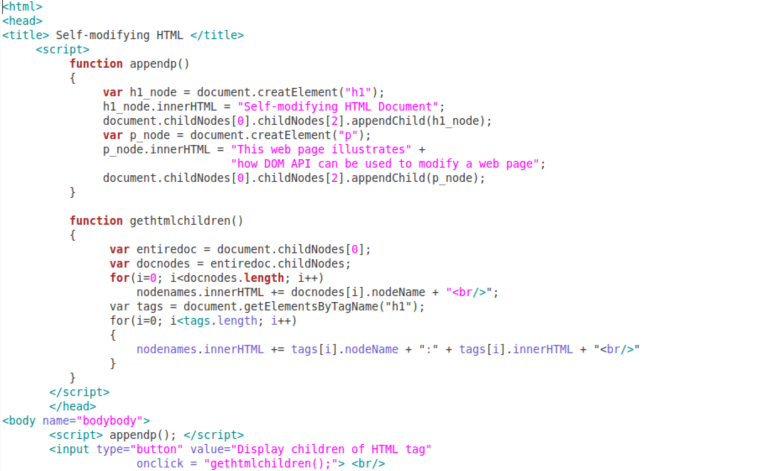
Web Same-Origin-Policy Exploration Lab

YUKUI YE

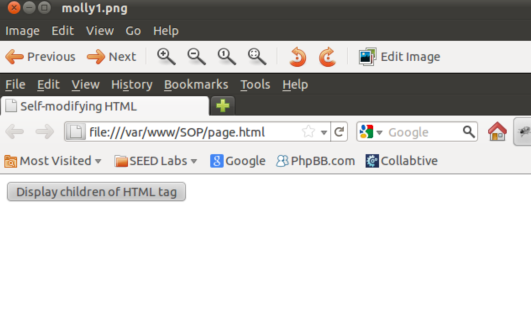
SUID: 439644268

Task1: Understanding DOM and Cookies

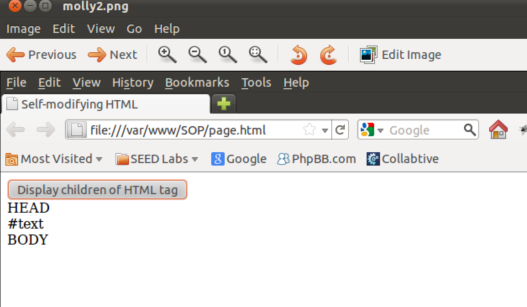
1. JavaScript



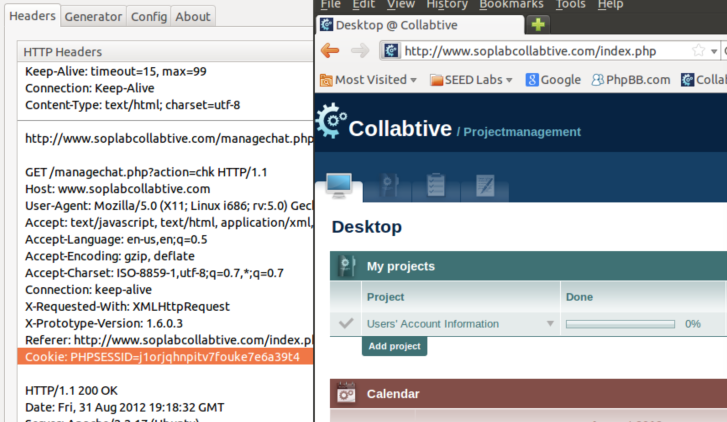
Open it with FireFox:



