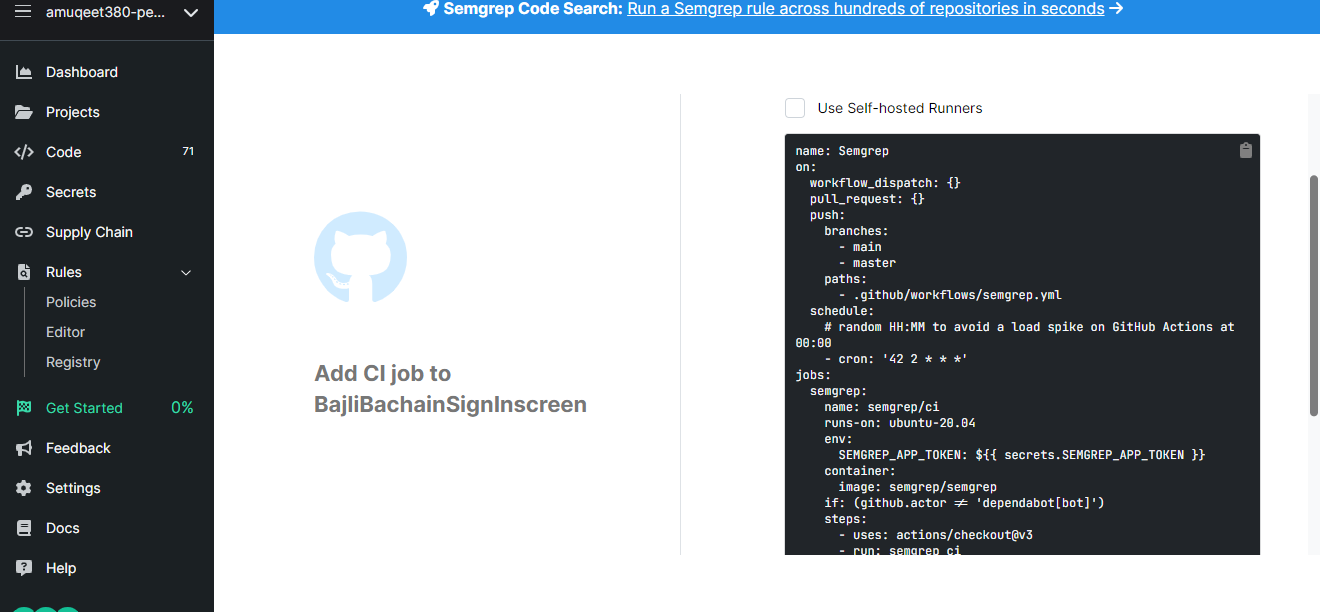
2) Recently I created a Screen of my app in JavaScript(react native) then i push on github

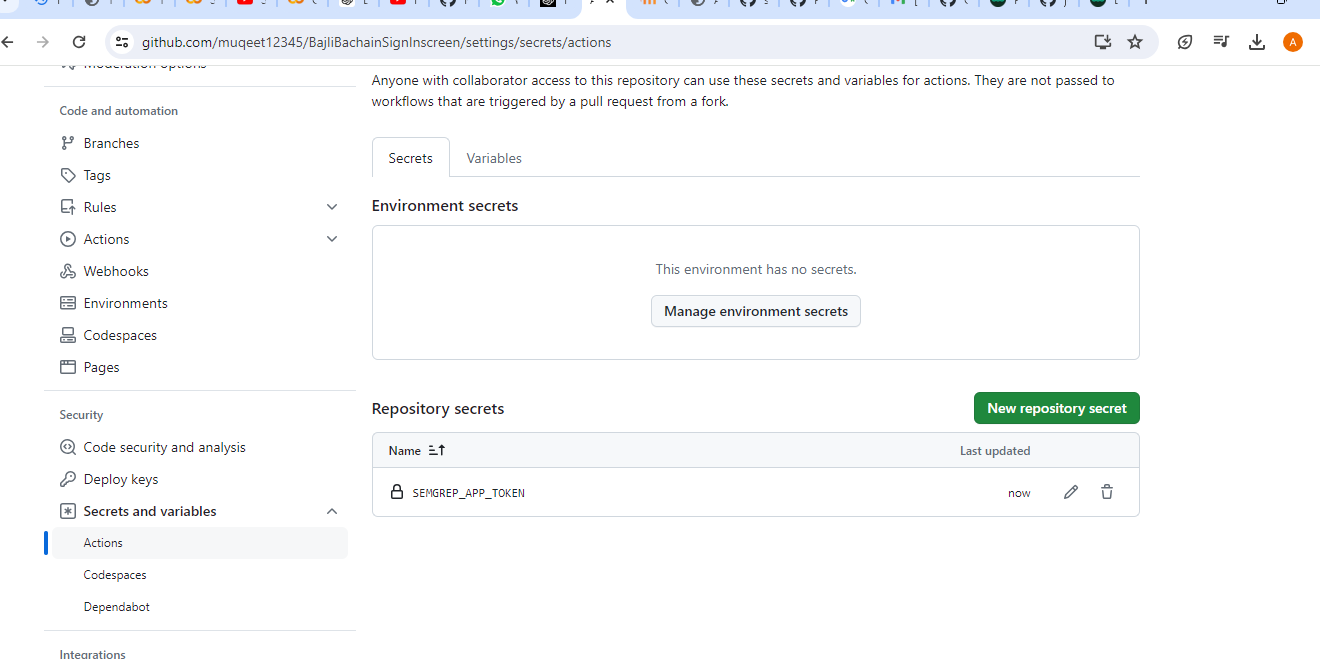
Here is the link of Github repository: https://github.com/muqeet12345/BajliBachainSignInscreen

