IT343
Applied Information Assurance
3rd Year, 1st Semester

Lab Report

Worksheet 4 – Cross Site Scripting

Submitted to

Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the

Bachelor of Science Special Honors Degree in Information Technology

10/03/2019

Declaration

I certify that this report does not incorporate without acknowledgement, any material previously submitted for a degree or diploma in any university, and to the best of my knowledge and belief it does not contain any material previously published or written by another person, except where due reference is made in text.

Registration Number : IT17122924

Name : Amarapala K.W.N.U.

Table of content

List of figures

Web for Pentester

Run the ‘web_for_pentester_i386.iso’ in Oracle VM Virtual Box.

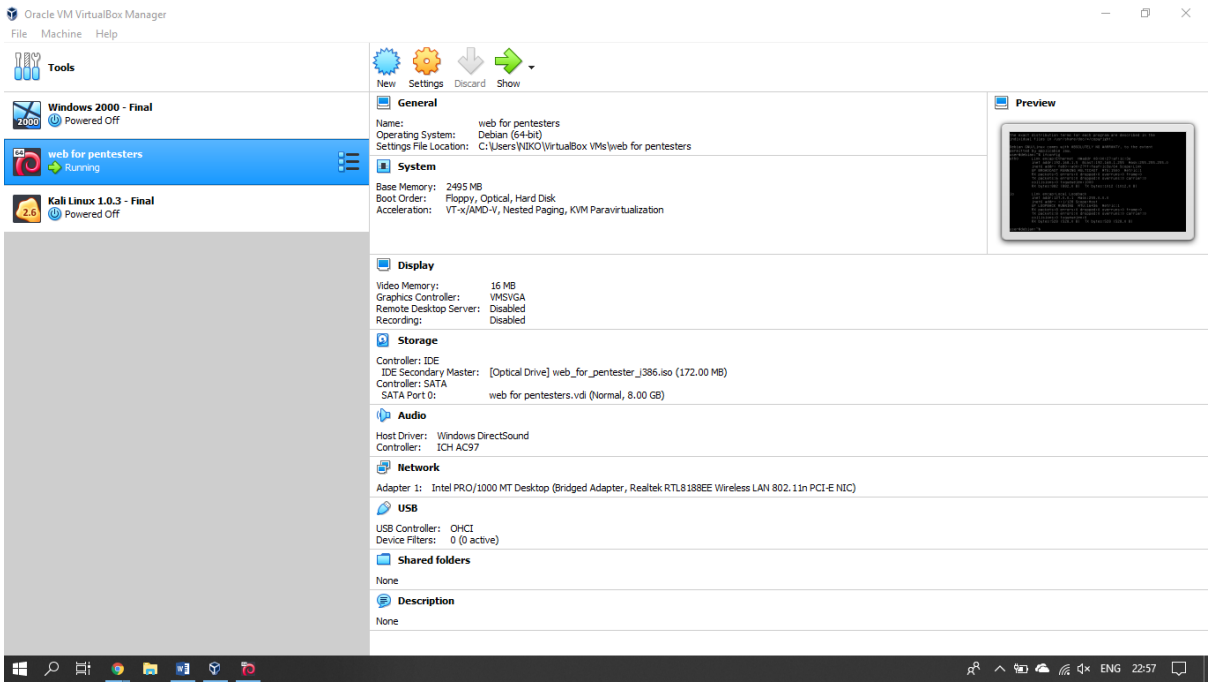

Figure 1. 1: Oracle VM virtual Box

Type ‘ifconfig’ and get the ipaddress for ‘web for pentester’.

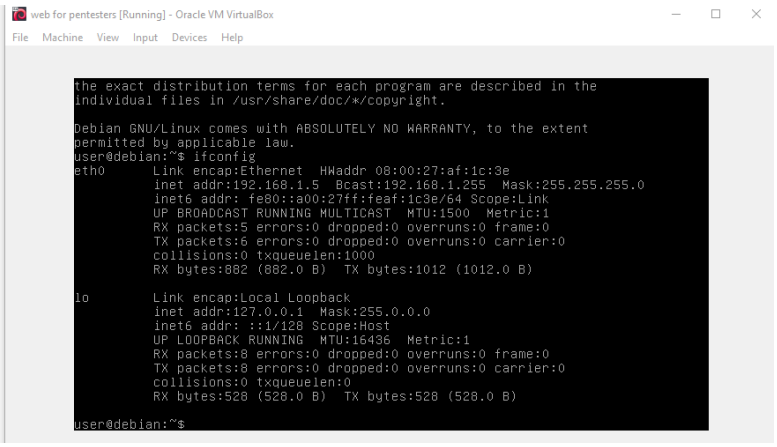

Figure 1. 2: Ipaddress of the web for pentester

The Ip address which I obtained is “192.168.1.5”. Type the ip address on the web browser.

