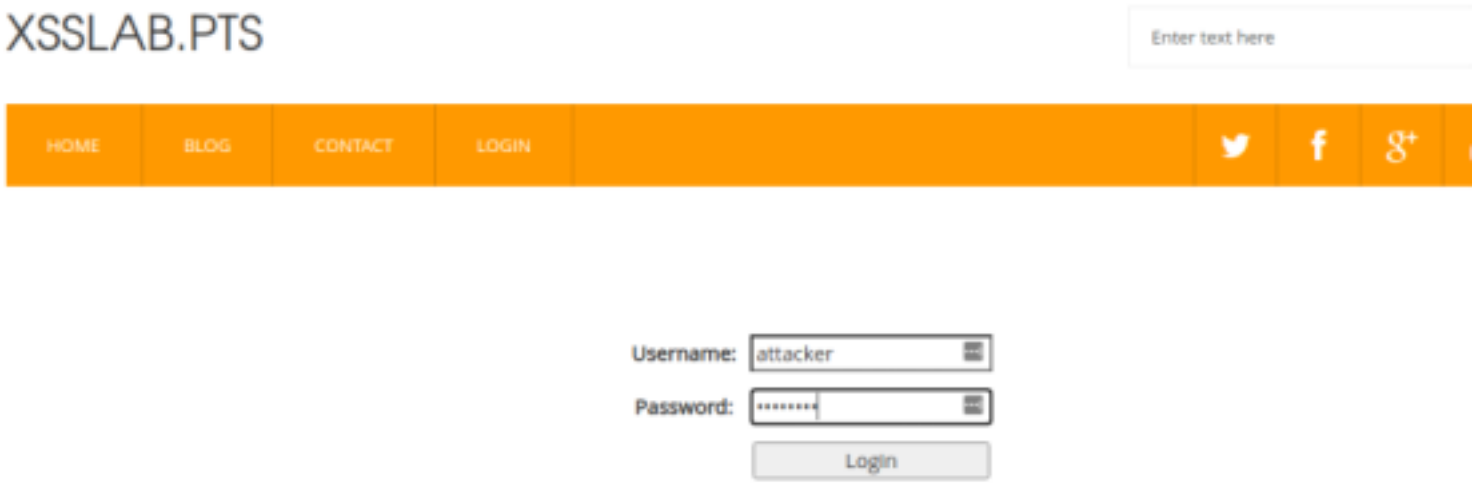
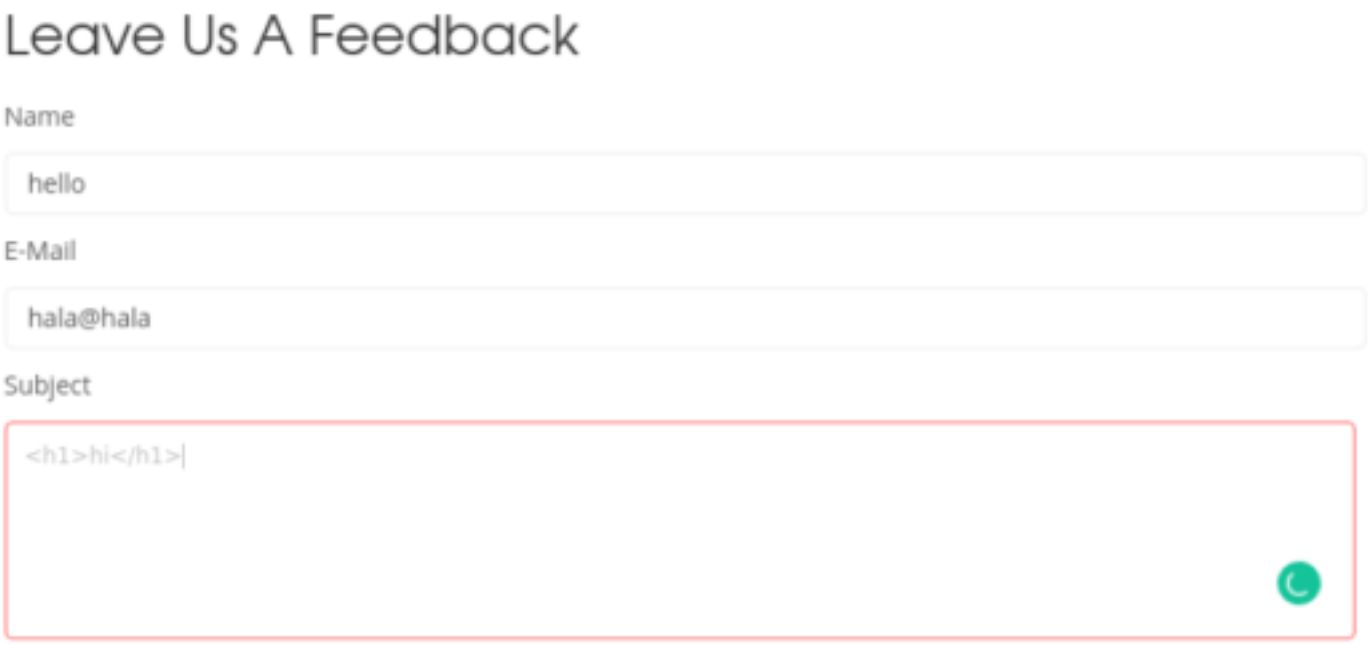
XSS