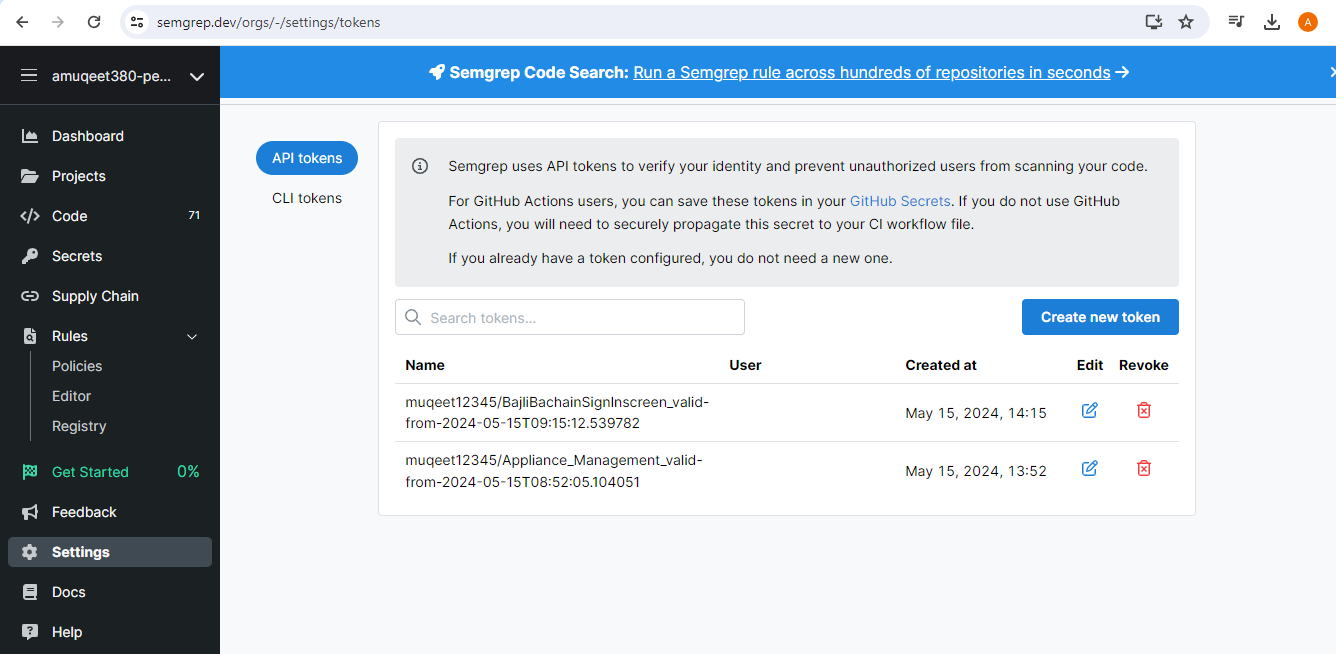
.Then I perform a Scanning a github Action on Semgrep App.