Browse this http://192.168.1.5/

The following webpage will display as the search result.

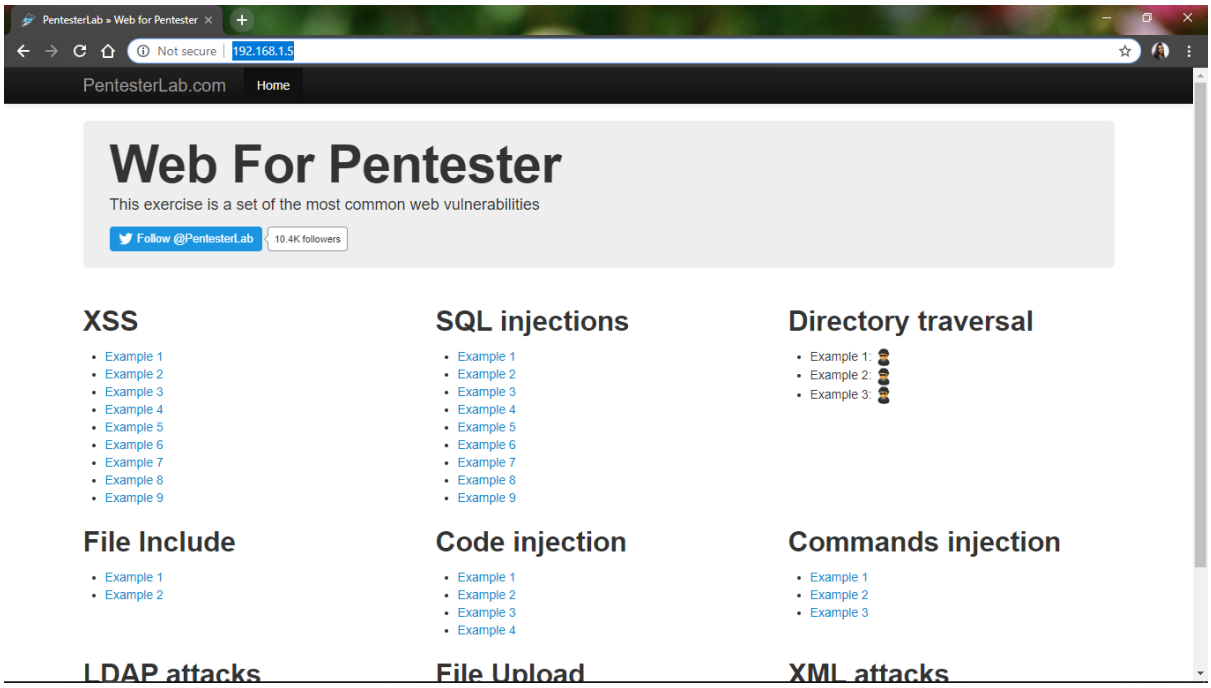

Figure 1. 3: web for pentester homepage

Click on the example links under XSS to try out those.

Example 7

The URL of Example 7 : http://192.168.1.5/xss/example7.php?name=hacker

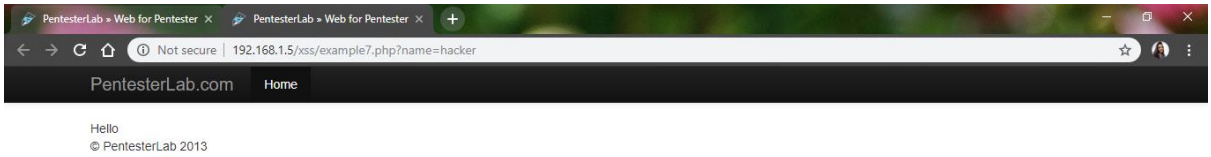

Figure 1. 4: Example 7

In this, some of the special characters we enter in the URL get HTML encoded.

