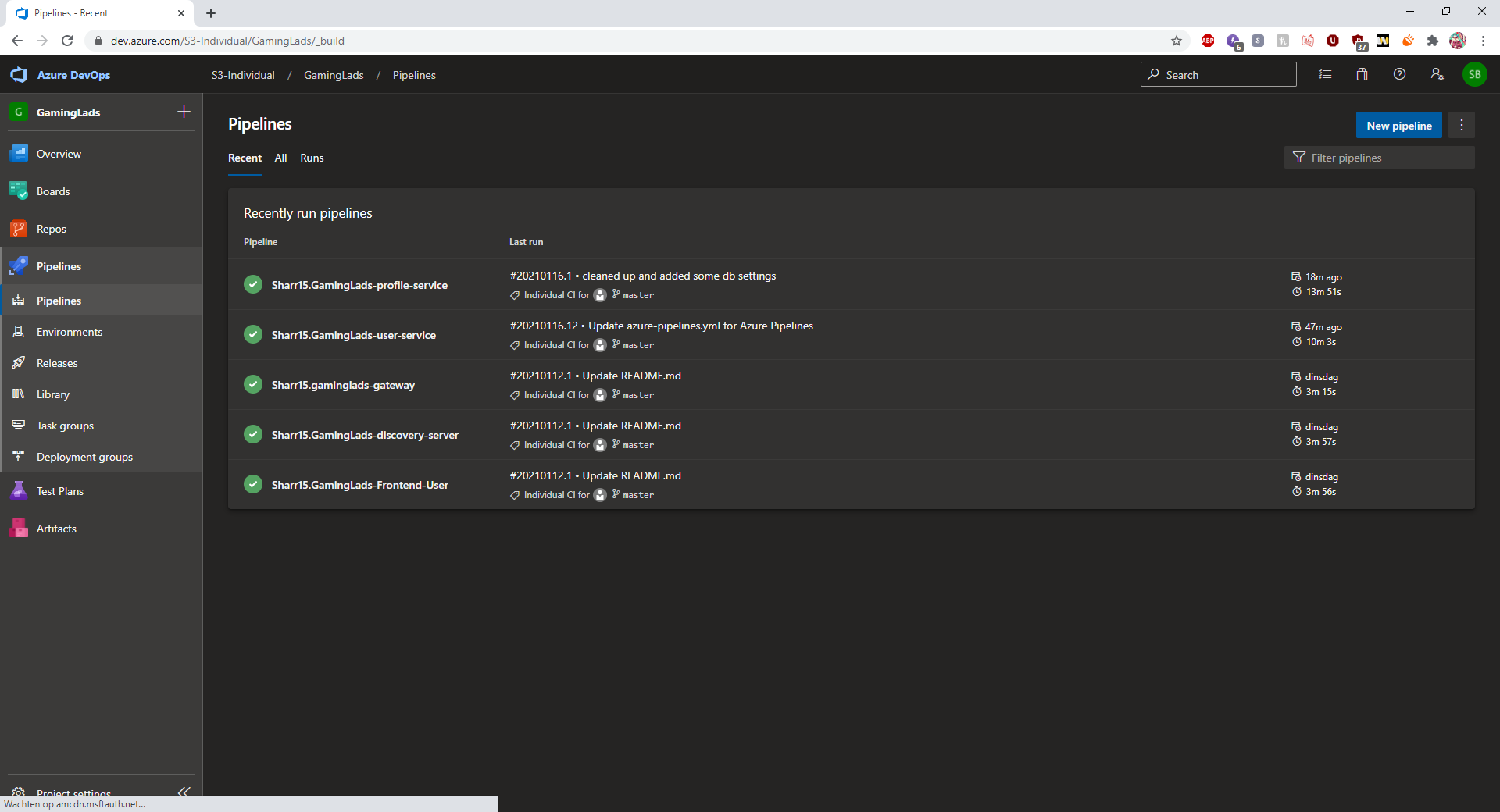
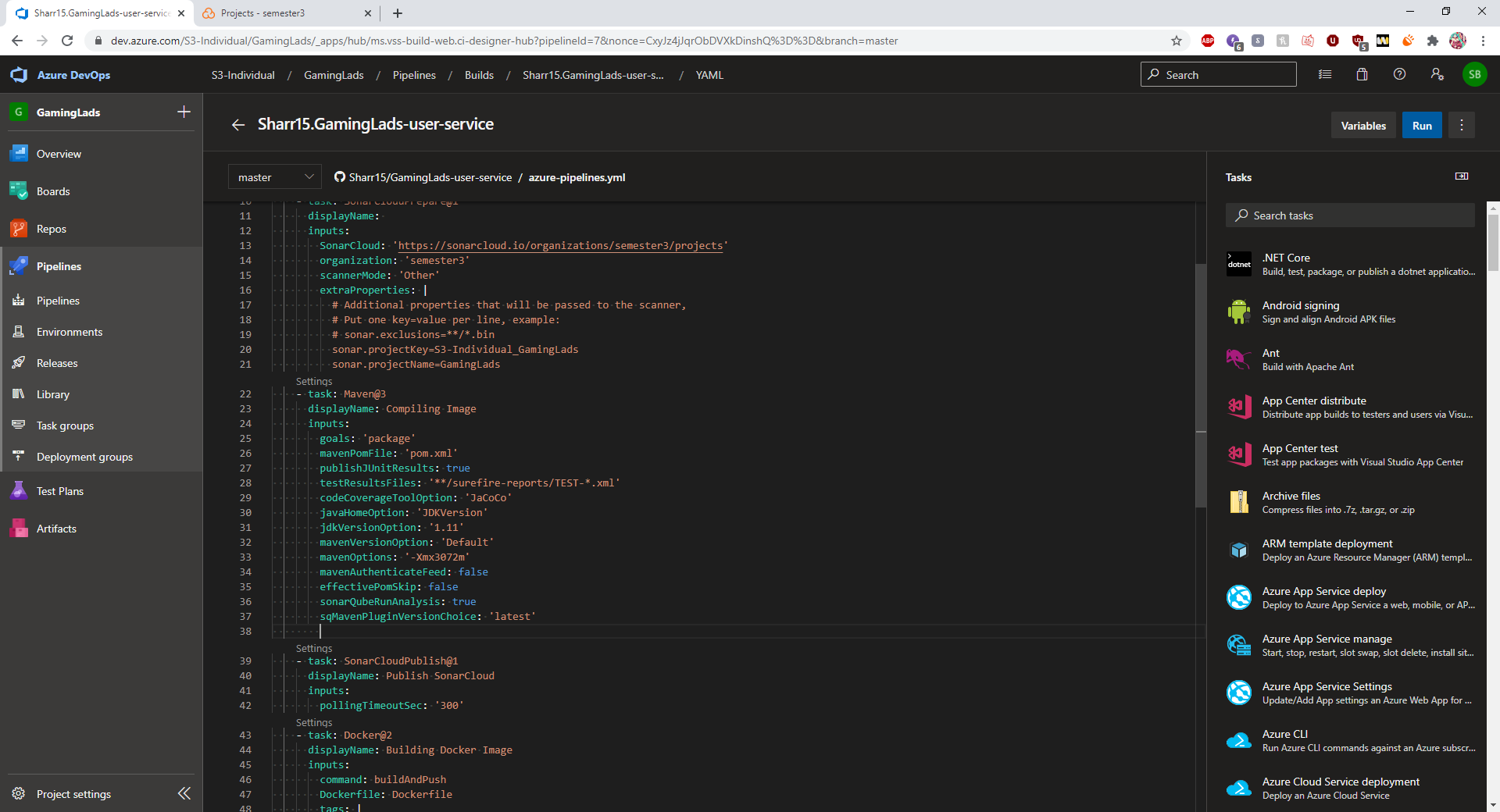
