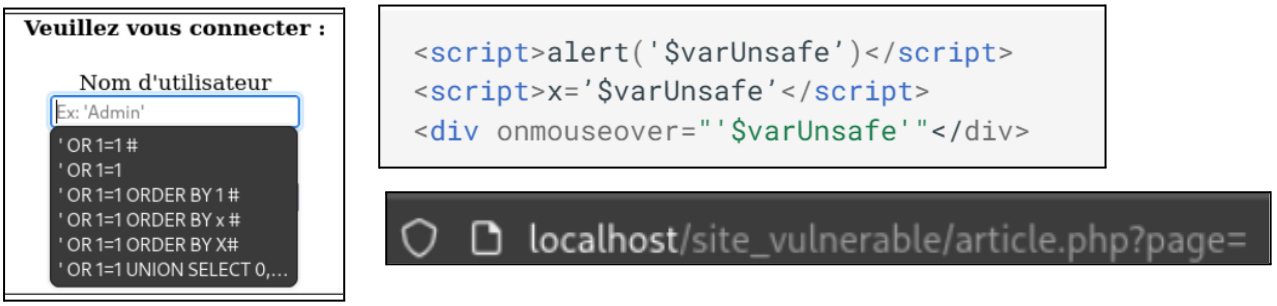
Sécurité Web

Introduction:

Dans le cadre de notre formation de Cybersécurité, une série de travaux dirigés ont été réalisés avec l'aide du code source d'un site fictif d'entraînement, "*Vulné Web*". Ce site simule un site web non sécurisé pour illustrer les vulnérabilités les plus communes des ressources web.

Objectif.s:

Il s'agit d'intenter plusieurs types d'attaques (évidemment fictives) contre le site *Vulné Web* (hors ligne). Celles-ci dépendent de vecteurs et de caractéristiques de vraisemblance et de gravité d'attaque variés selon les critères d'analyse EBIOS. Les menaces explorées incluent: l'injection SQL et XSS, l'attaque CSRF, et l'intrusion LFI.



**(De gauche à droite/haut en bas): Page de connexion Vulné Web; Exemple type d'une attaque XSS; URL du site utilisé dans une intrusion LFI*

Résultats:

Des failles du site ont été mises en exergue: vulnérabilité aux attaques de types injection par entrée utilisateur (SQL, XSS), accès au système de fichiers non sécurisé (LFI) et absence d'authentification des requêtes (CSRF).

Des mesures protectrices ont donc été appliquées: les entrées utilisateurs sont systématiquement filtrées lors de leur traitement (insertion dans la base de données et affichage sur le site), un token d'authentification est initialisé, une clause conditionnelle de validation de la session est intégrée.