Attack Project 2

Due Wednesday November 28 at 11:59 pm

Project Description

The objective of this project is to help students understand the Cross-Site Request Forgery (CSRF or XSRF) attack. A CSRF attack involves a victim user, a trusted site, and a malicious site. The victim user holds an active session with a trusted site while visiting a malicious site. The malicious site injects an HTTP request for the trusted site into the victim user session, causing damages.

In this project, students will be attacking a social networking web application using the CSRF attack. The open-source social networking application called Elgg has countermeasures against CSRF, but we have turned them off for the purpose of this project.

You will need to follow the project description located here:

- Go to the link below, then click on "Description"
- http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Web/Web_CSRF_Elgg/

For this project, you are only required to complete **Task 1** described in the link above. Make sure you are using the **SEEDUbuntu12.04** virtual machine.

You will submit **all of the code** that you used for this project along with a **readme.txt** that describes the files used for each task and how to run them. You will submit a project report that needs to include the following sections:

- An **"Abstract"** section that provides the overall summary of the project, your observations, and results.

- A **"Methodology and Results"** section that describes in detail the methodology you used for conducting the attack including the various steps you performed. You need to describe your code and include **screen captures** that clearly demonstrate the functionality of your solution. Provide details using LiveHTTPHeaders, and screen shots. You can also include Wireshark captures if you'd like (Wireshark is not required for this project). Finally, describe how you were able to collect your data if any.

- A **conclusion** that includes a summary of what you have learned from this project highlighting what you have found insightful. Discuss new directions that would have been interesting to explore for this project.

Submission

You need to submit all of the following via canvas:

- The written report in doc or docx format
- A readme.txt file that
- All the files you've used for the attack project

Do not compress these files into a .zip or .tar.gz. Each file must be uploaded separately.