Objectifs pédagogiques :

L’objectif de ce TP est de découvrir certains aspect de la cybersécurité.

Objectifs du TP :

* Gestion des zones

Applicatifs non sécurisés

Installer Wireshark sur votre poste

Prendre un client FTP et se connecter au serveur FTP, vérifier que vous bien les accès.

Construire un client en python qui se connecte au serveur, demande la liste des fichiers et clos la session.

Avec WireShark, retrouver le nom d’utilisateur et le mot de passe.

Connexion par champs

Une page web de test est disponible ici : <http://wooood.fr/manager_post.php>

Le codeur a fait des choix plutôt bizarre… Inspecter la page pour découvrir quelques surprises.

Quel est le nom qui doit être saisi pour pouvoir se connecter ?

Comment est réaliser la vérification de mot de passe ?

Modifier/forger une requête pour vous connecter.

Quels sont les erreurs à ne pas faire lors de la création d’une page de connexion ?

Injection SQL

Le codeur Jean CodeAvecMesPieds à déployé un petit serveur web.

Vous êtes employé pour vérifier la sécurité de l’accès. La page est disponible ici <http://wooood.fr/manager.php>

Essayé de vous connecter. Jean a été sympa avec vous, il oublié de commenter les lignes de debug.

Avant de commencer, un peu de lecture : <https://www.w3schools.com/sql/sql_injection.asp>

A vous de trouver le mot de passe qui permet de se connecter !

Comment éviter ce genre de problème ?

Quelques leçons pour voir d’autres vulnérabilités classiques :

https://www.hacksplaining.com/lessons