

Projet Sécurité: CTF



GROUPE	BACKDOOR	SCENARIO 21/10
PHASE 1	DEVELOPPEMENT CTF	WEB
NIVEAU	FACILE	



Sur la page d'accueil du site de l'université fictive XYZ ,vous remarquez un bouton qui vous rederige vers la page "login.html".

Temps estimé: 10 mins

Étape 1 : Injection SQL dans le formulaire de connexion

Vous découvrez une interface de connexion . elle vous invite à vous connecter avec un nom d'utilisateur et un mot de passe.

L'équipe d'Injections Inc. a mis en place une sécurité basique pour vérifier les informations de connexion, mais ils n'ont pas anticipé un attaquant astucieux. Connectez vous en tant qu'admin et récupérer le flag .

Étape 2 : Interrogation de la base de données

Après avoir réussi la première étape, vous êtes redirigé vers une nouvelle page . Ici, une interface vous permet d'interroger la base de données si vous etes admin. Vous remarquez un commentaire laisser au admin pour lui montrez la syntaxe de qustion à poser.

Posez la bonne question à la base de données pour récupérer un flag généré.