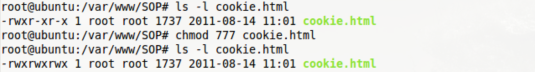
After click the buttom

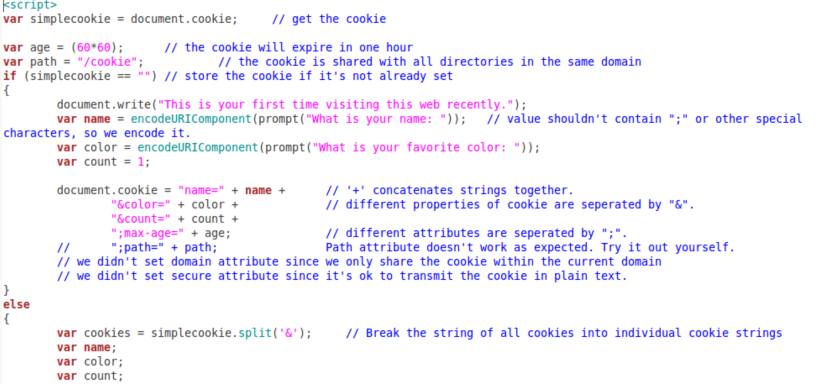


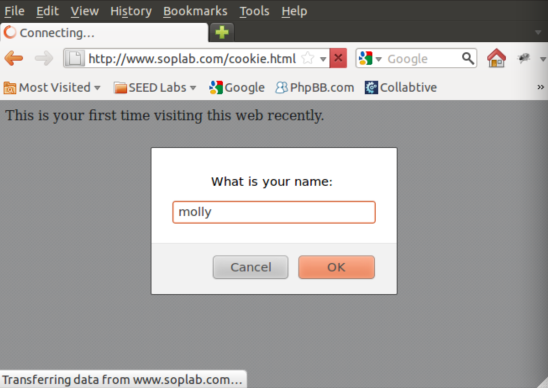
2)Find out when the web application creats the session cookie in the web browser by using LiveHTTPHeaders.

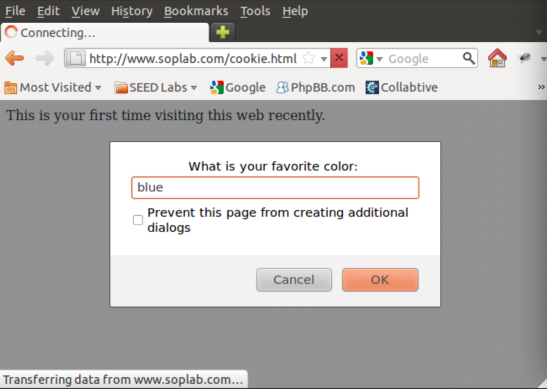


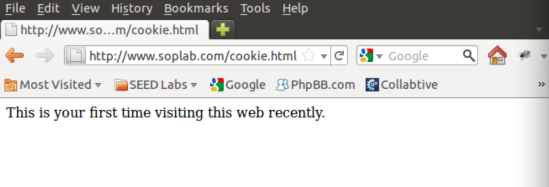
3)Write your own JavaScript in cookie.html to display the number of times that the web page has been visited by the current user.