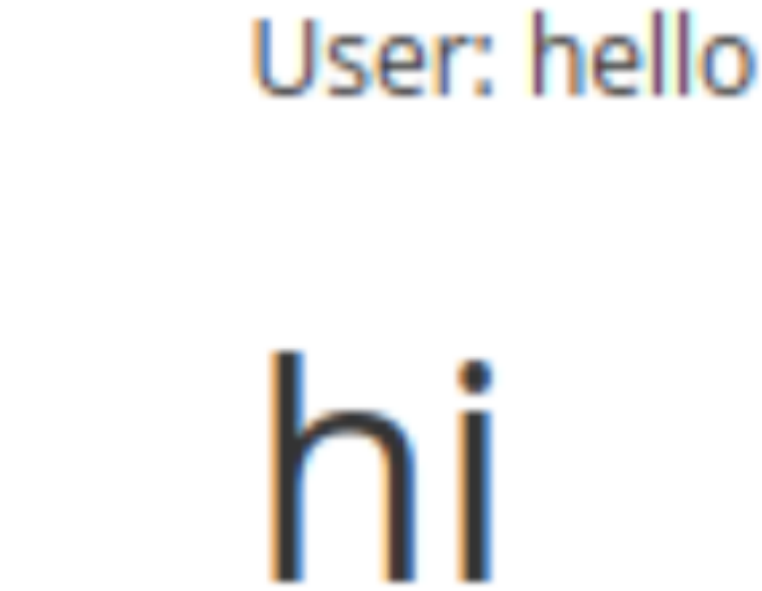
We have credentials to log in. Let's use them to login and check for vulnerable input fields.



