Semaine 7: Vulnérabilitées web, injection XSS
IPL I317B Sécurité : labo

Olivier Choquet & Thibault Vanwersch

3 novembre 2025

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://labo.poney.pink/v01/xss/ex1a/
Votre injection doit afficher une alerte[1] affichant le texte : "I hacked you" :

- Quelle valeur avez-vous entrée et où l'avez vous entrée ?

b) Pouvez-vous procéder à la même injection sur la variante suivante : https://labo.poney.pink/v01/xss/ex1b/

c) Pouvez-vous également afficher les cookies du site de l'exo *1a* avec votre injection xss ?

d) Pouvez-vous essayer les mêmes injections sur le formulaire suivant : https://labo.poney.pink/v01/xss/ex1d/ ?

e) Pouvez-vous essayer les mêmes injections sur le formulaire suivant : https://labo.poney.pink/v01/xss/ex1e/ ?

f) Pouvez-vous essayer les mêmes injections sur le formulaire suivant : https://labo.poney.pink/v01/xss/ex1f/ ?

1 https://www.w3schools.com/jsref/met_win_alert.asp

Exercice 2 :

a) Pour ce second exercice, vous allez utilisez le site, nous vous invitons à utiliser le service https://httpdump.app/ pour "exfiltrer" les cookies que vous avez récupérer lors du premier exercice : https://labo.poney.pink/v01/xss/ex1a/

b) Pour ce second exercice, vous allez utilisez le site suivant sur lequel vous pouvez créer un compte : https://xss.labo.poney.pink/

   - Votre objectif est de récupérer les cookies de l'administrateur.

c) Maintenant que vous avez voler les cookies de l'administrateur, parvenez-vous à récupérer son secret ? Si oui, comment ?
(oui, c'est faisable. Spoiler: toujours plus d'ajax ;-))