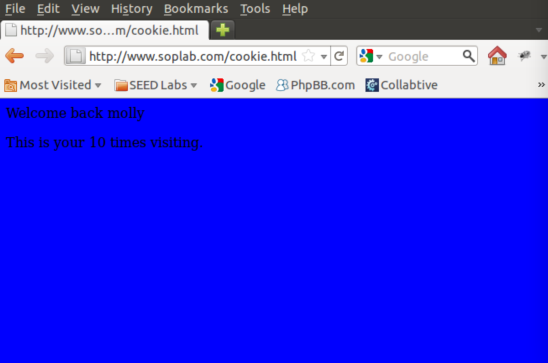




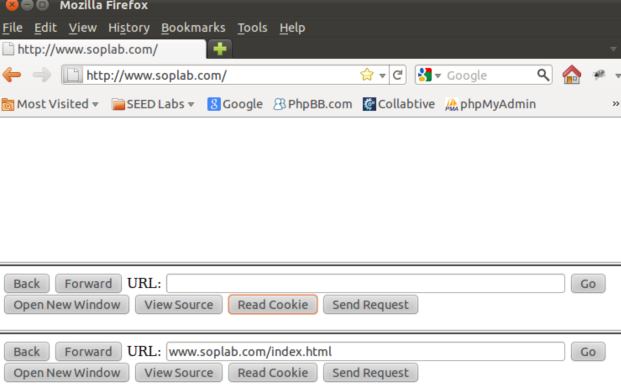


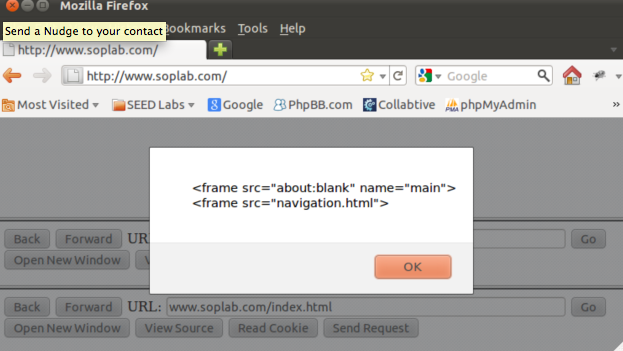


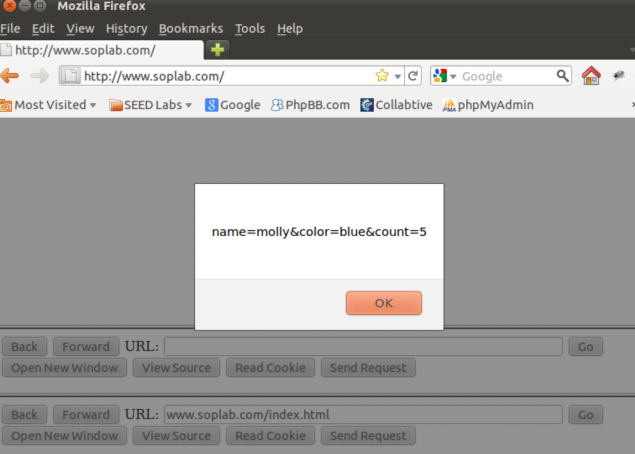
After several time reenter, it shows like below:



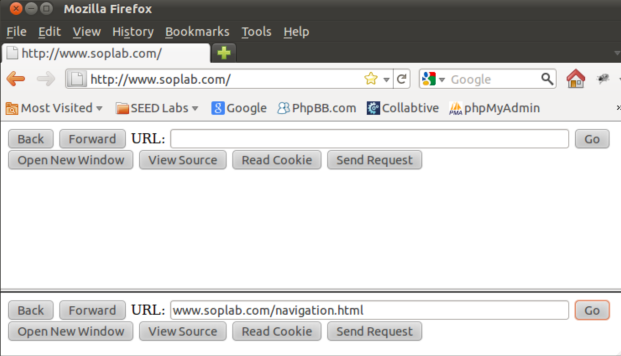
Task2:SOP for DOM and Cookies

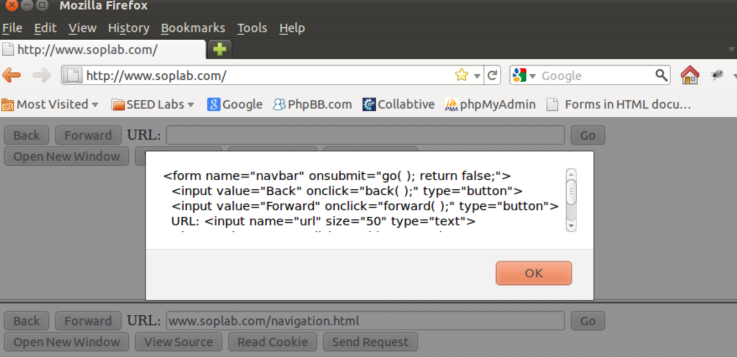
1). Successfully Accessing www.soplab.com/index.html