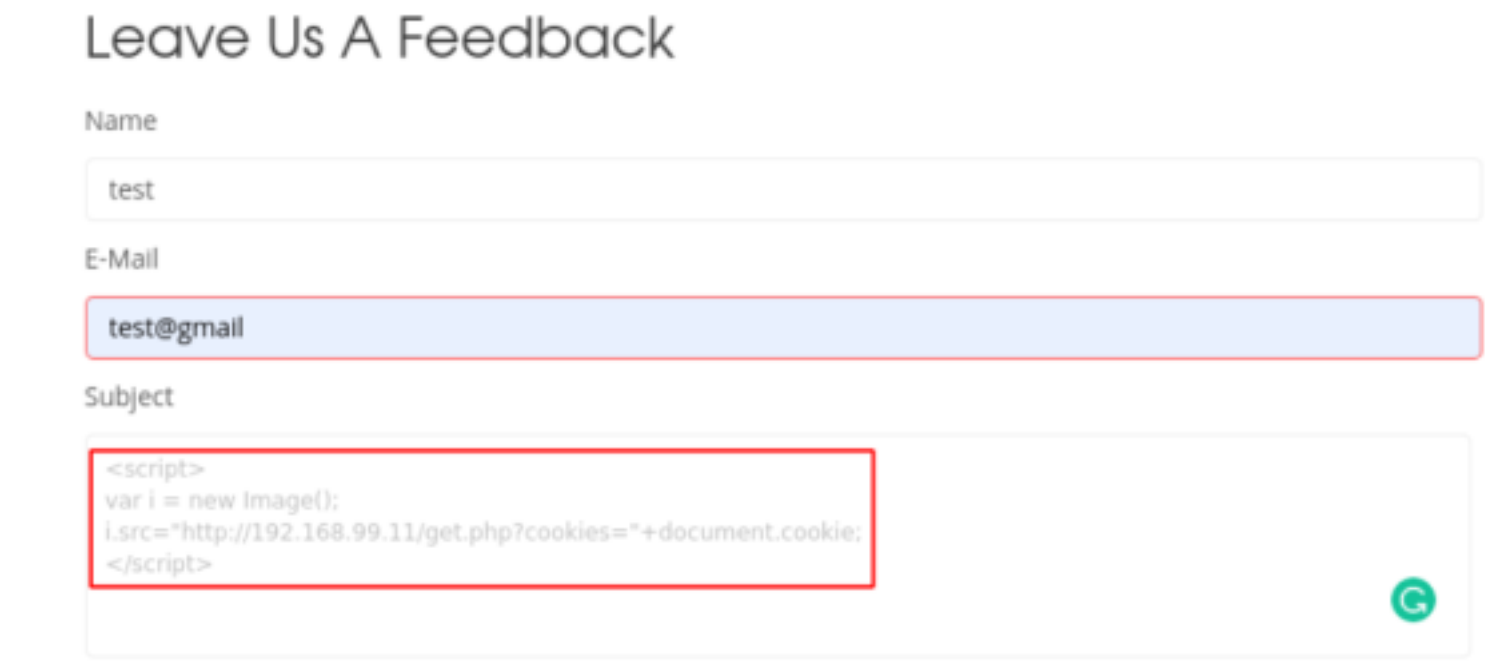
While checking, I noticed that feedback form subject field is vulnerable to stored XSS.



HTML code worked in it.

