Practical Attack & Defence
Kimmo Saurén
Metropolia

Exercise 6. Insecure direct object references and unrestricted URL-access

Insecure direct object reference is a type of vulnerablility where malicious user is able to access objects that he shouldn't. This can happen if contents of a webpage is generated using some key or parameter value. The malicious user can change these parameter values to access data that he is not authorized to.

It this laboratory exercise you have to break a holiday present website.

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-4-Obj/lab1

LAB 1:

This web application displays a holiday present choice to user. Your job is to following:

1. You don't really like ferrari. Change the car to porsche.
2. You would like to advertise something. Add a advertisement link at the top of the page so when the page is accessed the advertisement is shown everytime.
3. Create a new hacked page into the server and point a link to it from the main page.

LAB2:

This is an old exam question. So try to hack the application and find a password. The application will show you the password when you have cracked the application.

LAB3 (Broken Authentication & Session Management exercise):

This is an old exam question. You have found out that 'jsmith' is a correct username in this system, but you don't know the password. Find out which of the following usernames is also a correct username in this system. Explain why it is a correct and how did you found it out.

Usernames:
- ksmatin
- tkisaton
- jmotana
- aapeli
- correctone
- notthis

Correct username is:____________________