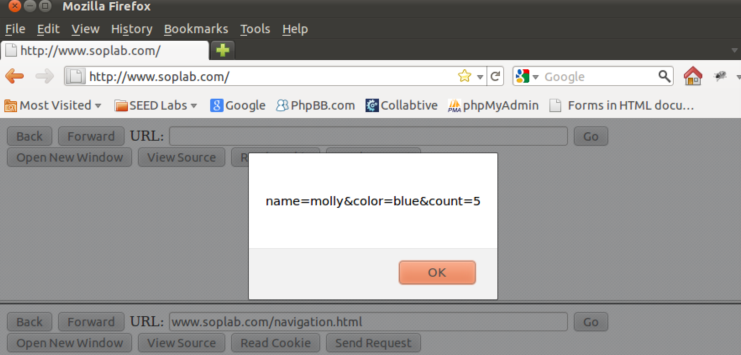




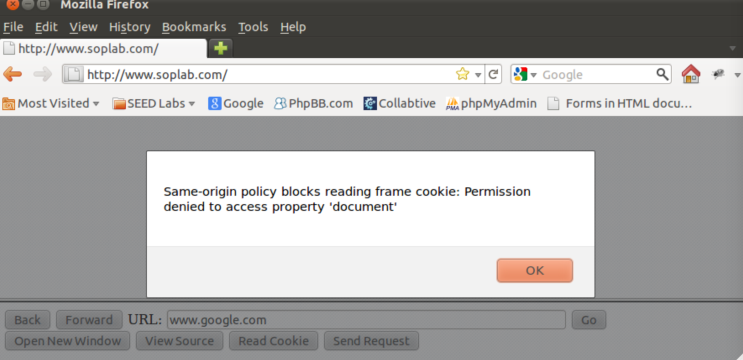
Successfully Accessed www.soplab.come/navigation.html

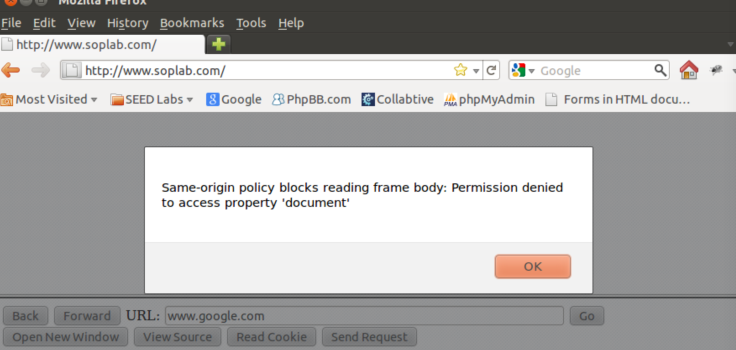




2)Cross-Domain URL

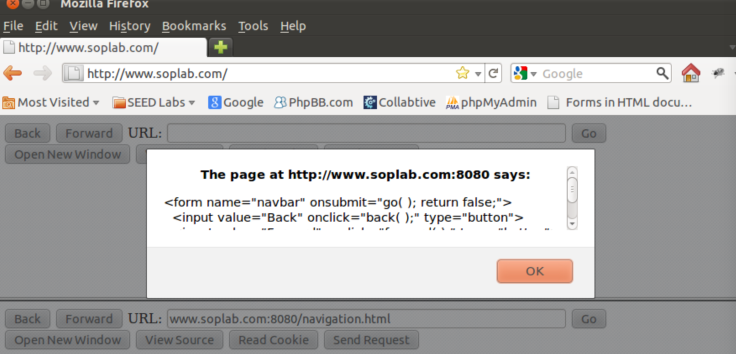
www.google.com





By trying to use some cross-domain URL such as www.google.com in the URL bar of the first web page and we can tell from the picture that we are unable to access its cookies and DOM objects.

