SLH 2024-2025

Lab 1

1. CSRF Simple

La cible sera le service (**accessible uniquement depuis le réseau de l'école, ou le VPN**) à l'adresse suivante: http://basic.csrf.slh.cyfr.ch

Votre nom d'utilisateur est la première partie de votre addresse email de l'école: `prenom.nom@heig-vd.ch` → `prenom.nom`. Le mot de passe par défaut est `1234`. N'oubliez pas de changer votre mot de passe.

Votre objectif est de vous connecter à un compte administrateur (chaque participant dispose de son propre compte admin: `prenom.nom_admin`).

1. Quelle fonctionnalité du site, potentiellement vulnérable à une faille **CSRF**, pourriez-vous exploiter pour voler le compte administrateur ?
2. Proposez une requête qui vous permettra de prendre le contrôle du compte admin, si elle était exécutée par l'administrateur
3. Ecrivez une payload javascript qui exécute la requête.
4. Quelle fonctionnalité du site, potentiellement vulnérable à une faille **Stored XSS**, pourriez-vous exploiter pour faire exécuter votre payload

par l'administrateur ?

1. Quel est le flag ? Comment avez-vous pu l'obtenir ?
2. Comment corrigeriez-vous la vulnérabilité ?

2. CSRF Avancée

Le scénario est identique au précédent, avec la cible suivante: http://advanced.csrf.slh.cyfr.ch

1. Qu'est-ce qu'un jeton anti-CSRF, comment fonctionne-t-il ?
2. Comment déterminer si le formulaire est protégé par un jeton anti-CSRF ?
3. Le site est également vulnérable à une attaque XSS. Quel est le flag du challenge ? Décrivez l'attaque.
4. Comment corrigeriez-vous la vulnérabilité ?

3. Injection SQL

La cible sera http://sql.slh.cyfr.ch

1. Quelle partie du service est vulnérable à une injection SQL ?
2. Le serveur implémente une forme insuffisante de validation des entrées. Expliquer pourquoi c'est insuffisant.
3. Quel est le flag ? Comment avez-vous procédé pour l'obtenir ?
4. Quel est le DBMS utilisé ? Auriez-vous procédé différement si le DBMS avait été MySQL ou MariaDB ?