Cross Site Scripting: Lab Exercise
IN618 Security

Introduction

In this lab you will exploit a cross site scripting (XSS) vulnerability in a web application. The application is online at http://in618.sqrawler.com. The site requires the user to supply a username and password, but any username/password combination will work. The user's browser is then issued a cookie that is checked on subsequent pages.

On the next page the user is presented with a text box. Anything entered into that box is written out on the next page. This application has basically the same XSS vulnerability that we explored in the first lab.

1 Tasks

Your task is to demonstrate two exploits of the XSS vulnerability:

1. Capture a session cookie from a logged in session. The cookies are unique to each sesssion, so you cannot just use the same cookie value that someone else captures.
2. Use XSS to alter the display of a web page in a nontrivial way, i.e., you can just pop an alert box.

2 Submission

You will submit two JavaScript files, one for each exploit listed above. You will also submit a text file explaining how each one works. Include the captured session cookie value in that file.

Files are to be submitted to your SVN repository. Instructions for using SVN will be distributed seperately.

You may consult with other classmates about the exercise, but the submitted materials must be your own. No credit will be given for copied work.

3 Resources

You will need a web server to host your exploit files. One has been set up. Obtain login credentials from the lecturer.

The example code from the previous lab will be helpful.

4 Marking

There are 10 marks for this exercise:

- Capturing a session cookie with XSS: 2 marks;
- Capturing the session cookie using an automated script (i.e., a script that writes the captured cookie to a file): 2 mark;
- Altering the display of an exploited web page: 3 marks;
- Explanation of the exploits: 3 marks.