Question 1 : Pourquoi devons-nous utiliser les secrets GitHub (DOCKER_USERNAME, DOCKER_PASSWORD) dans le fichier ci.yml pour l'authentification à Docker Hub ?

Nous devons utiliser les secrets GitHub (comme DOCKER_USERNAME et DOCKER_PASSWORD) car ce sont des **informations sensibles et privées** .

- Le fichier ci.yml est un fichier de code qui se trouve dans notre dépôt Git. Le code de notre dépôt est public (ou visible par toute l'équipe), y compris l'historique des modifications.
- Si on écrivait le mot de passe Docker Hub directement dans le fichier ci.yml, **n'importe qui pourrait le voir** en regardant le code .
- Les secrets GitHub permettent de **stocker le mot de passe en toute sécurité** sur GitHub, en dehors du code. Le pipeline peut y accéder pendant l'exécution sans que la valeur réelle ne soit exposée dans le fichier YAML ou dans les logs. C'est essentiel pour la sécurité .

Question 2 : Quels sont les risques associés au stockage des informations sensibles dans des pipelines CI/CD et quelles sont les meilleures pratiques pour limiter ces risques ?

Le principal risque est la **compromission de la sécurité** ou le **vol d'identifiants** .

Si un attaquant trouve notre mot de passe stocké par erreur ou si un secret est mal géré, il pourrait :

- **Pousser des images malveillantes** sur notre Docker Hub ou Registre Privé.
- Accéder à nos **serveurs de production** ou à nos services Cloud, si les identifiants ont trop de permissions.

Pour limiter ces risques, voici les **meilleures pratiques**:

- **Utiliser uniquement des secrets GitHub :** Ne jamais mettre d'informations sensibles directement dans le fichier ci.yml (comme notre mot de passe Docker) .
- **Donner le moins de droits possible :** Toujours créer des **Jetons d'Accès** (tokens) pour le pipeline qui ont seulement les permissions nécessaires (par exemple, seulement l'autorisation de **pousser** les images Docker, et non de les supprimer ou de modifier les paramètres du compte).
- **Limiter l'accès aux secrets :** Configurer les secrets de sorte qu'ils ne soient accessibles que dans les environnements et les branches de confiance (comme la branche main).