

Semaine 6: Vulnérabilités web, injection XSS

IPL I317B Sécurité : labo

Olivier Choquet & Thibault Vanwersch

25 octobre 2022

Objectif

Après les injections SQL, il est temps de passer à un autre type d'injection : les injections XSS. Pour ces exercices, nous vous recommandons d'utiliser le navigateur Firefox plutôt que Chrome, ce dernier dispose de certaines contre-mesures qui peuvent perturber les exercices.

Questions

Exercice 1 :

- a) Pour ce premier exercice, le but est de procéder à une injection xss trivial sur une variante le site suivant permettant de chercher les éléments du tableau périodique des éléments : <https://labosecuip.lalwaysdata.net/22/s06/ex1/>
Votre injection doit afficher une alerte affichant le texte : "I hacked you"
 - ◆ Quelle valeur avez-vous entrée et où l'avez vous entrée ?
- b) Pouvez-vous également récolter les cookies du site de l'exercice 1a avec votre injection xss ?
- c) Pouvez-vous essayer les mêmes injections sur le formulaire suivant : <https://labosecuip.lalwaysdata.net/22/s06/ex1c/> ?
- d) Pouvez-vous essayer les mêmes injections sur le formulaire suivant : <https://labosecuip.lalwaysdata.net/22/s06/ex1d/> ?
- e) Pouvez-vous essayer les mêmes injections sur le formulaire suivant : <https://labosecuip.lalwaysdata.net/22/s06/ex1e/> ?

Exercice 2 :

- a) Pour ce second exercice, vous allez utiliser le site, nous vous invitons à utiliser le service <https://requestbin.net/> pour "exfiltrer" les cookies que vous avez récupéré lors du premier exercice : <https://labosecuip.alwaysdata.net/22/s06/ex1/>
- b) Pour ce second exercice, vous allez utiliser le site suivant sur lequel vous pouvez créer un compte : <https://labosecuip.alwaysdata.net/21/s07/ex2b/>
 - ◆ Votre objectif est de récupérer les cookies de l'administrateur.
- c) Maintenant que vous avez volé les cookies de l'administrateur, parvenez-vous à récupérer son secret ? Si oui, comment ?
(oui, c'est faisable. Spoiler: toujours plus d'ajax ;-))