Laboratoire : XSS

420-523-RK || Piratage et sécurité informatique || Automne 2020 || Jérôme Blier

Ce laboratoire contient 5 questions pour un total de 15 points.

Objectifs :

- Réaliser des injections HTML et JavaScript
- Protéger une application du XSS

Récupérez l'application Web fournie par l'enseignant et ouvrez la page index.html. Écrivez vos réponses en commentaire dans le code. **Les injections HTML et Javascript doivent être réussies sans modifier le code source fourni.**

1. (3 points) Dans le champ permettant d'ajouter un texte au forum, tentez de faire apparaître l'image xss.jpg fournie en injectant du HTML. Écrivez le code injecté.
2. (3 points) Dans le champ permettant d'ajouter un texte au forum, tentez de faire afficher la valeur du cookie en injectant du JavaScript. Écrivez le code injecté en spécifiant le nom du navigateur sur lequel ça a fonctionné.
3. (3 points) Dans certains cas, l'instruction Javascript **document.cookie = "username=votreIdentifiantPersonnelConfidentiel";** semble ne pas fonctionner (sur certains navigateurs). D'après-vous, pourquoi en est-il ainsi ?
4. (3 points) Dans le champ permettant d'ajouter un texte, tentez d'effacer les textes contenus dans le forum en injectant du JavaScript. Écrivez le code injecté.
5. (3 points) En appliquant les bonnes pratiques de programmation, protéger l'application du XSS (injections HTML et Javascript). Vous n'avez pas à changer drastiquement le code, apportez des correctifs simples.

Remise : dossier à votre nom incluant le projet corrigé avec vos réponses en commentaire.