

Cross-Site Scripting



Le principe


Injecter un script dans un site web dans le but qu'il soit exécuté côté client





Dealabs

À la une
Hot 57
Nouveaux 99+
Commentés


- 

558°


+


il y a 2 min


Stick de streaming Amazon Fire TV Stick 4K UHD



44,99€ ~~59,99€~~ -25%  Bons plans [Amazon](#)

Fire TV Stick 4K Ultra HD avec télécommande vocale Alexa nouvelle génération, Lecteur multimédia en streaming Disponible au même prix chez Boulanger Apparemment sur Amazon il es... [Afficher plus](#)


Bafien




136

Voir le deal 
- 

456°


+


il y a 33 min


Set de nettoyage complet Vileda Ultramax



16,99€ Bons plans [Aldi](#)

set de nettoyage Vileda complet Ultramax Un balai ultra-pratique à prendre en main, microfibre, avec manche télescopique Une serpillère 2en1 Un seau essoreur Idéal pour nettoyer ... [Afficher plus](#)


zora.manimani




9


Voir le deal 
- 

611°


+


il y a 1 h et 2 min


PC Portable 15.6" Lenovo Ideapad 3 15ARH05 - Full HD IPS 120 Hz, Ryzen 7 4800H, SSD 512 Go, 16 Go RAM, GTX 1650 Ti



799€ ~~1099€~~ -27%  Bons plans [Cdiscount](#)

Retour à bon prix pour ce PC que je possède personnellement et qui fait très bien le taff (y) J'arrive à faire tourner quasi tout les jeux en full HD sans problème Attention le... [Afficher plus](#)


Comoriano




37

Voir le deal 
- 

575°


+


il y a 1 h et 32 min


13 Items Steam gratuits: Autocollants, Arrière-plans de profil, Cadres de profil, Avatars (Dématérialisés)


Bons plans [Steam](#)

Il y a actuellement un total de 13 objets Steam récupérable gratuitement en regardant des Streams. Vous n'obtiendrez que des autocollants, des images de profil, des cadres de prof... [Afficher plus](#)






24

Voir le deal 

Poster un nouveau deal

[ou poster un code promo](#)

Lien du deal (Facultatif)

Veuillez donner le lien de la page où la communauté pourra obtenir des renseignements, voir le produit et profiter du deal !

Description

PRIX (Facultatif)

€

PRIX HABITUEL (Facultatif)

€

FRAIS DE PORT (Facultatif)

€

☐ Livraison gratuite

CODE PROMO (Facultatif)

TITRE

140 caractères restants

DESCRIPTION

|



Vous devez remplir ce champ !

GROUPES

DESCRIPTION

```
<script>alert('bonjour')</script>
```

B



I



DESCRIPTION

```
<script>alert('bonjour')</script>
```



À la une

Hot 57

Nouveaux 99+

Commentés

www.dealabs.com indique

bonjour

OK



- 557° +

Stick de streaming Amazon Fire TV Stick 4K UHD

44,99€ 59,99€ -25% Gratuit | Bons plans Amazon

Fire TV Stick 4K Ultra HD avec télécommande vocale Alexa nouvelle génération, Lecteur multimédia en streaming Disponible au même prix chez Boulanger Apparemment sur Amazon il es... **Afficher plus**



Bafien



136

Voir le deal



- 456° +

Set de nettoyage complet Vileda Ultramax

16,99€ | Bons plans Aldi

set de nettoyage Vileda complet Ultramax Un balai ultra-pratique à prendre en main, microfibre, avec manche télescopique Une serpillère 2en1 Un seau essoreur idéal pour nettoyer ... **Afficher plus**



