

Lab 3 --- Format-String Vulnerability & Cross-Site Scripting Attack Lab

In this lab, you could use the previous Ubuntu 20 environment.

Requirement

Labs (90 points)

We will have a quick interview for these tasks. If you can't answer the questions related to the experiment details, you will lose some points. Don't worry if you do them by yourself.

A. (50 points) **Race Condition**(Format-String), you could learn how to use docker [here](#).

B. (40 points) **Dirty COW**(XSS)

Report (10 points)

Please describe how you do part A and B in your lab report, with screenshots, to describe what you have done and what you have observed. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will receive little credits.

TA for this lab: jpwan19@fudan.edu.cn (万俊鹏). Please email me If you encounter obstacles or do not understand certain requirements.