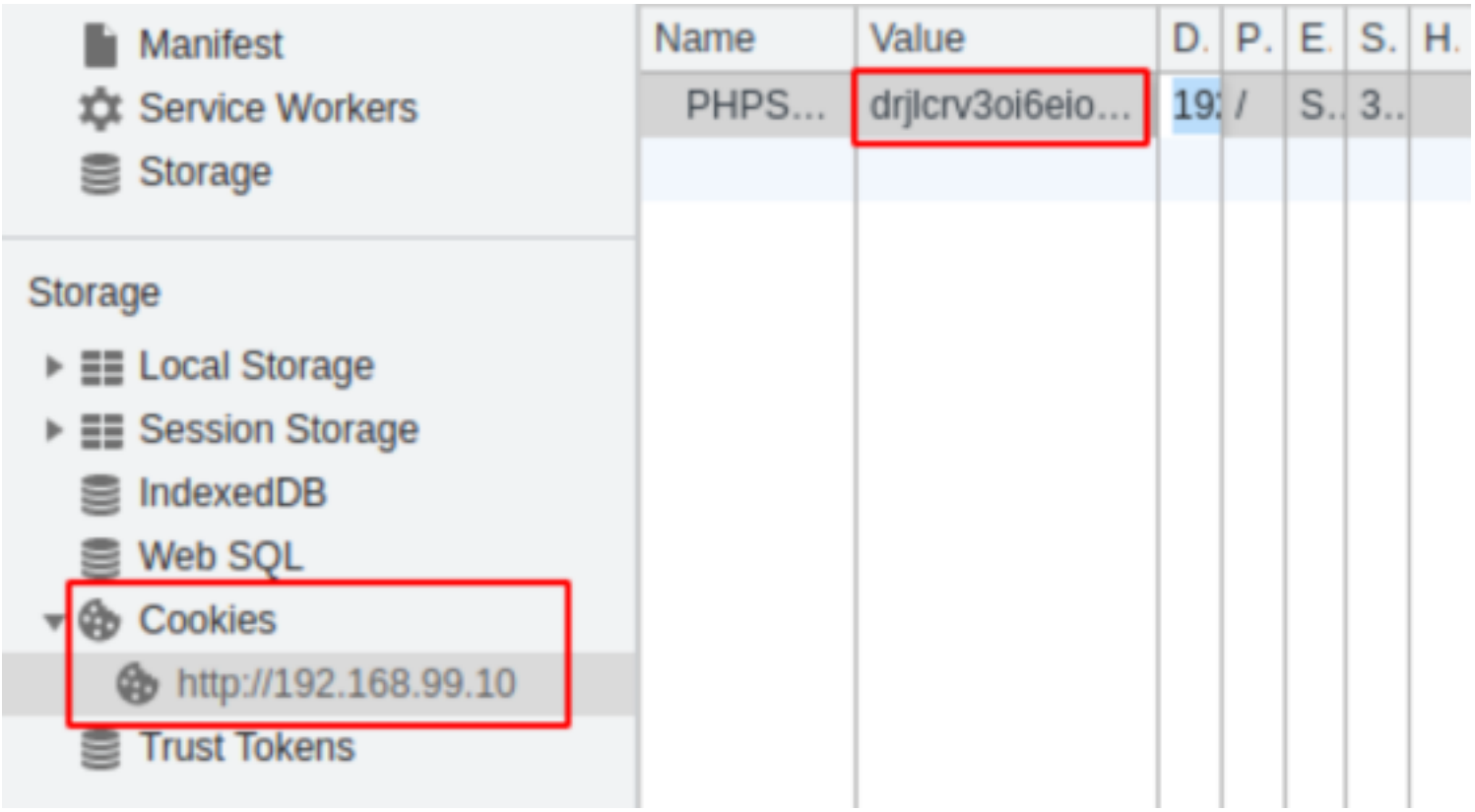


So, since the aim of the lab is to get the admin cookies and login as admin, let's insert the cookie stealing payload into the subject field.

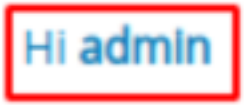


After a while, we got the admin cookies in our jar.txt file

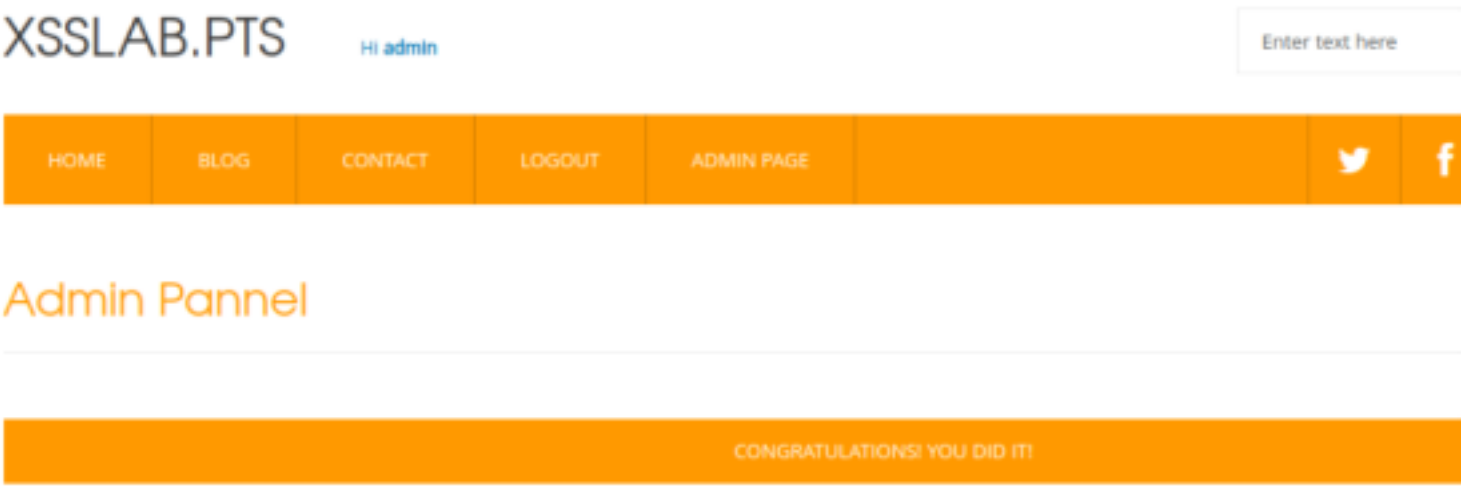
Let's replace our session cookie with this one. We can do this in the inspect window on firefox, under the storage tab.



We got the admin session while refreshing the page.



We also accessed the admin panel.


XSSLAB.PTS
Hi admin
Enter text here
HOME
BLOG
CONTACT
LOGOUT
ADMIN PAGE
Admin Pannel
CONGRATULATIONS! YOU DID IT!