Secure Programming Laboratory 4: Web Attack

SP Demonstrators: Arthur Chan / David Aspinall

14th November 2022

Orientation

This is the fourth Laboratory Session for **Secure Programming**

It is convened by Rob and David.

The **handout** and other resources are available online via the course web page.

- If you have question about the past labs, ask us.

What is this lab about?

Cross Site Request Forgery (optional)

- **Task 1** Web request analysing tools
- **Task 2 ~ 3** Cross Site Request Forgery
- **Task 4** Countermeasures for CSRF

What do we hope you will learn?

- Understanding client side web attacks
- Understanding countermeasure for web attacks
- Understanding further web security concerns

Warning

- You will be **attacking** a web server, always point your attack payloads to `localhost` of the seedlab.
- You will be **attacking** the web server on the following url
  - **http://www.csrflabattacker.com**.
  - **http://www.csrflabelgg.com**.

  We have modified the host file in the seed lab to point this url to the localhost of the SEED Lab. Don't change this setting as it is protecting you not to attack the dice environment and the real network.
- **ALWAYS KEEP YOUR ATTACK TRIAL WITHIN THE SEED LAB ENVIRONMENT**

Solutions and Checkpoints

You do not need to submit a lab report to us, but please keep answers to the **checkpoint questions** for your own use, to check your understanding and when revising the material for the lab.

Please **do not post solutions** on any forum. If solutions are distributed it will spoil the experience for other students using SEED labs around the world.

During the lab we will provide individual help and guidance, and also make announcements during the lab with hints and tips.

You can always discuss the checkpoint question or any materials with us during the lab section or through Piazza.

Good Luck!

We hope you enjoy the lab.