CIS 643 Computer Security

Lab 7 Web Same-Origin-Policy Exploration Lab

**Instructor: Wenliang (Kevin) Du**

Contents

Task 1: Understanding DOM and Cookies 2

1. Figure 1 illustrates the use of some DOM API. 2

2. Find out when the application creates the session cookie in the web browser 3

3. Understand how to store, read and process the cookies. 3

Task 2: SOP for DOM and Cookies 5

1. The same origin URL 5

2. Cross-domain URL 6

3. Try different port: 7

4. History object and the URL of the frame 8

Task 3: SOP for XMLHttpRequest 9

1. Using XMLHttpRequest API 9

2. The dangers of not extending the SOP to the HTTP requests created using XMLHttpRequest 9

Task 4: Exceptions from SOP 9

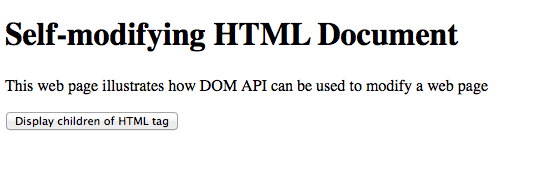
## Task 1: Understanding DOM and Cookies

### 1. Figure 1 illustrates the use of some DOM API.

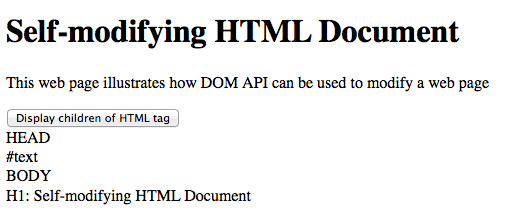
Html page.



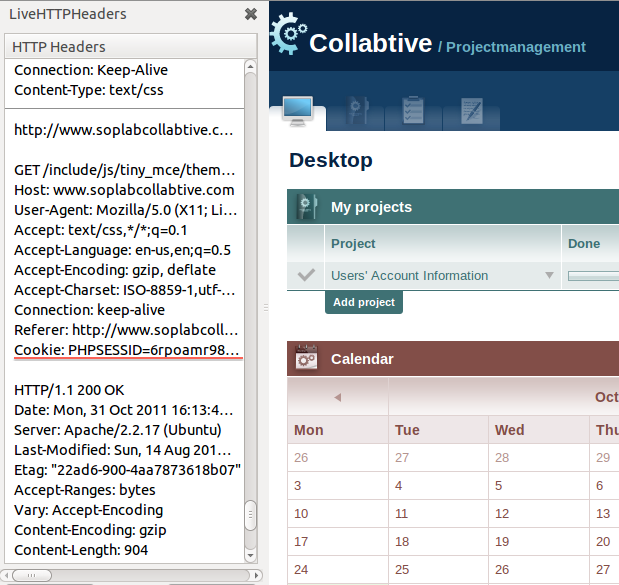
Displayed on Firefox:



After button clicked:

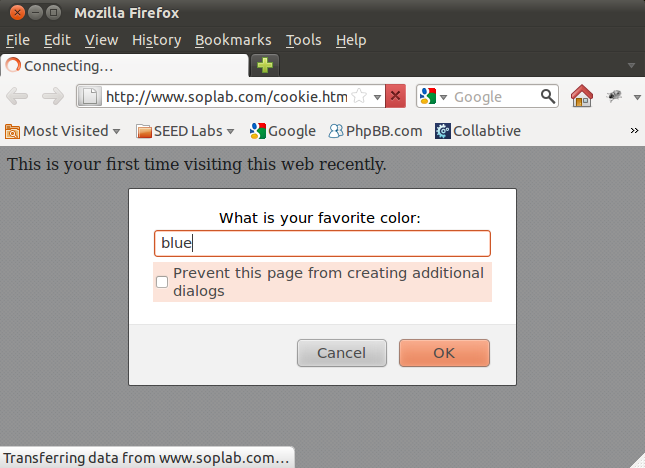


### 2. Find out when the application creates the session cookie in the web browser

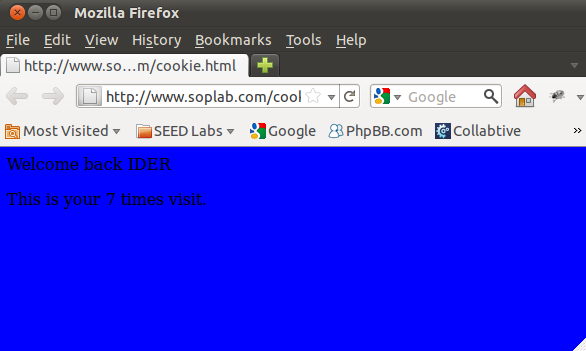


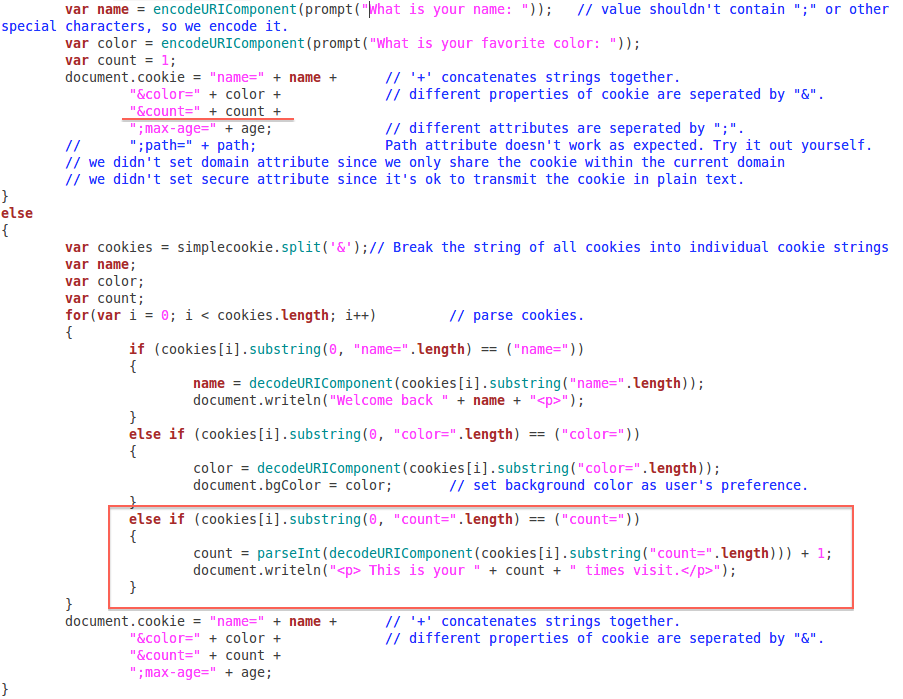
### 3. Understand how to store, read and process the cookies.



\

After several times reenter:

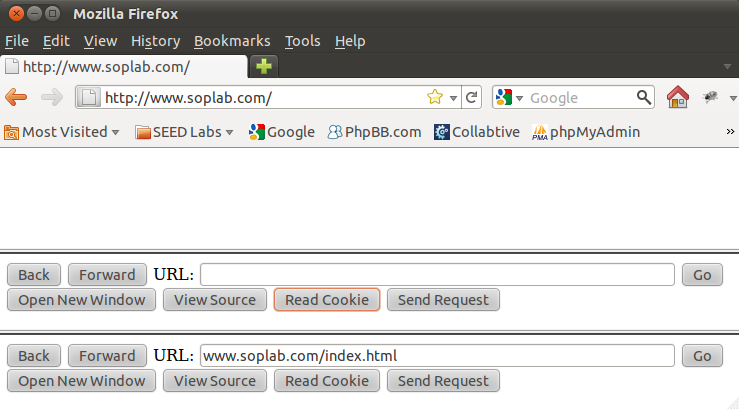




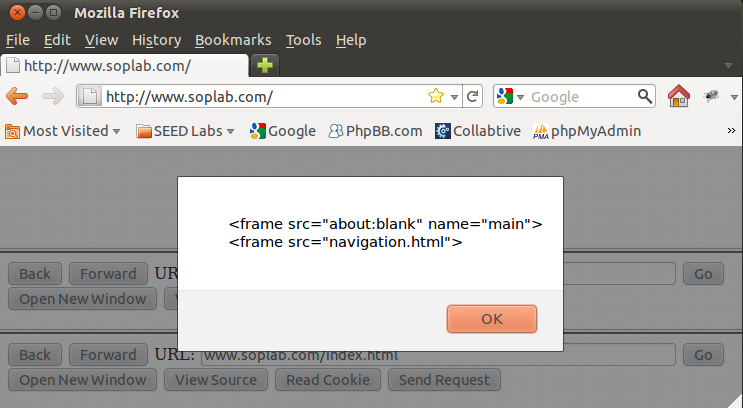
## Task 2: SOP for DOM and Cookies

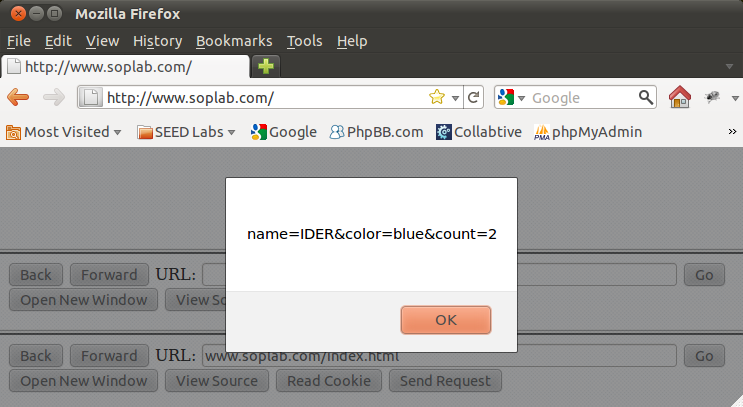
### 1. The same origin URL

a) [www.soplab.com/index.html](http://www.soplab.com/index.html)



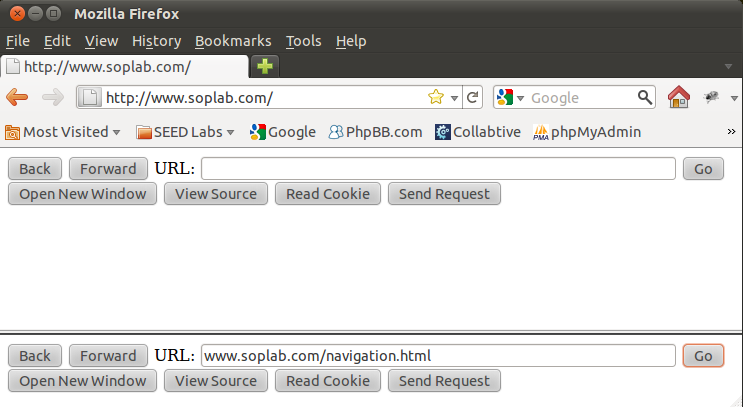
Because the pages are from the same origin, so we could get the cookies and source codes of the page:

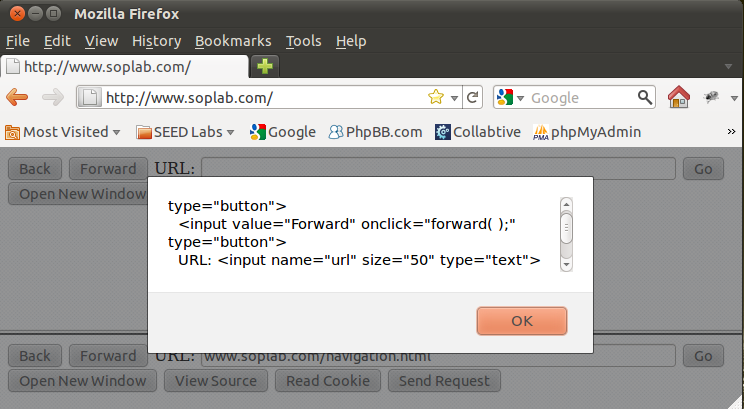




b) [www.soplab.com/navigation.html](http://www.soplab.com/navigation.html)

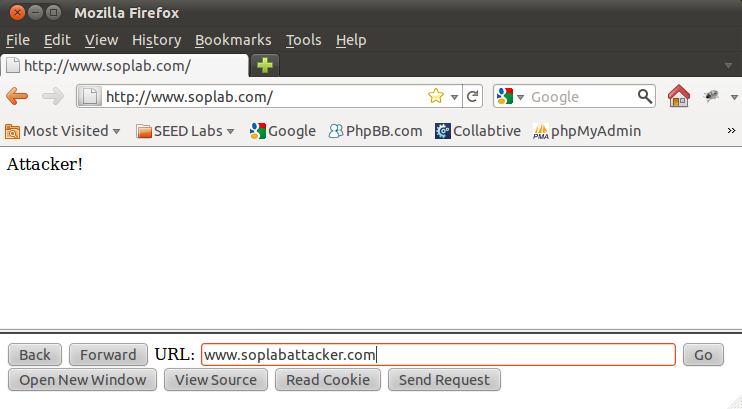
The sane reason as before, we could also get the source and cookies from the page:



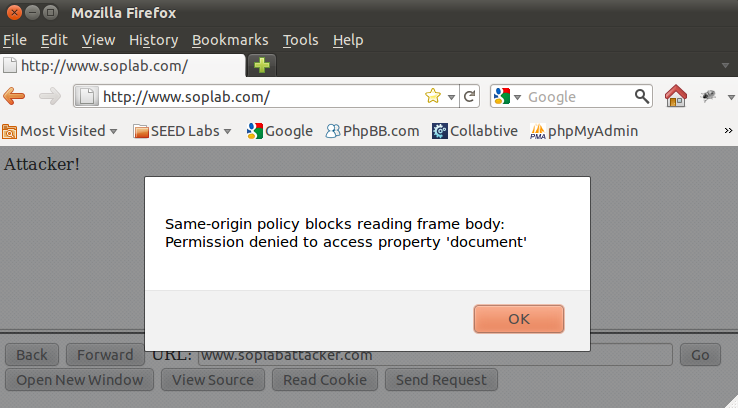


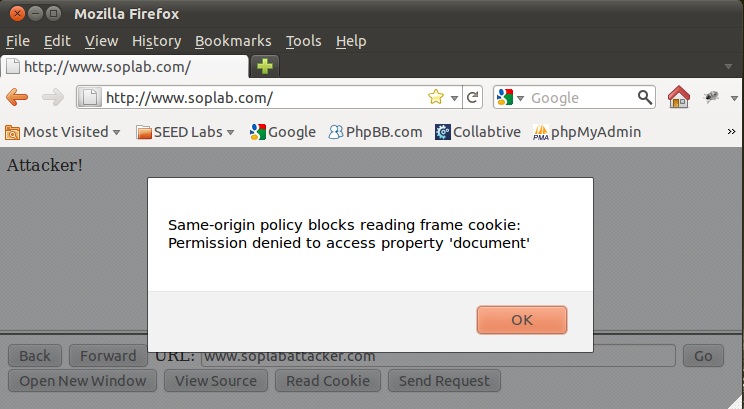
### 2. Cross-domain URL

[www.soplabattacker.com](http://www.soplabattacker.com)



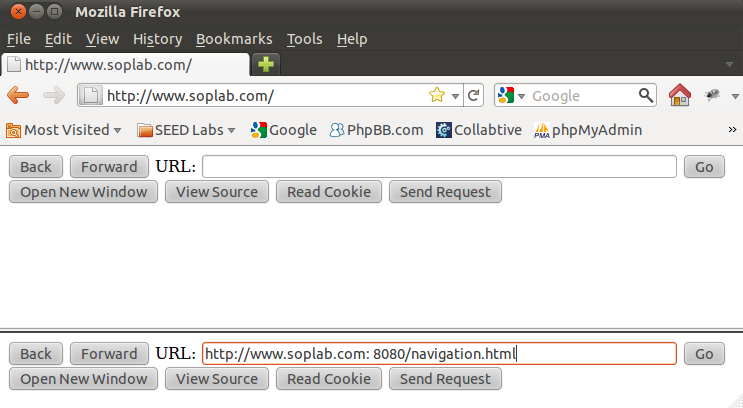
Because the above site is from different source, so the web application forbid the script to read the source and cookies:



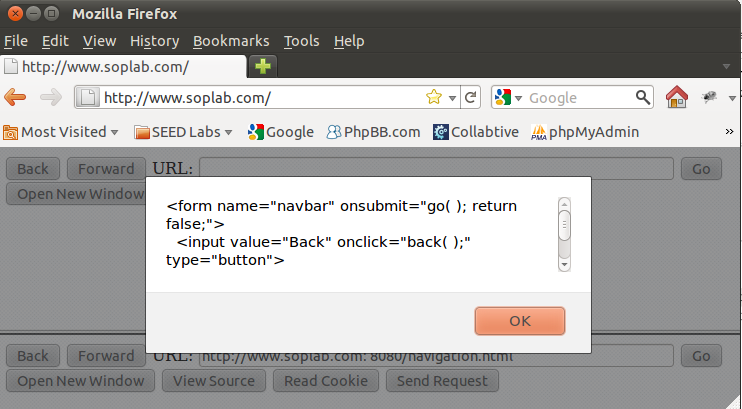


### 3. Try different port:

<http://www.soplab.com:8080/navigation.html>

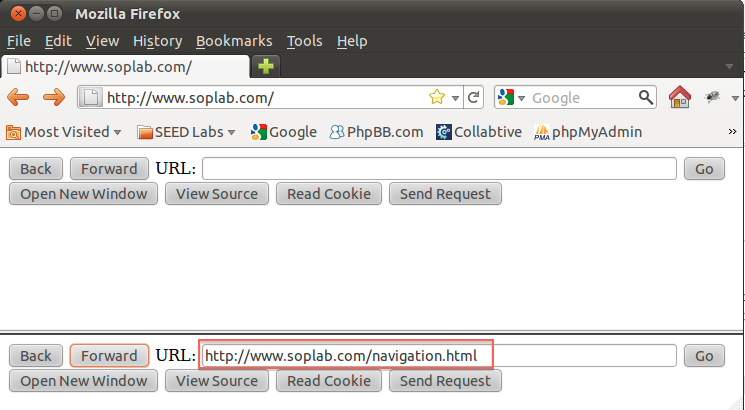


Although the website has two port, it is still the same origin, source and cookies are still readable:

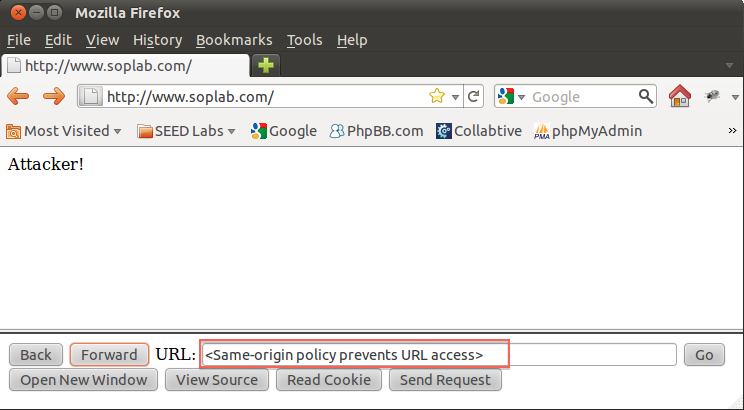


### 4. History object and the URL of the frame

If the page is from the same origin, both the History and URL are accessible:



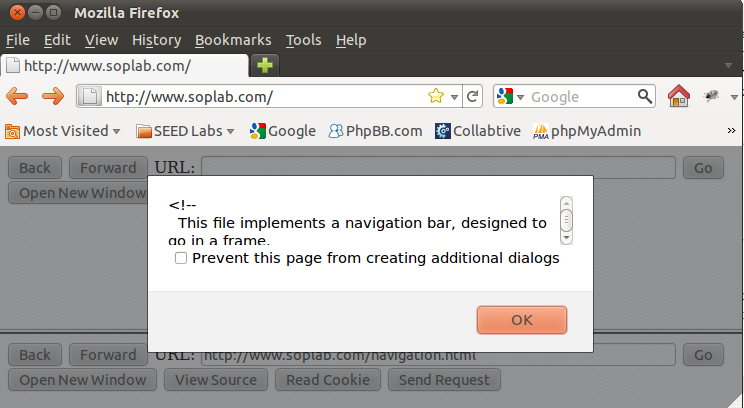
If the page is different origin, the History is still accessible, but URL is not.



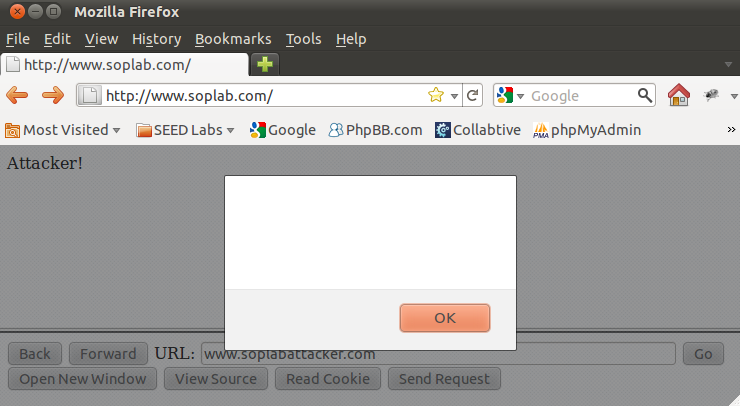
## Task 3: SOP for XMLHttpRequest

### 1. Using XMLHttpRequest API

We could send XMLHttpRequest to the same origin server, and get correct result



But the different site would return nothing back:



### 2. The dangers of not extending the SOP to the HTTP requests created using XMLHttpRequest

If the SOP did not extend to XMLHttpRequest, the attacker could use this requests to send request to the server, and web application would attach session cookie automatically, which will allow attacker get information from good website.

And every resource could get through XMLHttpRequest..

## Task 4: Exceptions from SOP