IDATT2503 - Exercise 4 - Edvard Berdal Eek

25.09.2025

Simple SQL-injection

Introduction

First i wanted to make a challenge exploring vulnerabilities with OAuth 2.0. However, i realized that this would require to much work. I then wanted to try out a buffer overflow vulnerability as i wanted to learn more about it, but i ran into issues due to using a computer with arm architecture. I then finally only had time left for a simple SQL-injection vulnerable application.

Task Description

How to run

Build Docker Container

docker build -t sql_ctf .

Run Container

docker run -p 8080:8080 sql_ctf

Access the Challenge

Open http://localhost:8080 in a browser.

Hints

As the task is rather simple i would not provide any hints. Maybe not even provide a hint in the task name, possibly leading users to try other exploits first.

Solution

By typing **' OR '1'='1' --** in the username, the first entry in the database will be returned containing a flag. A bypass is if a user guesses the correct password they will get the flag.