Hébergement & Cybersécurité

TP 1

IUT de Lannion - BUT3 MMI

1 Rendu

Cette section décrit très succinctement le contenu attendu du rapport de projet. Cette section constitue une base de travail et ne se substitue pas aux consignes données en cours par votre enseignant.

Ce TP devra faire l'objet d'un rendu sous la forme d'un compte-rendu détaillé et rédigé. Le fichier contenant votre rapport devra donc obligatoirement être au format PDF. Le fichier sera nommé comme suit : « **CyberSecu_nom1_nom2.pdf** ». Malgré la présence de vos noms dans le nom du fichier, il est nécessaire de les inclure aussi dans la première page du rapport ! Il est possible de compléter le rapport avec du code source rassemblé dans une archive et déposé aussi sur moodle.

La date de rendu est fixée au **Samedi 26 Octobre 2024** à 23h55.

2 Le plus mauvais site du monde

Dans cette partie, nous allons étudier un site Internet jouet particulièrement mal codé. Installez et lancez un Apache sur votre machine et déployez les fichiers du site web dans le répertoire racine défini par Apache.

2.1 Infiltration

Mettez-vous dans la peau d'un attaquant disposant du code source du fichier index.php mais n'ayant pas connaissance du contenu mdp.txt et n'ayant évidemment pas accès aux fichiers sur le serveur. En observant le code de index.php, proposez 2 attaques par injection de code pour :

- Vous authentifier sans login ni mot de passe valides
- Récupérer la liste des utilisateurs et mots de passe (nécessite un peu de recherche sur les commandes Unix, notamment || pour enchaine des instructions)

Ensuite :

- Que constatez-vous sur la limite HTML du champ mdp ?

- Le passage des paramètres en POST serait-il plus sécurisé, jusqu'à quel point ?
- En ajoutant "légitimement" un utilisateur "spécial" dans le site, faites que si un utilisateur cherche son amie "alice", il soit automatiquement redirigé vers un site pirate (univ-rennes1.fr).

2.2 Protection

Dans cette section, nous aborderons le problème du stockage des mots de passe.

- Protégez les mots de passe en les hachant lorsqu'ils sont insérés dans le fichier utilisateur
- Faites un programme pour retrouver un mot de passe valide par force brute
- Comment éviter de recalculer toutes les combinaisons pour chaque nouveau hash
- Utilisez les fonctions de protection de mots de passe de PhP (password_hash(), password_verify()) pour hasher le mot de passe.
- Quelles sont les différences par rapport à l'utilisation uniquement de md5 ?
- Pouvez-vous encore attaquer simplement le mot passe par force brute ?
- Pouvez-vous encore utiliser une table arc-en-ciel ?

3 Aller plus loin avec HTTPS

La sécurisation du canal de communication est un problème très complexe qui nécessite des outils adaptés dans le cas de transport de données sensibles. C'est ce que propose en particulier la sous-couche SSL/TLS.

- Mettez en place un micro site internet (un simple site qui dit "bonjour" suffira) avec un serveur apache2 ou nodejs (au choix).
- A quoi sert le protocole SSL ? Comment fonctionne t'il ?
- Sécurisez votre site pour changer le protocole de HTTP à HTTPS