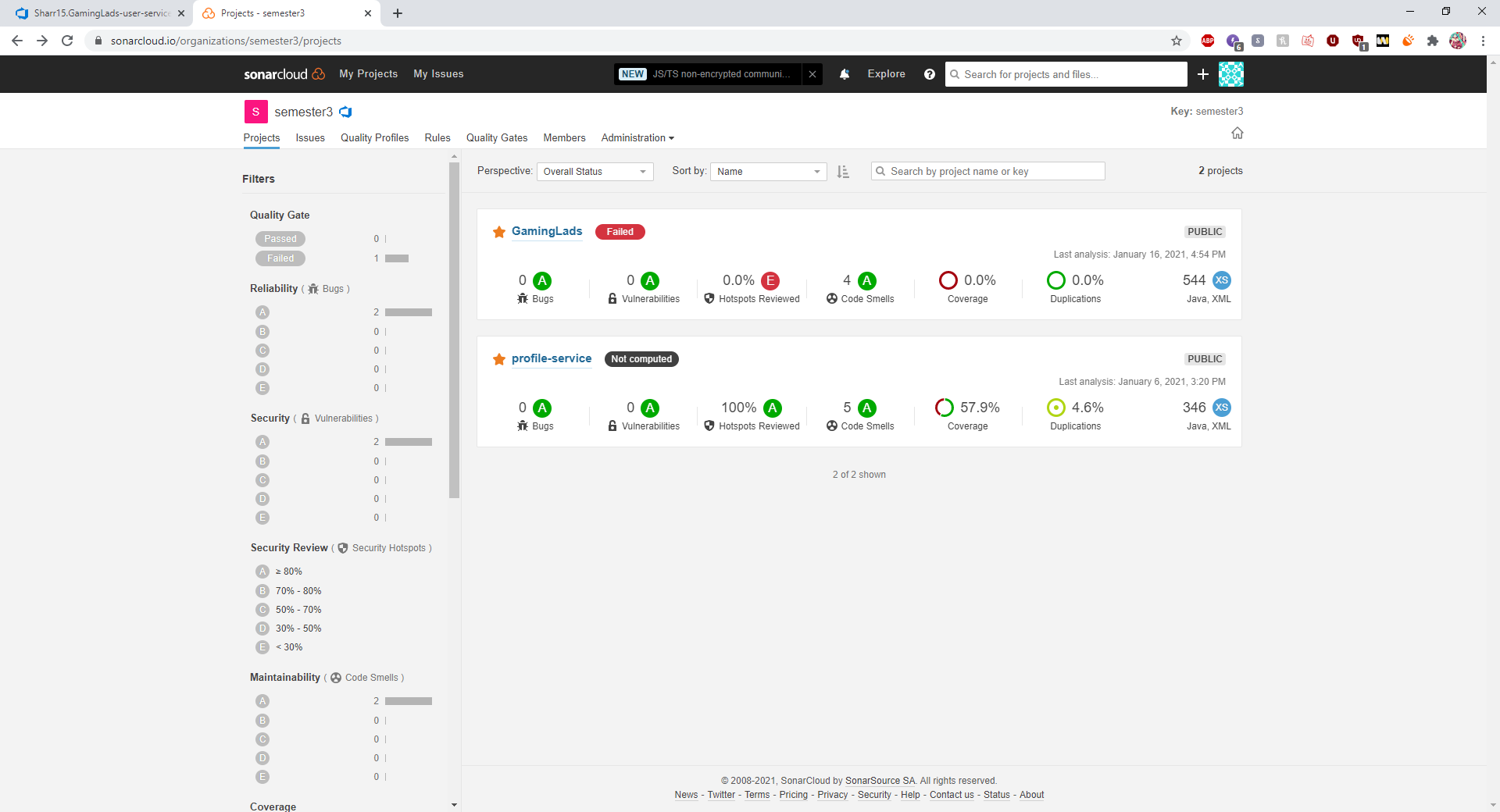
CI/CD met Sonarcloud en Heroku

