TDT4237 Software Security - Exercise 1

Introduction

In this exercise your task is to plan and conduct penetration testing of the highly insecure web online bookstore "Amu-Darya" and discover as many security vulnerabilities as possible. The exercise consists of two separate parts, as described below.

Rules

1. Hack nondestructively; If you bring the entire application down, you won't get any work done until we redeploy it.
2. You are not allowed to exploit the server OS, meaning that you should not run attacks that affects other groups than the one you are attacking.
3. DoS (Denial of Service) attacks are not allowed.

Part 1

For the first part you should plan and conduct a penetration test *without* access to the source code. You will only need to do "Part 1" of the "Setup Guide" to complete this part of the exercise.

Fill out a Vulnerability Reporting Form documenting the vulnerabilities found, and write a report explaining how the penetration test was planned and executed.

The delivery deadline for Part 1 is Friday September 20th 1800.

Part 2

For the second part you should plan and conduct a penetration test *with* access to the source code. Doing "Part 2" of the "Setup Guide" will be helpful in completing this part of the exercise.

Make a *separate* "Vulnerability Reporting Form" covering *only* the new vulnerabilities found in part two, and write a final, extended report that covers the entire exercise.

The delivery deadline for Part 2 is Friday September 27th 1800.

Expected Deliverables

1. A report explaining how this exercise was planned and executed. Note that it should include rationale for your selection of tests to perform. Hint: It should include a page map.
2. Two completed vulnerability reporting forms; One for each part of the exercise.