Enter the following URL, no alert box will be displayed on the page as the charaters entered get encoded.

http://192.168.1.5/xss/example7.php?name=hacker';alert("NIKO");//

The URL given below will display after entering the previously given URL.

http://192.168.1.5/xss/example7.php?name=hacker%27;alert(%22NIKO%22);//

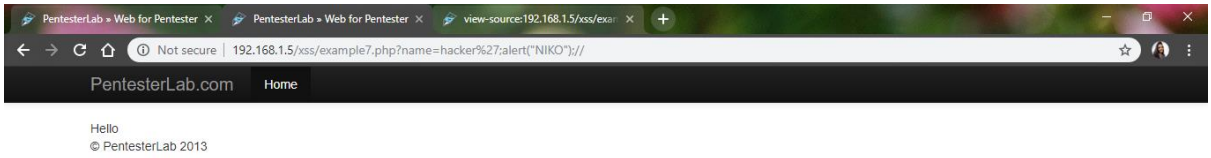

Figure 1. 5: Example 7

No alert box will display.

The source code will display as follows.

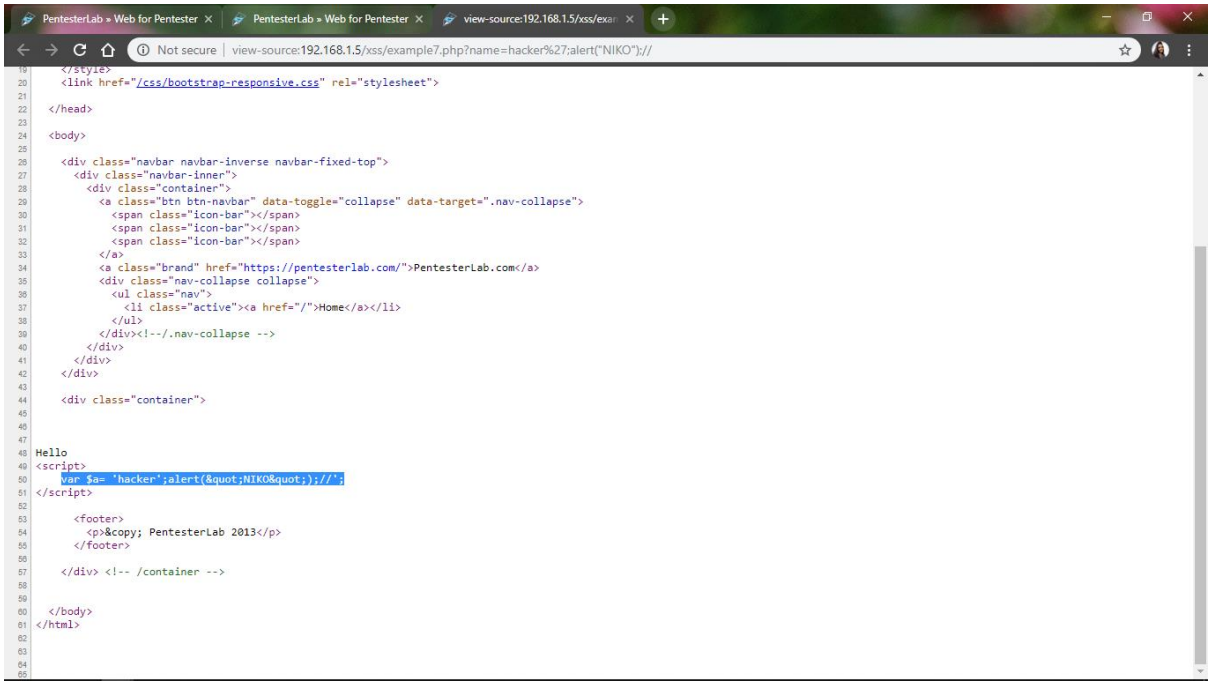

Figure 1. 6: Source page

Enter the following URL

http://192.168.1.5/xss/example7.php?name=hacker';alert('NIKO');//

The special characters will get encoded. The new URL displays as given below.

http://192.168.1.5/xss/example7.php?name=hacker%27;alert(%27NIKO%27);//

Figure 1. 7: Example 7 alert box popup

Alert box will be displayed on the page.

