Practical Attack & Defence
Kimmo Saurén
Metropolia

Exercise 5. XSS and CSRF

Cross-site scripting attacks and Cross-site request forgery attacks are very common attack methods agaist users of certain web-application.

XSS attack is possible when web-application does not filter user input and displays this input unfiltered in it's webpages. This makes it possible for attacker to run scripts in victims session. This leads to information disclosedure and possible executing actions on victim's application session.

CSRF attack is possible when web-application has predictable URLs. Attacker can then make request from evil web-site to user's other web-application sessions.

It this laboratory exercise you are going to try to evade different input filters.

Do following steps to start your laboatory:

1. Download a special xampp from http://users.metropolia.fi/~kimmosa/xampp-attack.zip
2. Extract and go to directory xampp
3. Run setup-xampp.bat (this will take care of right path for the software)
4. Run xampp_start.exe
5. Open Firefox and browse to http://localhost/lab-3-XSS/lab1

You have three labs.

Lab1:
Simple XSS exercise. Just try to get an alert box displayed.

Lab2:
Simple XSS exercise. Just try to get an alert box displayed.

Lab3:
CSRF/XSS lab.

Part 1: Using XSS to steal cookies from a user.

1. Create a cookie stealer webpage in your own website. Something like stealer.php
2. The stealer.php should take one GET parameter "cookies" and store this into file. You can probably find cookie stealer PHP from internet. Host it on your web site.
3. Now you know that lab3 application is XSS vulnerable, so you goal is to create such input to application that it will send your cookies to stealer.php.

Part 2: The CSRF part can be done in following steps:
CSRF: While the victim is using guestbook, he browses to a malicious webpage which adds an entry to guestbook without victim noticing that.

1. Implement a separate webpage which user will visit while using lab3 web-application.
   - This web page should be in your own users webpage (like users.metropolia.fi/~kimmosa)
2. Try to add a "YOU HAVE BEEN HACKED ENTRY" to lab 3 questbook web-application with your evil webpage.