Secure Programming Laboratory 3: Race Conditions

SP Demonstrators: Rob Flood/ Aspinall

31st October 2022

Orientation

This is the third 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.

What is this lab about?

- Ask if you need have questions on the previous lab

Race Conditions

- **Tasks 1-4** Attack and defence for race condition vulnerability

Shellshock Attack (*if time*)

- **Tasks 1-4** Understanding Shellshock and a RCE example

What do we hope you will learn?

- Understanding race conditions and TOCTOU (Time Of Check to Time Of Use) design flaw
- Understanding soft symlink / path attack
- Shellshock: exploiting the vunerability with a reverse shell

Checkpoints and Solutions

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 public forum. If solutions are distributed it will spoil the experience for other students using SEED labs around the world.

Discussion

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.