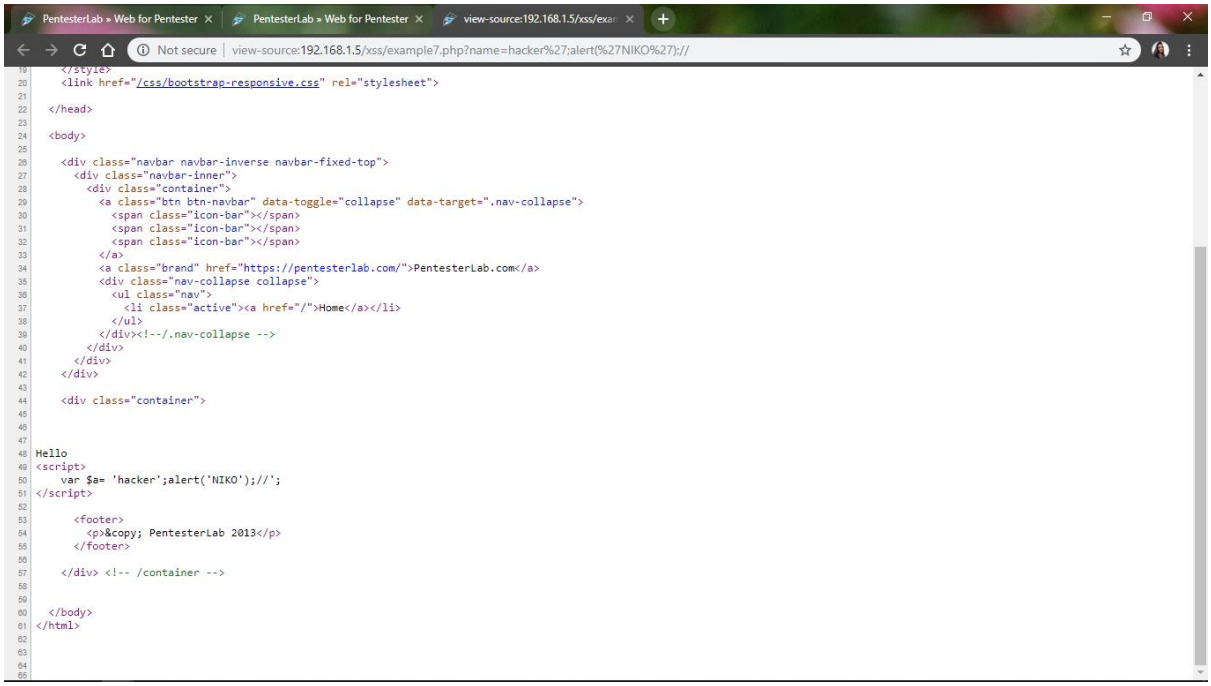

Figure 1. 8: Source Page

Example 8

Example 8 URL: http://192.168.1.5/xss/example8.php

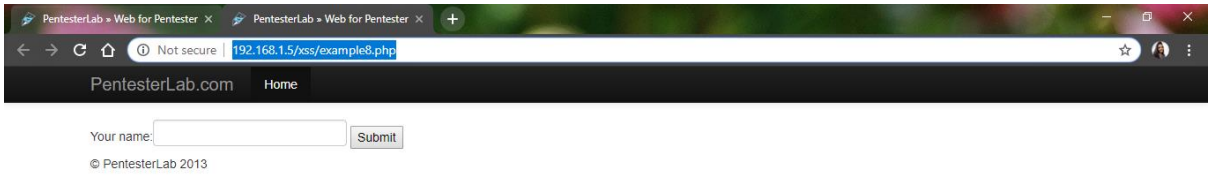

Figure 1. 9: Example 8

Type the URL given below

http://192.168.1.5/xss/example8.php/”><script>alert(“XSS”)</script>

The alert box will display.

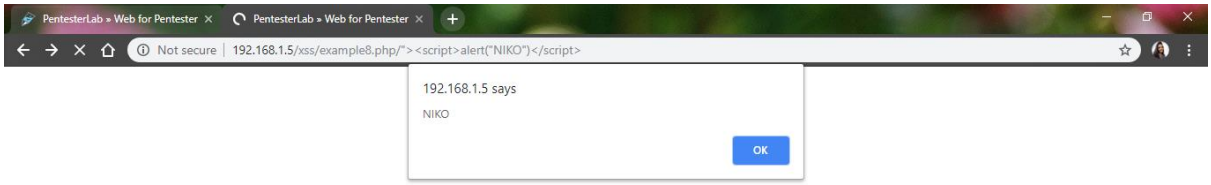

Figure 1. 10: Example 8 alert box