Flaggjakt Hacking Challenge: A Good Offense is the Best Defense

Didrik Bergström
Martin Clason
Joakim Argillander
Arunava Naha
Ingemar Ragnemalm

November 14, 2025

Version 1.0

Contents

Chapter 1

Introduction

Have you ever taken a computer security course and wanted to learn more? Tired of just listening to the lecturer going on about hacking computers while you dream about actually breaking into stuff? Now is your chance! In this lab course, you will be taking on the role of a penetration tester, or pentester for short. This means you'll be shown a selection of vulnerable web applications, with the goal of breaking into them and/or make the application perform tasks that it was not designed for.

1.1 Overview

In Flaggjakt (the lab system), you will practice penetration testing. Using a set of increasingly difficult assignments or challenges, you will gradually learn the basics of how an adversary might exploit badly designed applications and security systems. The goal is to give you the basics in practical security work and to understand some common pitfalls when developing web applications. After the lab, you should be well-equipped to avoid these security issues whenever you develop your own web application.

Flaggjakt is a completely new system for this year, so things might be a little brittle. If you see something that seems odd or broken, please reach out to us at flaggjakt@groups.liu.se. To help our administration of the course, kindly use "BUG:" as a prefix in the subject heading.

1.2 Lab Organization

This lab will run from the start date 14th November 18:00 until the end of the exam week in January. The lab system is publicly available, and you can work on the assignments in your own time on the lab computers or your personal laptops. Since the server is accessible from the Internet, you can also work from home. Your lab progress will be stored on the server so you can come back

at any time. You are required to complete the lab yourself. However, you are allowed (and encouraged!) to cooperate to a reasonable degree.

There will be dedicated time slots when the lab assistants, Didrik Bergström and Martin Clason, will be available to help you out if you are having problems. Please note that these slots, named Laboration in the schedule, do not have mandatory attendance.

Assistance will be provided on a first-come, first-served basis. Also note that the teacher can give you hints and tricks, but we won't solve the assignments for you. Help with the mandatory assignments will take priority over the optional challenges. Plan carefully, because time will be limited for each student.

1.3 Deadlines

The lab starts on Friday, the 14th of November 2024 at 18:00. **The lab must be finished before 18:00 on the 16th of January 2026.** At this time, the assignments will be disabled, and no further progress can be made. If you haven't finished the lab by this date, you will have to re-take the lab next year. There is also another, soft deadline. **At 18:00 on Sunday the 28th of November 2025 the competitive part of the lab ends and the scoreboard will lock.**. Remember, the competition is optional, and the points you collect have no impact on your grades in the course. When you have finished all mandatory assignments, you are done with the lab. We retrieve your completion status from the TopDog server after the final deadline and report it in LADOK. Hence, there is no need to contact the teacher or examiner when you are done.

1.4 Write-ups and notes

It is strongly advised that you keep notes on how you solve the challenges; however, you don't have to submit them. The most pragmatic reason is that if something were to happen with the lab system or database, it would be much easier for you to reproduce the solutions. It is also used in a professional setting, where you submit a pentest report detailing the vulnerabilities you might have identified. It can also be quite handy to not only keep notes on what worked in the end, but also what you have tried and concluded didn't work. E.g., if you are trying to crack a SQL injection challenge, you can easily keep track of what you've tried and not waste time on trying the same things over and over.

1.5 Rules and Disciplinary Stuff

Each student is expected to perform the lab to pass. In addition, you are expected to understand and follow the university-wide rules for disciplinary matters, and, like any other examination, you are not allowed to cheat or disrupt examinations. The latter includes intentional (or through carelessness) DOS of the lab service.

Do not share cookies or flags with other students, as it will not help you, and we have logging systems in place to track that you actually perform the necessary steps for each challenge.

Do not try to hack or mess with CTFd (the portal) or the multi-juicer balancer. You should only attack the challenges. (For the moment, all challenges are served through juice shop.)

1.6 Ethics

This lab and what you learn are for educational purposes only. Do not attempt to use these techniques out in the wild without proper authorization. If you are caught engaging in unauthorized hacking, most companies will take legal action. **Claiming that you were doing security research will not protect you!**

1.7 Contact Information

The email flaggjakt@groups.liu.se is where you reach the lab assistants for questions regarding the challenges, and it is also where we would like you to contact us regarding issues with the lab system.

Chapter 2

Preparing for the Lab

Begin by reading through the entirety of these lab instructions. Also, note that we are continuously improving these instructions, so be sure to check the latest version on Lisam.