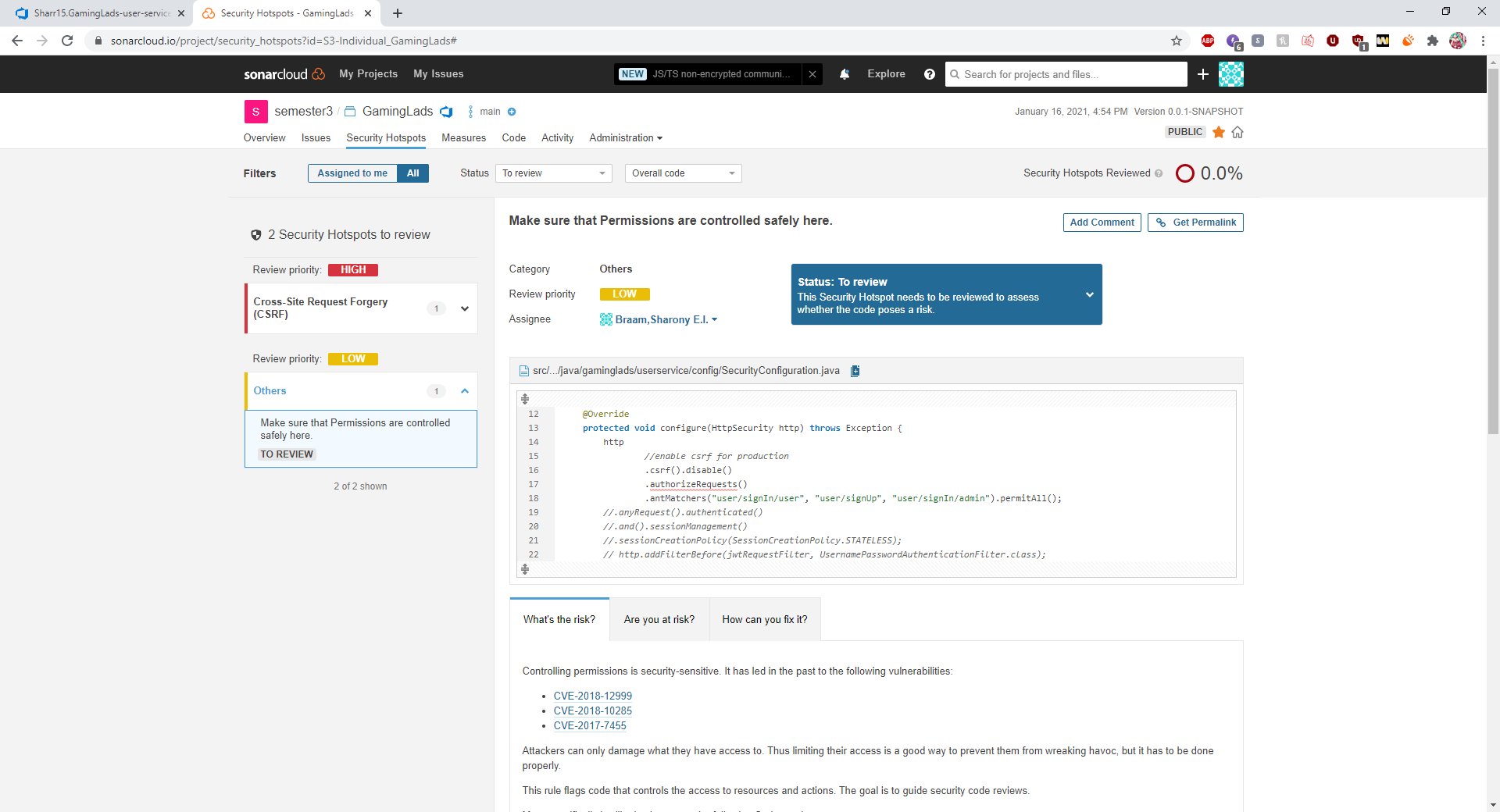
De CI/CD runt in Azure DevOps. Elke service, server en front-end die gebruikt worden in het GamingLads worden gebruikt heeft een eigen pipeline.



