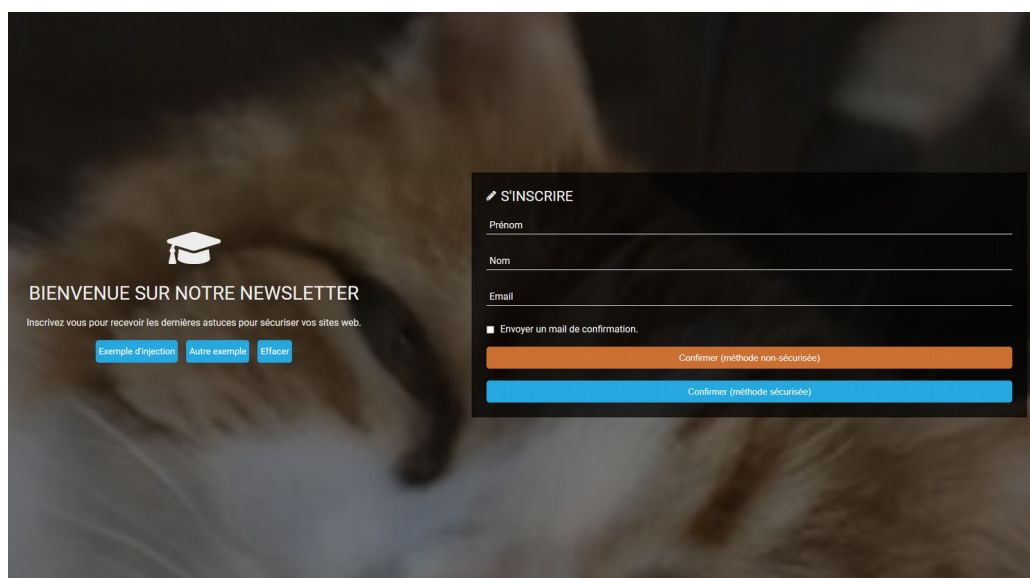


Compte-Rendu Simulateur d'injections SQL

La page du simulateur est représentée ci-dessous :

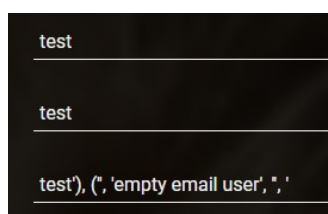


Le site simule une inscription à une newsletter.

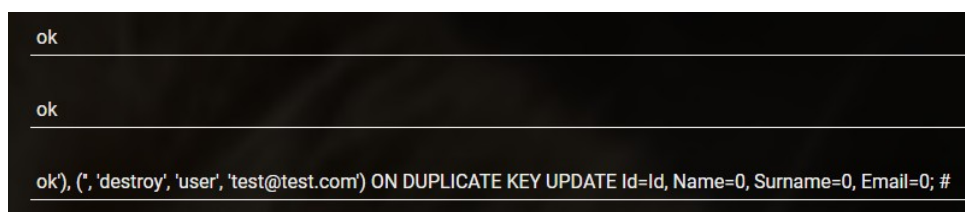
Il enregistre un utilisateur avec son nom, prénom et adresse e-mail dans la table subscribers de la base de donnée appelée secunews.

Le bouton orange traite les données du formulaire de manière non-sécurisée.

Avec les boutons de gauches, on peut pré-écrire les deux injections suivantes :



Cette requête crée un utilisateur à l'Email vide, ce qui est un jeu de données potentiellement illégal et pouvant provoquer des dysfonctionnement.



celle-ci va neutraliser les information de l'utilisateur ayant l'adresse choisie (ici "test@test.com") si il existe.

Le bouton d'envoi sécurisé utilise les requêtes pré-écrites et y insère les entrées utilisateurs en toute sécurités.