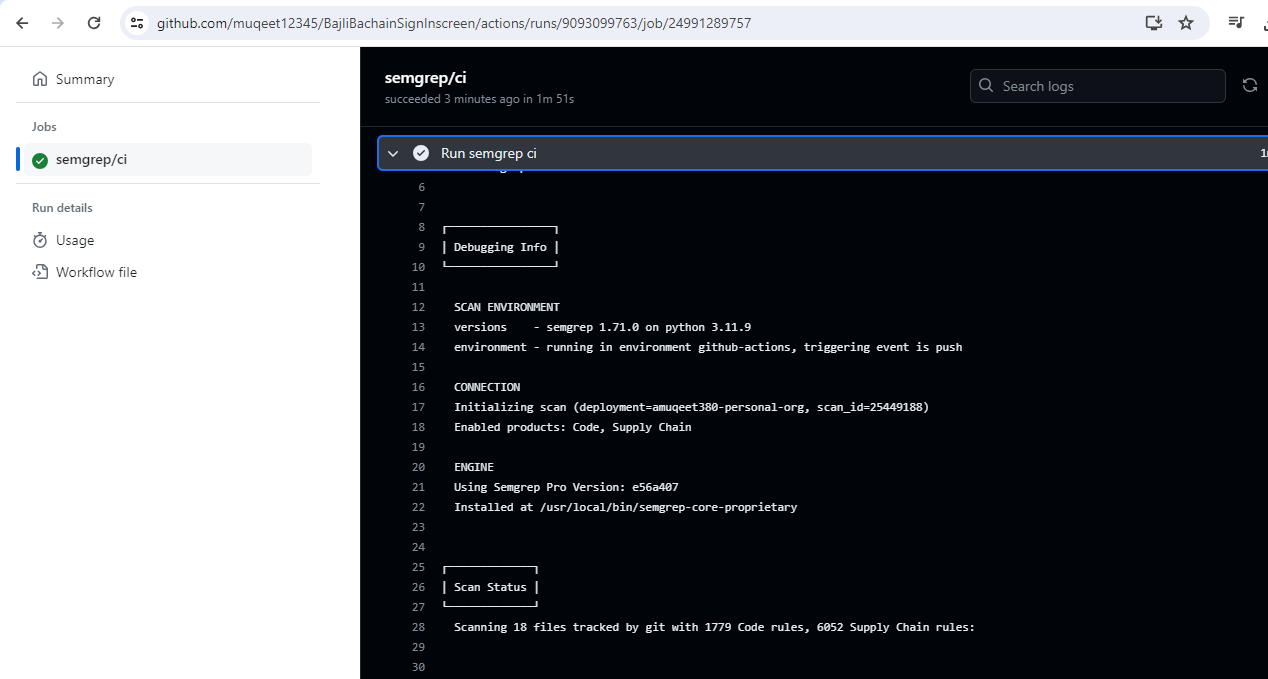
**Rules**

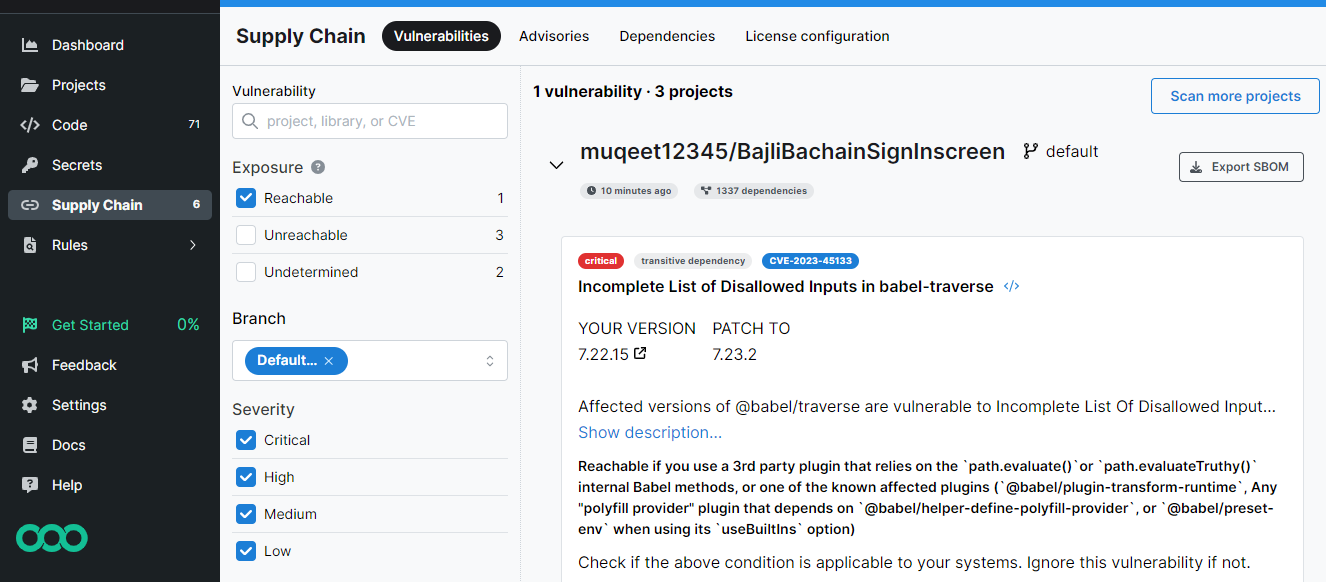












**Secuirty Issues:**

Semgrep identified several security issues and coding errors in the project codebase that could have a significant impact on project integrity and security One important issue found was a possible SQL injection vulnerability in some database queries .SQL injection vulnerabilities arise when user-controlled input is added directly to SQL queries without proper cleaning, opening the door for attackers to execute arbitrary SQL commands, corrupt the database, and obtain compromised information need In addition, cross-site scripting (XSS) by Semgrep ) flagged instances of vulnerabilities, which occur when untrusted data is added to a network without proper escape, allowing attackers to run scripts negatively penetrate networks viewed by other users XSS vulnerabilities can lead to cookie theft, session hijacking, and unauthorized access to user accounts. In addition, Semgrep found coding errors such as zero pointer dereferences, resource leaks, which could lead to application crashes, data corruption, or denial-of-service (DoS) attacks if left uncorrected. It is important to reduce the risk of service disruption and reputational damage Address these issues first to ensure the business can withstand potential cyber threats and retain users and a they trust the participants.

**References**

# YouTube video:”Scanning code with Semgrep using GitHub Actions”

https://www.youtube.com/watch?v=BqU7P84ZaUc