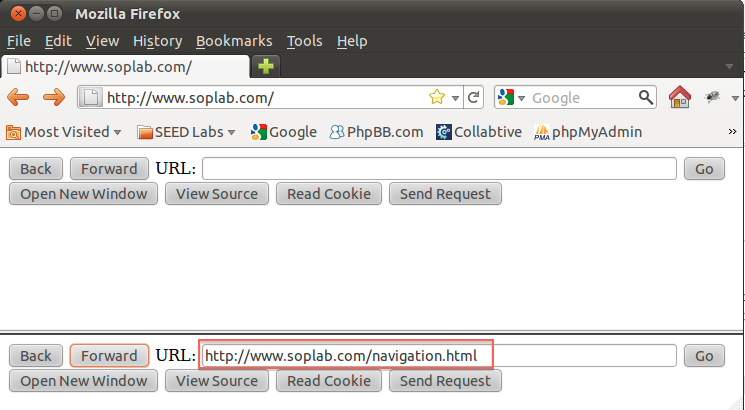
3)Change the Port: www.soplab.com:8080/navigation.html



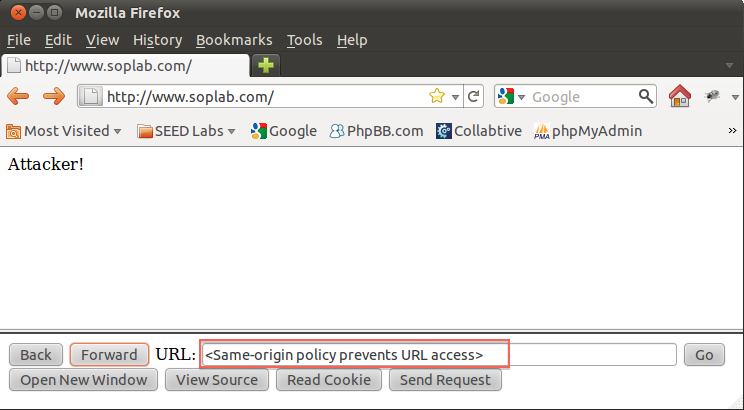


We can still successfully access its cookies and DOM objects.

4) the History object and the URL of the frame



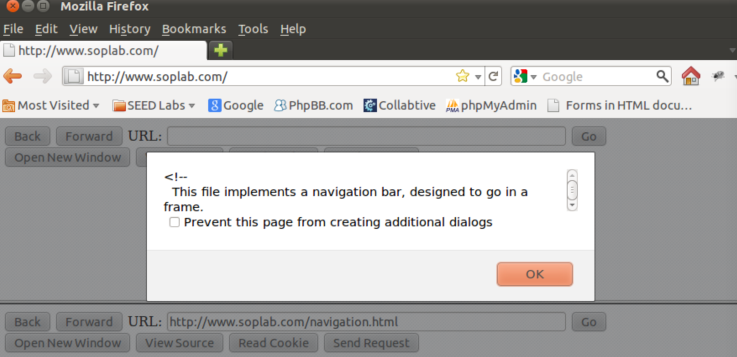
Both HISTORY and URL are accessible if page is from the same original.



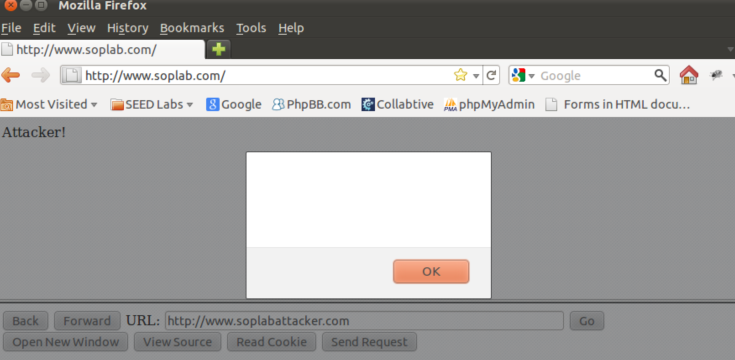
Only HISTORY is accessible if page is from different original.

Task3: SOP for XMLHttpRequest

1)Using XMLHttpRequest API



From above screenshot,we could tell that we can send XMLHttpRequest to the same original service. But for different site only returning nothing shown as below.