zora.manimani



9

Voir le deal

il y a 33 min



- 611° +

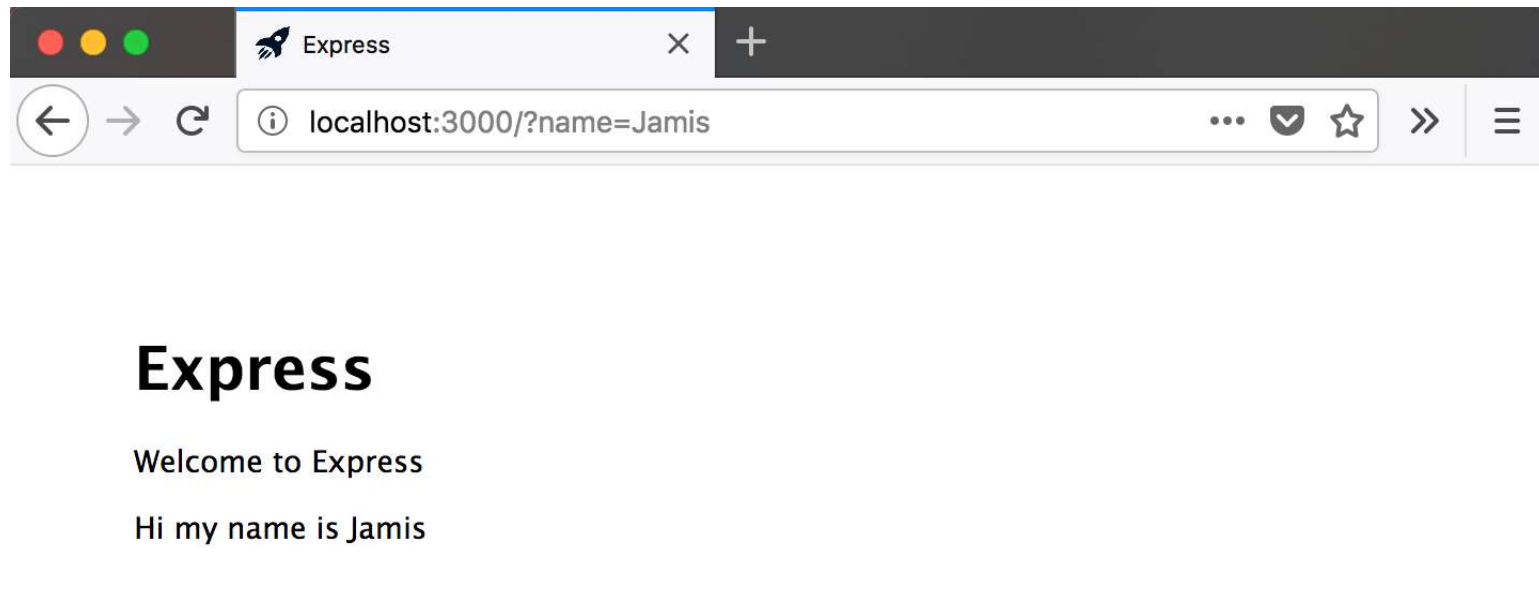
PC Portable 15.6" Lenovo Ideapad 3 15ARH05 - Full HD IPS 120 Hz, Ryzen 7 4800H, SSD 512 Go, 16 Go RAM, GTX 1650 TI

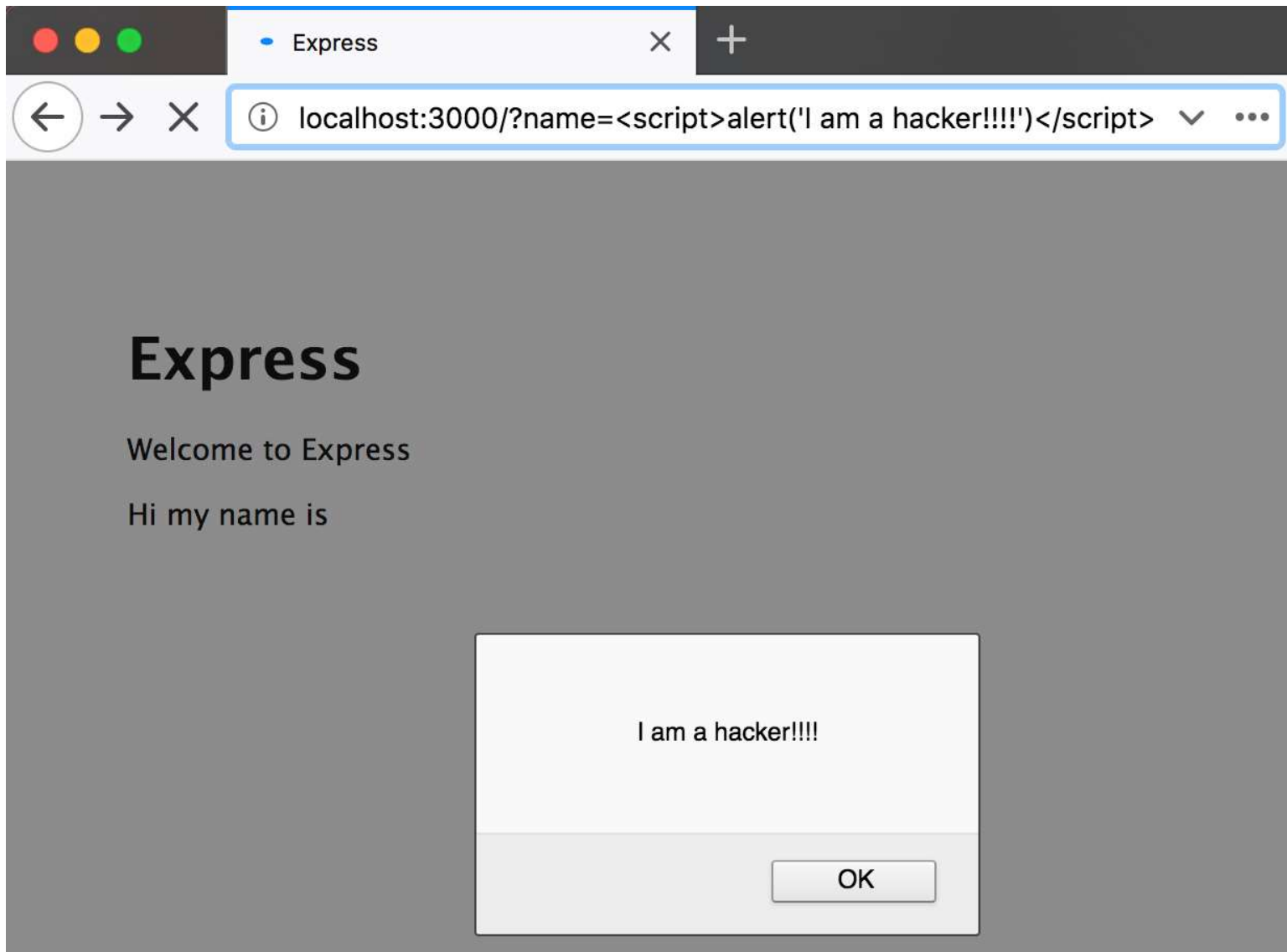
799€ 1099€ -27% Gratuit | Bons plans Cdiscount

