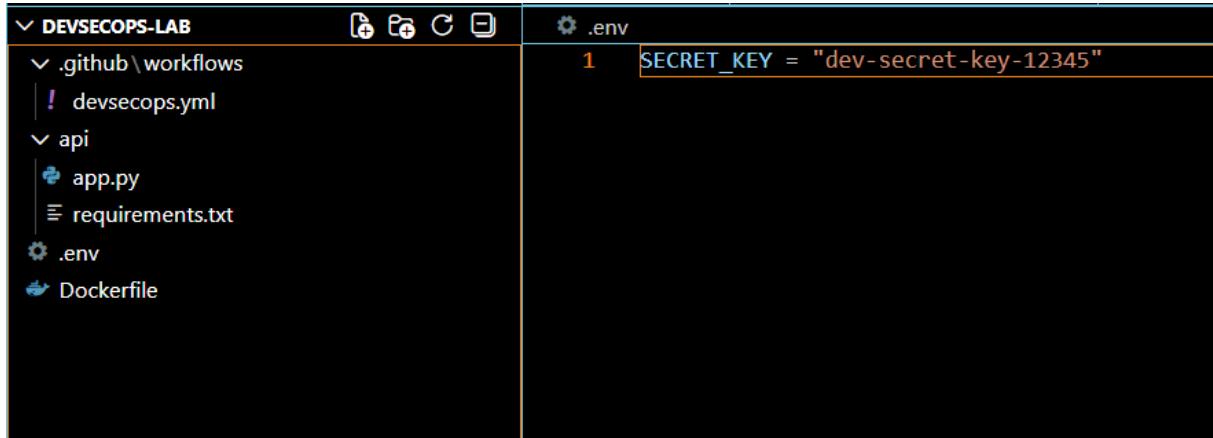


Nom : ARCHILLE Prénom : Vladimir Date : 20 Décembre 2025

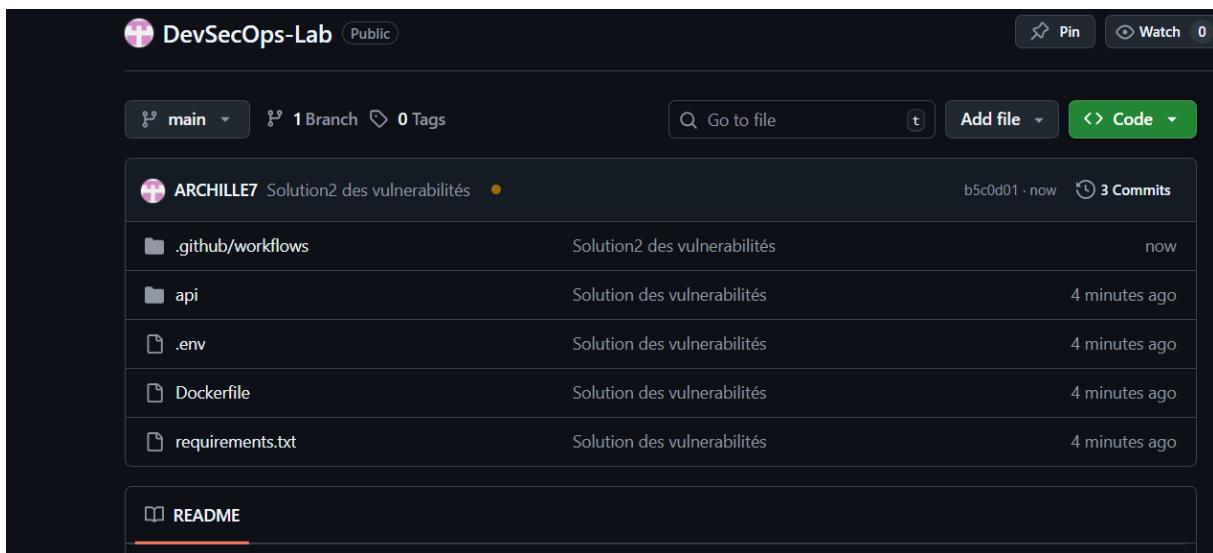
Rapport Atelier DevSecOps-LAB

1. Création d'un fichier .env pour stocker le SECRET_KEY

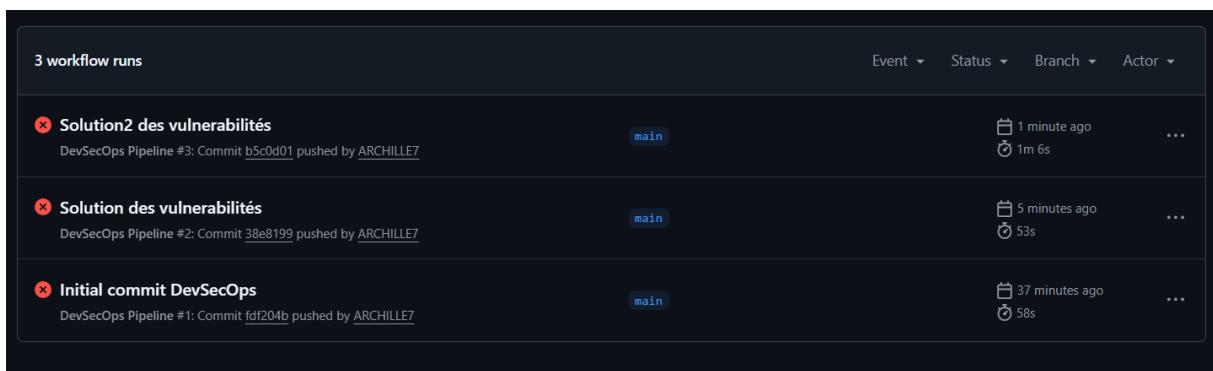


```
SECRET_KEY = "dev-secret-key-12345"
```

2. Exécution en cours



3. Le résultat après exécution, avec les erreurs de vulnérabilités.



4. Le résultat après exécution, Sans les erreurs de vulnérabilités

4 workflow runs			
	Event	Status	Branch
✓ Solution3 des vulnérabilités DevSecOps Pipeline #4: Commit e29fb49 pushed by ARCHILLE7	main	3 minutes ago ⌚ 1m 34s	...
✗ Solution2 des vulnérabilités DevSecOps Pipeline #3: Commit b5cd01 pushed by ARCHILLE7	main	16 minutes ago ⌚ 1m 6s	...
✗ Solution des vulnérabilités DevSecOps Pipeline #2: Commit 38e8199 pushed by ARCHILLE7	main	20 minutes ago ⌚ 53s	...
✗ Initial commit DevSecOps DevSecOps Pipeline #1: Commit fdf204b pushed by ARCHILLE7	main	51 minutes ago ⌚ 58s	...

5. Corrections apportées :

- Création d'un fichier .env pour stocker le code secret
- Protection de l'injection SQL
- Contre l'exposition des informations sensibles dans /debug
- Le docker s'executait en root maintenant on a renforce la sécurité runtime
- La dépendance qui n'était pas contrôlée maintenant le Scan Trivy est plus fiable