Audit de code

Analyse de code HTML et PHP pour la recherche de vulnérabilités web

1 Objectif du TP

Ce TP à pour objectif de vous montrer le travail d'auditeur en boite blanche. Autrement dit, le but est de trouver les failles de sécurité dans une application web en analysant le code source html et php et de comprendre comment les corriger. Votre rôle est nommé **white hat**.

2 Réalisation du TP

Vous avez à votre disposition une machine (VirtualBox) sur laquelle est installée Trisquel (GNU/Linux basé sur Ubuntu). Tout les logiciels nécessaires (MySql, Apache2 et PHP) au TP sont déjà installés. Le code source de l'application se trouve dans le répertoire **public_html** dans **/home/introsecu/**. NE REPRODUISEZ PAS SE QUE VOUS APPRENEZ ICI SUR DES SITES WEB NE VOUS APPARTENANT PAS. Vous devrez rechercher tous types de failles (Injection SQL, XSS, …) dans le code source. Ensuite, vous pouvez, seulement pour confirmer le résultat, tester l'attaque en allant sur le site web à l'aide d'un navigateur internet. Le site web se trouve à l'adresse :

localhost/~introsecu/index.php

3 Questions :

Question : Expliquez où se trouve les failles de sécurité, comment les attaques fonctionnent et comment corriger ces vulnérabilités. Vous pouvez utiliser le code source pour les explications.