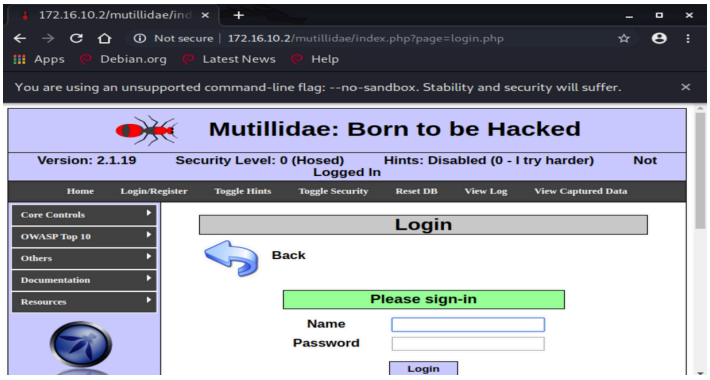
Injection SQL et codage sécurisé

DOCUMENT CREATED
BY ERICSSON

CYBERSÉCURITÉ

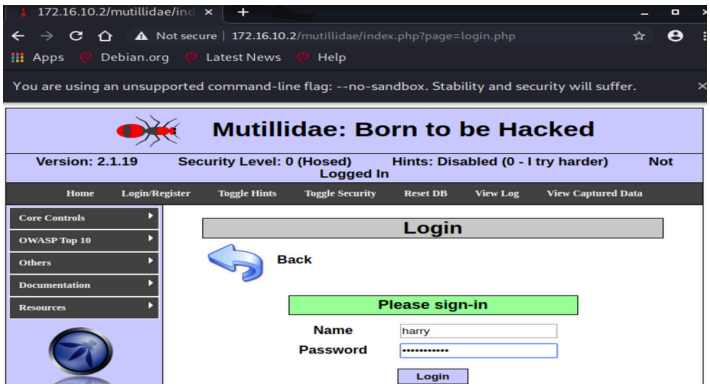
Étape 1 : Accéder à Mutillidae

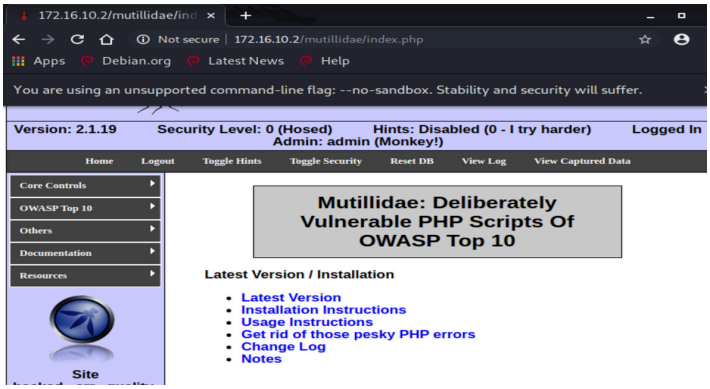


Ouvre un navigateur sur Kali et entre l'URL suivante :

http://<IP_de_Metasploitable>/mutillidae

Étape 2 : Réaliser une injection SQL





Naviguer vers la page de connexion :

- Clique sur **Login/Register**

Renseigne les champs comme suit :

Login : harry

Mot de passe : ' OR 'a'='a

Étape 3 : Analyser la vulnérabilité

Pourquoi cette injection fonctionne-t-elle ?

Le code backend ne filtre pas correctement les entrées utilisateur, ce qui permet d'injecter du code SQL dans la requête.

Quels sont les risques associés ?

Accès non autorisé, fuite de données, modification ou suppression des données.