Dit is een voorbeeld van een pipeline:

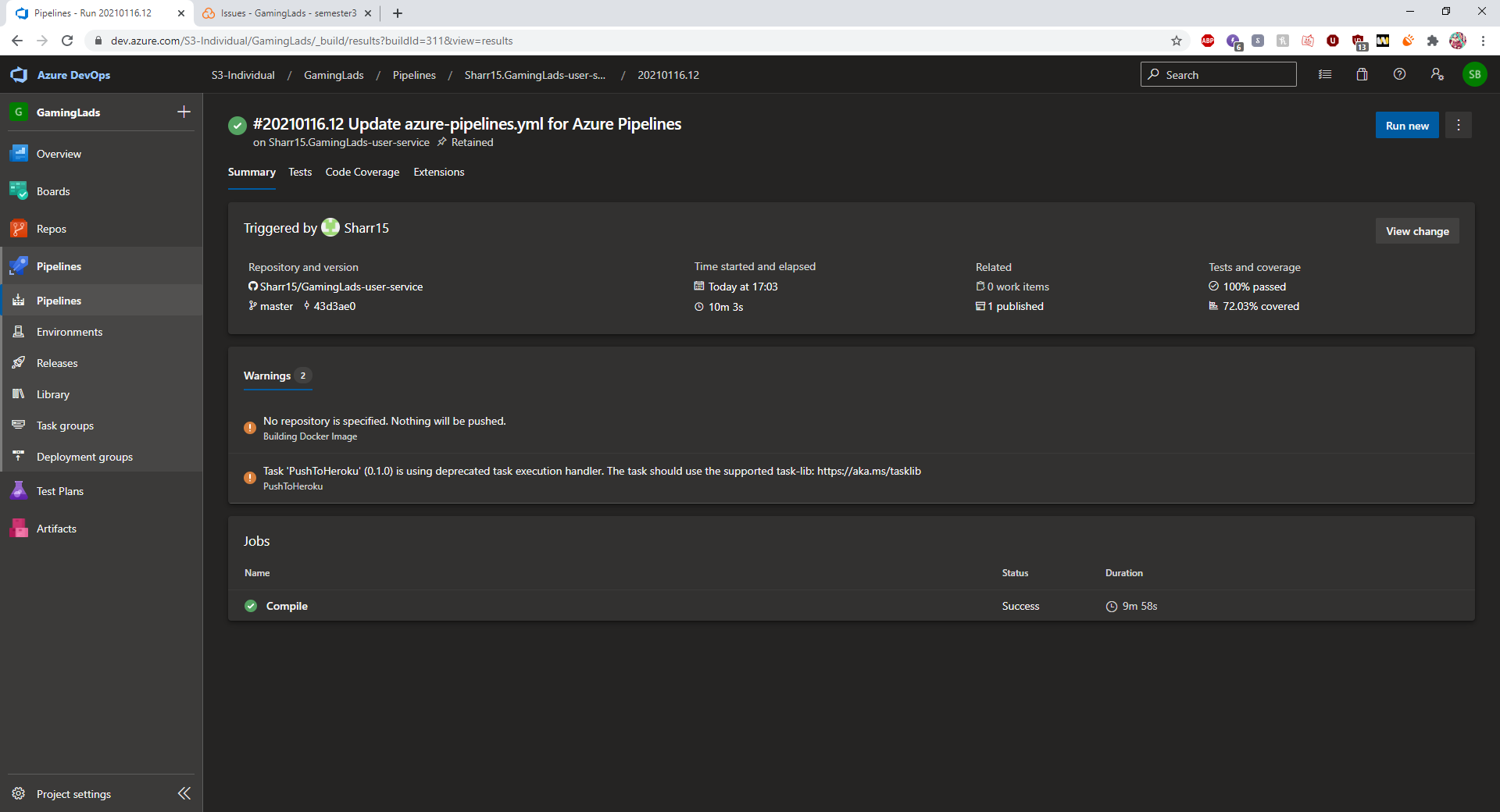


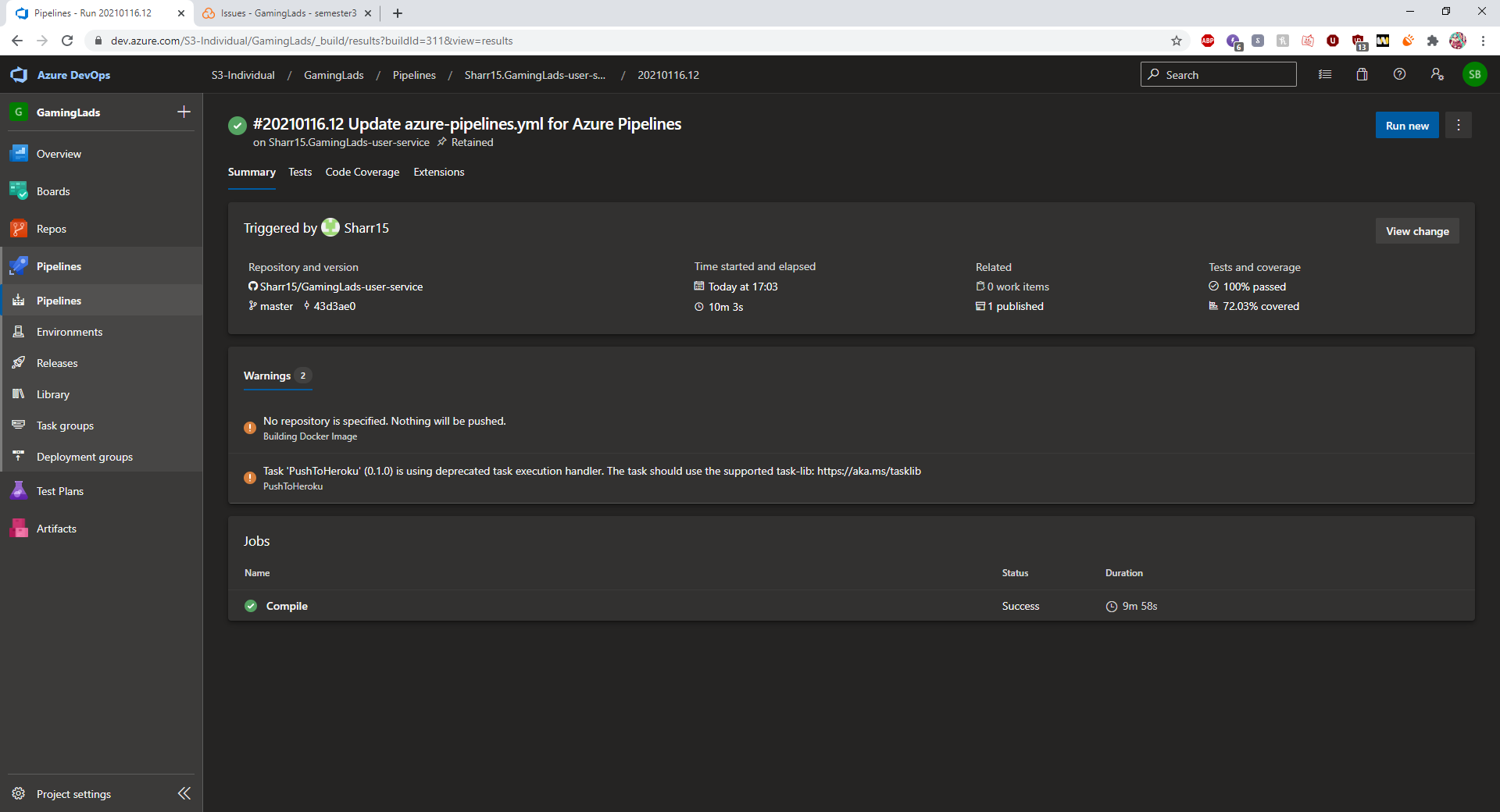
De resultaten worden naar sonarcloud gepusht. Alleen code coverage werkt daar niet. Als er lokaal naar sonarcloud wordt gepusht, werkt dat wel. Dat is te zien in deze foto.