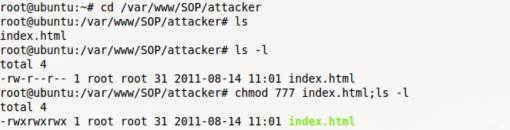


2)The dangers of not extending the SOP to the HTTP requests created by using XMLHttpRequest

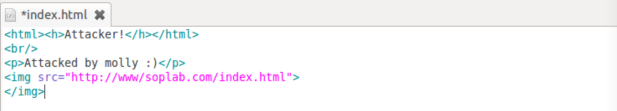
The attacker could use the requests to send request to the servicer if the SOP does not extend to XMLHttpRequest. And the web application would automatically attach session cookie, which would allow attacker to get information from good website. Besides every resource could get through XMLHttpRequest.

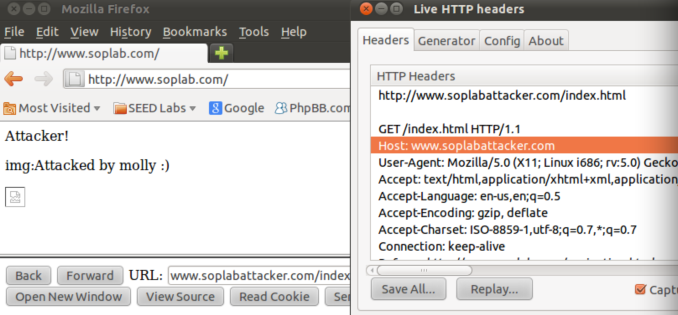
Task4: Exceptions from SOP

First change the permission of index.html to enable writable.



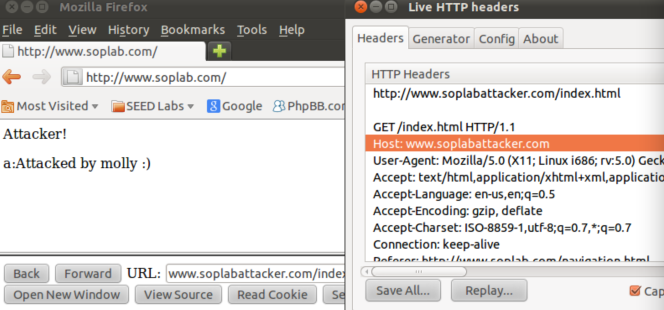
change <img>code,



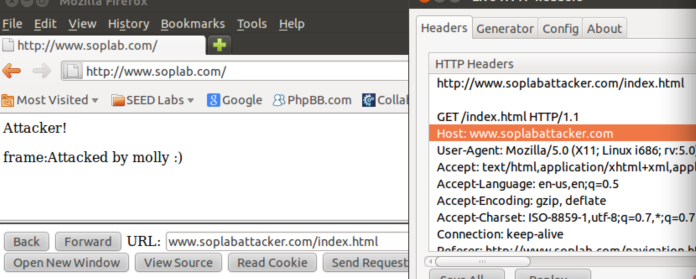


a

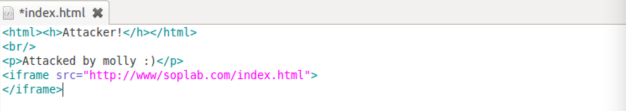


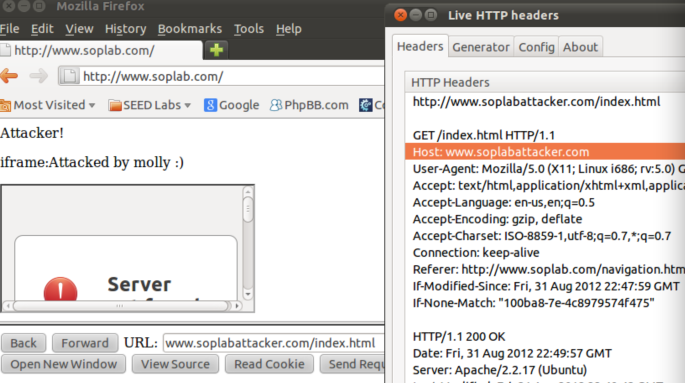


frame



iframe





we could see that the above attack all succeed.