

Cross-site scripting (XSS)

...

(ou comment gossier sur un même challenge pendant 5h de temps sans comprendre pourquoi que ça marche pas)

Objectifs

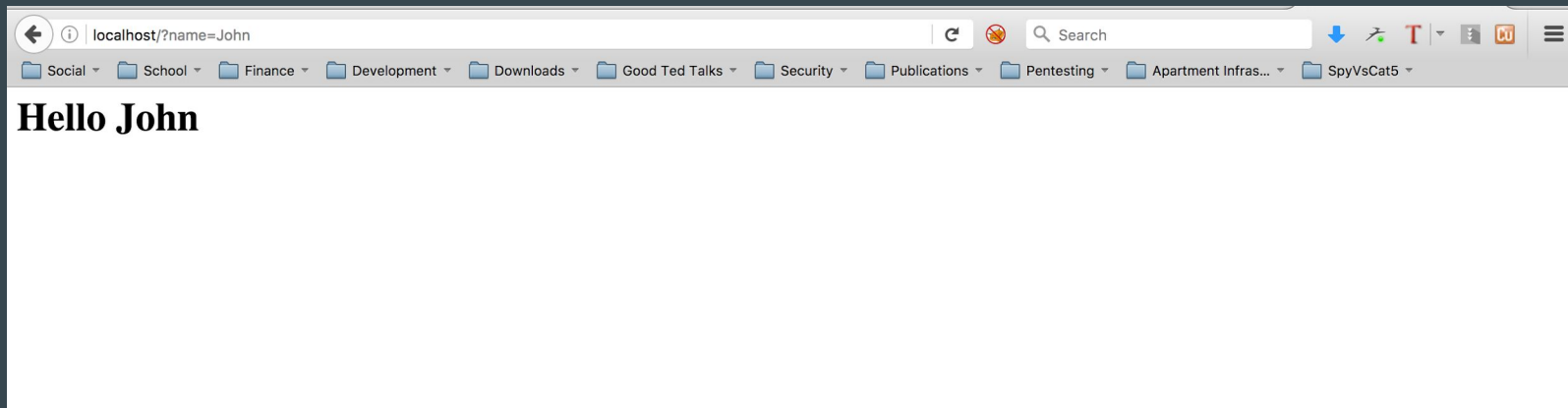
- Détecter des cas de XSS
- “Hijacker” des sessions
- Contrôler l'utilisateur comme une marionnette

* SAVOIR GOOGLER CE QUE TU NE
CONNAIS PAS *

Comment ça marche?

<http://bonjour.com/?name=John>

http://bonjour.com/?name=John



`http://bonjour.com/?name=John`

```
<html>  
  <body>  
    <h1>Hello John</h1>  
  </body>  
</html>
```

`http://bonjour.com/?
name=<script>alert(1)</script>`

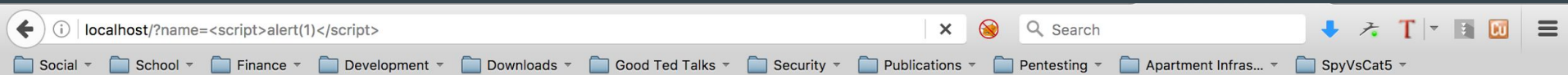
`http://bonjour.com/?name=John`

```
<html>  
  <body>  
    <h1>Hello John</h1>  
  </body>  
</html>
```

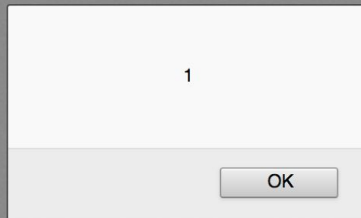

`http://bonjour.com/?name=<script>alert(1)</script>`

```
<html>
  <body>
    <h1>Hello <script>alert(1)</script></h1>
  </body>
</html>
```

http://bonjour.com/?name=<script>alert(1)</script>



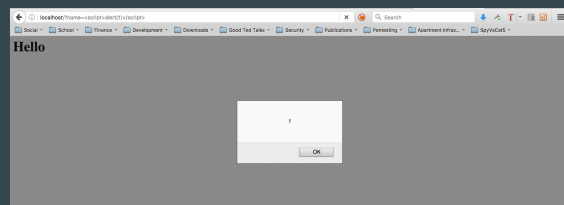
Hello



[http://bonjour.com/?name=<script>alert\(1\)</script>](http://bonjour.com/?name=<script>alert(1)</script>)



[http://bonjour.com/?name=<script>alert\(1\)</script>](http://bonjour.com/?name=<script>alert(1)</script>)



**Qu'est-ce qu'on peut faire
avec ça?**

Attaques possibles

- Modifier le contenu du site web vulnérable
- Voler les cookies de session d'un utilisateur
- Forcer l'utilisateur à effectuer des actions indésirables

Défi #1

(Modifier le contenu d'un site web vulnérable)

Outil indispensable : <http://requestb.in>

Russia and the Jester

<http://arstechnica.com/information-technology/2016/10/how-the-jester-fooled-russians-and-fox-news-with-one-simple-trick/>

**Voler les cookies de
session**



[http://bonjour.com/?name=<script>\[MON_SCRIPT\]</script>](http://bonjour.com/?name=<script>[MON_SCRIPT]</script>)





[http://bonjour.com/?name=<script>\[MON_SCRIPT\]</script>](http://bonjour.com/?name=<script>[MON_SCRIPT]</script>)



[Execute le script malicieux]



`http://bonjour.com/?name=<script>[MON_SCRIPT]</script>`



`PHPSESSID=ha89sdhfnasidf7as8dfbags`

[Execute le script malicieux]

Défi #2

(Voler un cookie de session et l'utiliser)

Google it.

<http://security.stackexchange.com/questions/49185/xss-cookie-stealing-with-out-redirecting-to-another-page>

Défi #3

(Forcer l'utilisateur à effectuer des actions indésirables)


BeEF

Current Browser

▶ Offline Browsers

Module Results History

Command results

➤  Social Engineering (6)

id	date	label
0	2013-02-07 15:23	command 1
1	2013-02-07 15:34	command 2

5 Thu Feb 07 2013 15:23:50 GMT-0500 (Eastern Standard

Re-execute command

 Ready

Ringzer0team.com time!