2.1 Logging In

2.1.1 Account Creation Issues

Just before the lab starts, you will receive an email with instructions on how to create your lab account. If you have issues creating your account, please contact us at flaggjakt@groups.liu.se.

Log in to CTFd

To log in to CTFd, where the progress is tracked and where you can see the list of challenges, go to `https://flaggjakt.isy.liu.se/ctfd`. The first time you log in, use the provided one-time password from the email. You will then be prompted to change your password. Please remember to write down the new password you create, as you have to get in contact with us if you need to reset it. (We will improve this in the future.)

Access/create your juice shop instance

To access your juice shop instance, visit `https://flaggjakt.isy.liu.se/` and if you don't have an active session (a balancer cookie), you will be redirected to `https://flaggjakt.isy.liu.se/balancer`. Here you can log in to your juice shop instance or create one if it is not running at the moment. You do this by entering your liu-id and clicking "join team" (see figure 2.2a).

You will then get a passcode, which you use to log in to your juice shop instance, see 2.2a. If you lose the passcode, you will not be able to reset it yourself, so write it down. You can reach out to us and we can reset it for

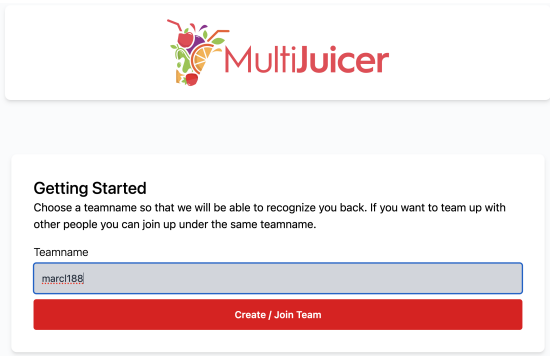
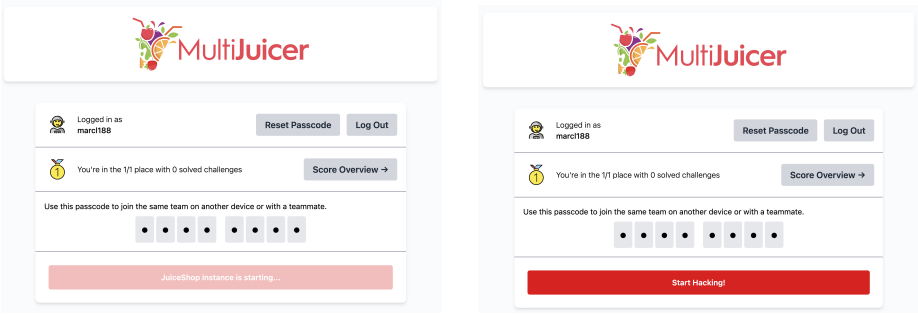


Figure 2.1: How to create a new juice shop instance in. Use your liu-id as the team name.

you, but you could also wait 30 minutes, since the instance will automatically be deleted after some time of inactivity. Then, you can create a new team with your Liu-ID. It really shouldn't be called team since it's your personal instance, but that's how it is for the moment. As long as you have the balancer cookie, you will have your juice shop instance available at the root `https://flaggjakt.isy.liu.se`.

After a minute or so, your personal juice shop instance should be ready and you can start hacking (see 2.2b).



(a) Waiting for the instance to start.

(b) Instance ready.

Figure 2.2: The balancer spinning up your juice shop instance and the passcode for this instance, write it down!

Chapter 3

Working Through the Lab

The lab consists of mandatory challenges (marked on `https://flaggjakt.isy.liu.se/ctfd/challenges` as <Mandatory>), which are the following:

- Score Board
- Privacy Policy
- Zero Stars
- Confidential Document
- Poison Null Byte
- Missing Encoding
- DOM XSS
- Empty User Registration
- Exposed credentials
- Login Admin
- Weird Crypto
- Reflected XSS
- View Basket
- Manipulate Basket
- HTTP-Header XSS
- Server-side XSS Protection
- Allowlist Bypass
- User Credentials
- Two Factor Authentication
- Unsigned JWT
- Forged Coupon

The remaining challenges are optional but can earn you points in the competition and help you purchase hints.

Chapter 4

Contributing to the Lab

If you see any issues with the lab, don't hesitate to write us at flaggjakt@groups.liu.se. Moreover, if you'd like to develop the lab, we welcome discussions/suggestions on thesis work.