

Manuel utilisateur

site-malveillant.com

Par Emilien Cosson

Sommaire

[Sommaire](#)

[Questions préliminaires](#)

[Manuel d'utilisation](#)

[Règles d'utilisation](#)

[Les injections sur liste noire](#)

Questions préliminaires

Qu'est-ce que site-malveillant.com ?

site-malveillant est un site Web permettant de tester et d'exploiter légalement la faille XSS persistante.

Qu'est-ce qu'une faille XSS persistante ?

Une faille XSS, pour « Cross-site scripting », est une faille informatique, sur les sites Web, qui consiste à détourner l'usage d'un site tel qu'il a été conçu.

Cette faille permet donc de modifier le contenu d'une page Web, de faire télécharger des fichiers sur l'ordinateur du visiteur, d'interagir avec le navigateur Web avec Javascript, de voler des informations de session et de cookie, de rediriger vers un site distant...

Le caractère « persistant » de la faille XSS consiste à ce que la modification du comportement de la page Web par l'attaquant est pérenne et affecte les autres visiteurs du site.

Quel est le but de site-malveillant.com ?

Le but est de permettre de tester l'attaque par la faille XSS à des fins préventive et pédagogique.

Manuel d'utilisation

La page principale de site-malveillant.com est composée :

- d'un entête comprenant notamment la barre d'**input*** (zone de saisie).
- d'une section signalée par un cadre noir laissée à la libre contribution* des utilisateurs.

*La contribution est soumise aux [Règles d'utilisation](#).

Le principe est le suivant : les utilisateurs postent du contenu sur la section signalée par un cadre noir par le biais de la barre d'input.

Seulement, cette zone de saisie est volontairement permissive et il est possible de changer l'apparence du texte dont sa taille, sa couleur, son orientation, son espacement... Il est même possible de publier des images, des vidéos...


Il suffit pour cela d'ajouter des balises HTML et d'y ajouter optionnellement du code CSS et Javascript.

Par exemple, la balise **h1** permettra de styliser le texte en tant que titre. De ce fait, il sera plus gros et plus gras. Entrez dans la zone de saisie :

```
<h1>J'entre un titre</h1>
```

Pour changer sa couleur, on ajoutera des propriétés CSS grâce à l'attribut HTML style :


```
<h1 style="color:red">J'entre un titre rouge</h1>
```

 **Attention** : toutes les balises, propriétés et scripts ne sont pas autorisés. Lisez attentivement les [Règles d'utilisation](#) ainsi que la liste des [injections sur liste noire](#).

Règles d'utilisation

Parce que ce site ne doit pas devenir un « nid à virus », quelques interdits ont été définis dans le code source de site-malveillant.com. Toutefois, le développement de toute application informatique est sujette aux bogues et aux failles ; et particulièrement pour site-malveillant.com qui joue le juste équilibre de la sécurité et de la permissivité.

Ainsi, avant de lancer vos requêtes XSS, assurez-vous que :

 vos modifications du contenu de la page n'affectent que la section signalée par un cadre noir prévue à cet effet et ne débordent pas au-delà ;

- ✓ vos modifications ne suppriment et ne cachent pas les contributions des autres utilisateurs ;
- ✓ vos modifications sont de taille raisonnable ;
- ✓ le contenu que vous publiez est dit « non sensible » et est adapté aux enfants.

Vous ne pouvez pas :

- ✗ faire exécuter du code JavaScript au chargement de la page par l'utilisateur ;
- ✗ faire exécuter du code JavaScript au survol d'un élément par l'utilisateur ;
- ✗ mettre en péril la sécurité ou la performance du matériel de l'utilisateur ;
- ✗ remettre en cause la disponibilité, la sécurité ou la performance du serveur Web.

site-malveillant.com se garde le droit de couper l'accès à son site à toute personne qui ne respecterait pas ses règles.

site-malveillant.com lègue toute responsabilité en cas de dégât ou de préjudice subit au cours de la navigation de l'internaute.

Il n'est pas permis de tester des failles de sécurité sur site-malveillant.com sans l'autorisation préalable de son administrateur. Le code source étant disponible sur [GitHub](#), vous êtes invité à réaliser vos essais sur votre propre infrastructure.

Les injections sur liste noire

Toute modification de contenu doit respecter les [Règles d'utilisation](#).

L'utilisation de la balise <script> est proscrite.

La propriété CSS order est bloquée.

D'autres interdits seront par la suite établis dans le [code source](#). Vous pensez à des usages problématiques ? Contribuez ou signalez-les !

⚠ Toute les attaques XSS ne sont pas permises sur site-malveillant.com ! Prenez le temps de lire les [règles d'utilisation](#).