Secure Programming Laboratory 4: Web Attack

SP Lab Demonstrators

Orientation

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

The **handout** and other resources are available online via the lab web page https://opencourse.inf.ed.ac.uk/sp/lab-4

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 Elgg application running in the web server on the following URL:
  - **http://www.seed-server.com**.
- The attacker’s web site is
  - **http://www.attacker32.com**.

Please check the `/etc/hosts` file on the SEED VM to check the hosts file contains these domain names.

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.

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.