il y a 1 h et 3 min



Top groupes





Code XSS connu

source : <https://apcpedagogie.com/les-injections-html-xss/>



dealabs home

Code XSS connu



dealabs home

Code XSS connu



dealabs home

Supprimer les balises "
<script>"

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

=> alert(document.cookie)

Supprimer les balises " <script>"

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

=> alert(document.cookie)

Il suffit d'imbriquer les balises <script>

Supprimer les balises " <script>"

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

=> alert(document.cookie)

Il suffit d'imbriquer les balises <script>

<sc<script>ript>alert(document.cookie)
</sc</script>ript>

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

Supprimer les balises "<script>" (2)

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

=> alert(document.cookie)

Supprimer les balises " <script>" (2)

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

=> alert(document.cookie)

on peut essayer avec des majuscules

Supprimer les balises "<script>" (2)

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

=> alert(document.cookie)

on peut essayer avec des majuscules

<sCript>alert(document.cookie)</sCRlpt>

=> <sCript>alert(document.cookie)</sCRlpt>

Supprimer les balises " <script>" (3)

Ne pas passer par une balise <script>

```
<img src='zzz.jpg' onerror= alert('xss') ></img>
```

Une video qui résume bien

Tout SAVOIR sur la faille XSS - La faille la plus EXPLOITÉE par les PIRATES ! [Sécurité Web]





```
<form
  action="http://example.com/account/remove"
  method="POST"
  id="form-doing-bad-things">
  <input type="hidden" name="account" value="X"/>
</form>
<script>
  document.getElementById("form-doing-bad-things").submit();
</script>
```




```
fetch(url, {  
  method: 'POST',  
  headers: {  
    'Content-Type': 'application/json'  
  },  
  body: JSON.stringify(data)  
});
```




```

```

Solutions

- Désactiver le load automatique du HTML
- Mettre des guards sur les actions sensibles de l'application

CSRF Token

CSRF Token

- Généré aléatoirement

CSRF Token

- Généré aléatoirement
- Sécurise les requêtes

ex : ?id=27&token=45421587d1s548s

CSRF Token

- Généré aléatoirement
- Sécurise les requêtes
*ex : ?id=27&**token=45421587d1s548s***
- L'attaquant ne peut donc jamais le connaître

Plus de références :

- OWASP CSRF page
- Cross Origin Request Policy from the web bible

Une video qui résume bien

Sécurité Web : Faille CSRF et image piégée



Merci pour votre attention !

Des questions ?



via GIPHY