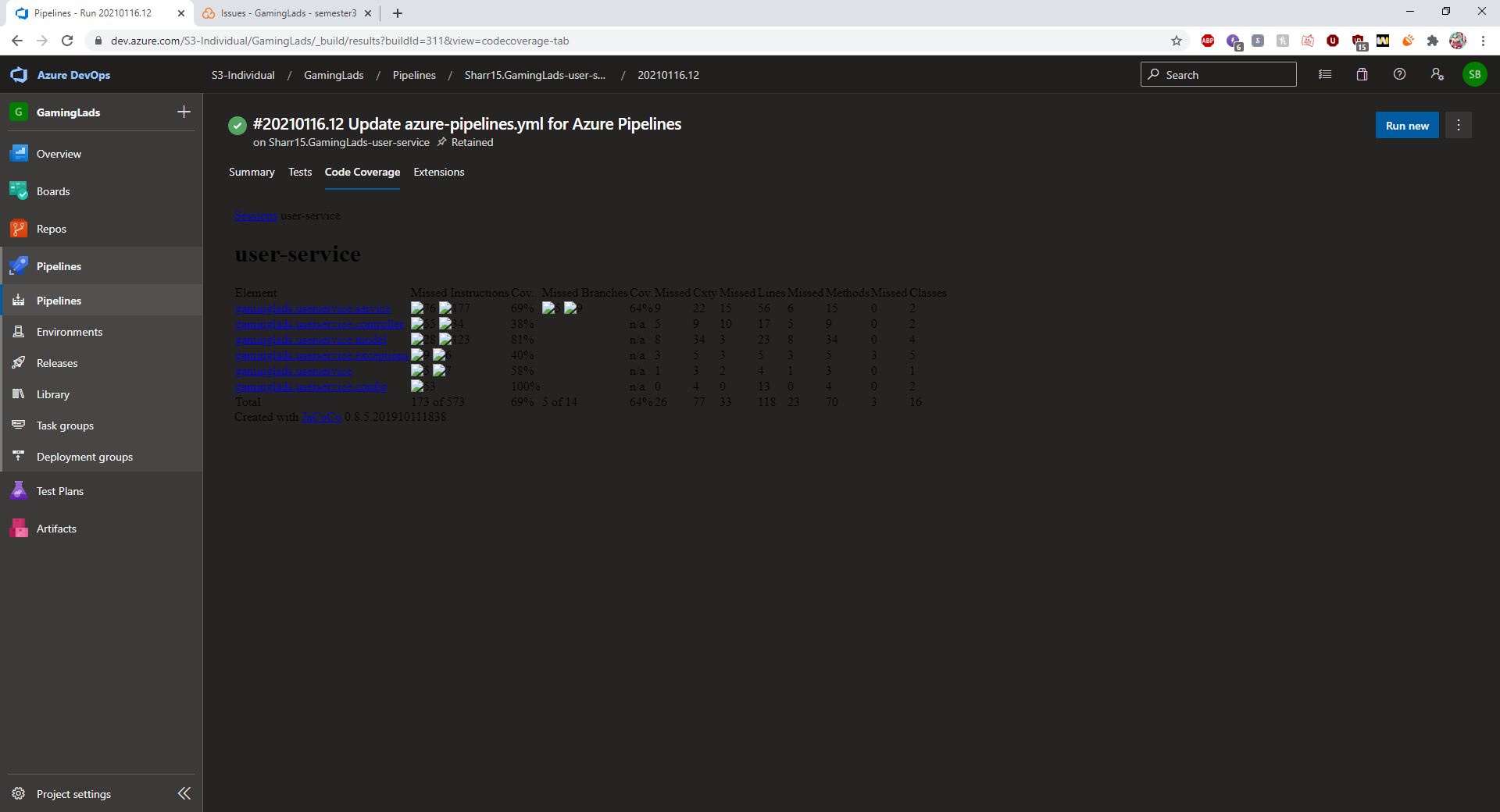


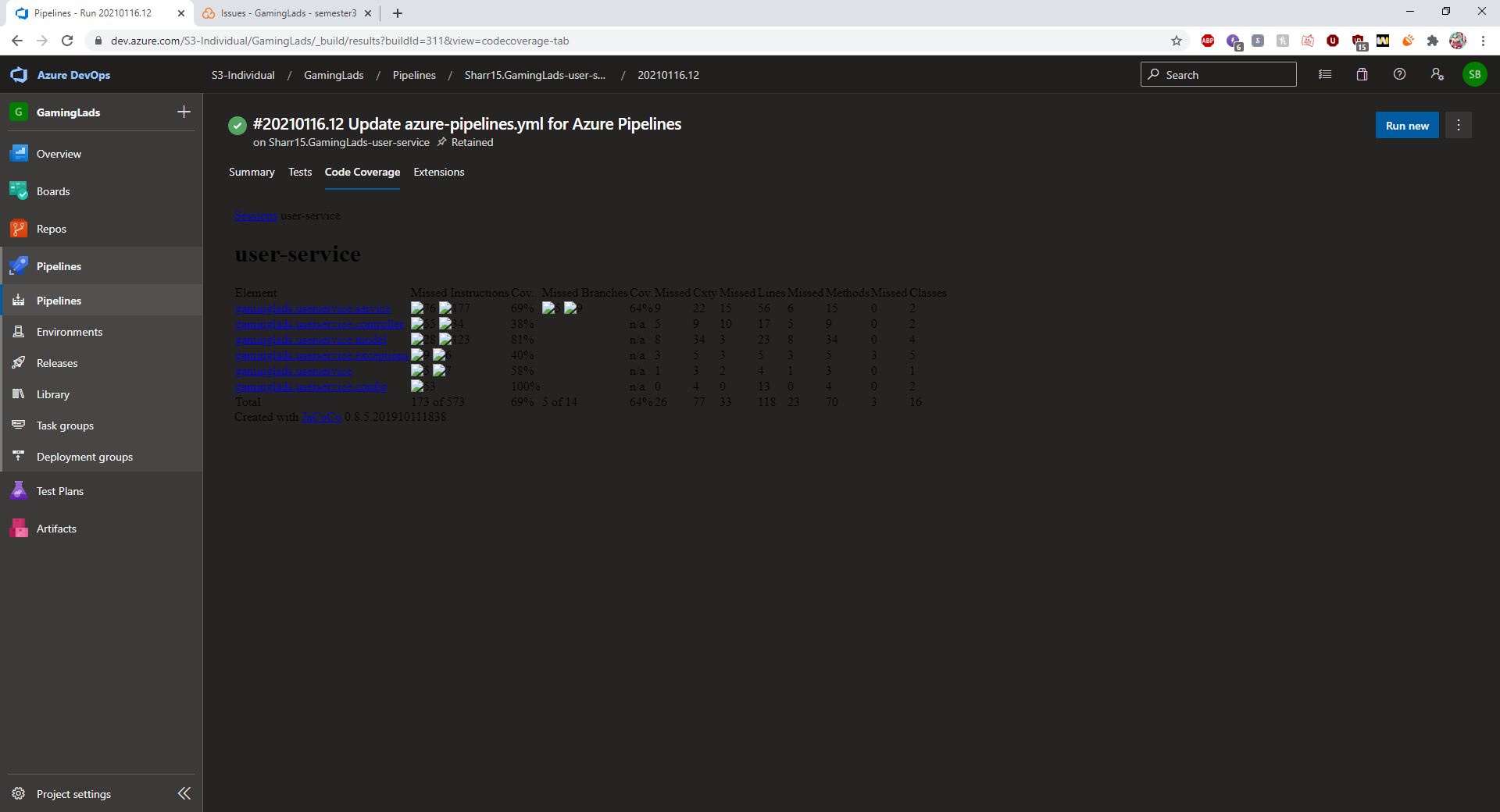
Er zijn twee security hotspots. De eerste heeft te maken met CSRF. Dit betekent Cross-Site request Forgery en houdt in dat een persoon een request kan sturen en er een klein script in kan schrijven die wat dingen uitvoert en dan wordt bijvoorbeeld een slachtoffer erin geluisd om ergens op te klikken, wat niet van de website zelf is. Dit is in production heel gevaarlijk, er kan namelijk data naar buiten worden gelekt op deze manier. Om dit aan te zetten is heel simpel. “csrf.enable()” en het is gedaan. Vaak hebben front-end frameworks geen automatische csrf protection dus moet dat via de backend geregeld worden. Hij is hier disabled omdat er een hoop errors waren en er was nog geen oplossing voor gevonden. De tweede security hotspot gaat over de authorizerequests. Het project zou rollen krijgen, maar daar was geen tijd meer voor.

Het jacoco rapport staat wel in Azure DevOps. Hierin staat wel de code coverage.









Nadat de resultaten naar SonarCloud gepusht zijn, wordt het naar heroku gepusht.

