Attack A. Cookie Theft

For this attack, we insert the “email script” javascript text after “http://zoobar.csl.toronto.edu/users.php?user=">” so that it will be executed. It must be URL encoded or else it won’t work. The payload is set to “document.cookie” to get cookie information. We quickly reload the page to hide the errors from the user.

Attack B. Cross-Site Request Forgery

For this attack, we create a form with fields identical to the "http://zoobar.csl.toronto.edu/transfer.php" "transfer\_form" and specify the transfer of 10 zoobars to "attacker" in the form. We submit the form to an <iframe> instance of "zoobar.csl.utoronto.edu" and imitate a "send" button click. Finally, we listen for when the form is submitted and quickly redirect to "http://ece568.csl.toronto.edu/".

Attack C. Password Theft

For this attack, we create a form with fields identical to the "http://zoobar.csl.toronto.edu/login.php" "login\_form" and submit it with a "special" "username.value" string. The "special" string is constructed such that its content will be evaluated and it will listen for a "Log in" button click and send the "username","password" using the email script. Certain sections of the string must be escaped for it to process without errors. We use "event.preventDefault();" to stop all actions until email script has been processed. We also have "image.onerror" to listen for when email script is starting to be processed, and then remove listener and click login button so that everything appears as normally would for the user.

Attack D. Profile Worm

The vulnerability is that there is an eval on document.getElementById('zoobars').className. The malicious profile text consists of a span element that contains the same id ‘zoobars’ as an existing element. Since this inserted span element comes first, the eval will now be passed an arbitrary string as the class name. Two iframes are created, one to transfer 1 zoobar to the attacker and the other copies the attacker profile to the viewer profile. To set the attacker profile to appear to have 10 zoobars, the string contains “total = 10;”. This initializes total and since the later assignment to total will fail, total remains unchanged.