

COMSM1500 (Systems Security)
Coursework 2

Students: cy13308 and rz13310

Contribution:

cy13308: completed Lab 4 tasks 1-3, helped with Lab 3 tasks 1,2.

rz13310: completed Lab 3 tasks 1-4, helped with Lab 4 task 1.

Overall contribution: cy13308 50%, rz13310 50%

1 Overview

This coursework investigates two basic yet powerful vulnerabilities: format strings and buffer overflow. In the upcoming experiments, the SEED labs virtual machine is used. We target audiences who have some programming experience in C and a basic understanding about memory layouts. Required source code files should be found in

<https://www.cs.bris.ac.uk/Teaching/Resources/COMSM1500/>.

In each technical report, we first introduce the problem at hand by providing the context. Then, we illustrate how the respective mechanisms break down in under certain circumstances. We proceed to exploit these vulnerabilities and finally, reflect on the bigger picture.

2 Network Attacks: Technical Report

3 Network Attacks: Reflective Report

4 SQL injection: Technical Report

5 SQL injection: Reflective Report

References