Secure Programming Laboratory 1: Introduction

SP Demonstrators: Rob Flood / David Aspinall

10th October 2022

Orientation

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

It is convened by Rob and David.

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

What is this lab about?

Core: Environment variable and SETUID program

- **Task 1 ~ 2** Environment variables.
- **Task 3 ~ 7** Inheritance of environment variables.
- **Task 8 ~ 9** Case study with environment variable.

You might like to try the optional labs if you haven't covered this topics before:

- Classic Buffer Overflow (Set-UID) Version

In your own time you might also try the Server Version of the buffer overflow attack lab and the Return-to-Libc Attack.

What do we hope you will learn?

- Understanding/revising the basic permissions model of Unix/Linux
- Understanding environment variables and their implications for security
- Some security precautions when executing binaries in Unix/Linux

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.

Resources

- Use **anything**! You are encouraged to search on the web for help, tutorials, manuals, etc.
- You can get plenty of help this way. But it is probably more rewarding to try to solve the exercises for yourself first. Make sure to spend time experimenting, not only reading.
- **Warning**: experiment with care! If you download sample exploits, generation tools, etc, install and run these in the Virtual Machine, **not on the host DICE environment**. The VM already has several interesting tools provided.
- **Ask us!** We are here to help, as much as we can.
- **Ask each other!** There may be expert x86 programmers, C hackers, exploit developers(?) among you. . .

Timing

You may not have time to complete all exercises in this lab session.

- Don’t worry!
- Of course, you can spend more of your own time later if you are interested. Completing the lab is desirable but not essential: at least, try to look at each exercise a little bit and discuss with colleagues if you find things hard or ask questions on Piazza. The important thing is to understand the concepts well.
- If you are familiar with the environment variable and permission model of Unix/Linux, you may finish this lab fast. You can always try to complete the optional lab which is some fun and optional challenge for revisioning on memory corruption topic which are taught in the Computer Security course.

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.

We will give you enough time to complete the task. At some certain time, we will stop you and demonstrate the lab and discuss some important points. You may also raise question between the demonsrtation period.

Setup of the SEED Lab

This is the first lab, we will demonstrate on how to setup the SEED lab which will be used in all 5 labs in the future.

Good Luck!

We hope you enjoy the lab.