JENSEN yrkeshögskola
TRÄNING FÖR VERKLIGHETEN

Course name: Secure communication over the internet
Class: FWK23G
Semester: Autumn semester 2023 and Spring semester 2024

BLOG PLATFORM PART 2

INTRODUCTION

Background description, question, delimitation and goals	Background: Security is always an important aspect of any application. Students will have the opportunity to develop a simpler blog application that uses modern methods to communicate over the internet. The application also now includes OAuth and a basic role system for managing permissions. Students also protect their application against XSS and CSRF. Goal: Create a simpler application that uses modern methods of security. For example, salting and hashing of passwords and token-based session management. Limitation: The blog only needs to contain text and title.
Why should you do this work?	Purpose: • Learn to manage passwords. • Learn to manage different privileges. • Learn about OAuth 2.0. • Learn about Role-based Access Control • Learn to prevent common attacks such as XSS and CSRF.
What will you deliver?	The following must be delivered: 1. Link to a public GithubRepo In the report, it must be clear to the teacher: • Which users exist and their passwords. • How I recreate your database. Two suggestions regarding Redis: • Write a file 'commands.redis' where all SETs are separated with a new line between each command • Use SAVE and submit the .rdb file in the submission on LearnPoint • Which dependencies are used. Therefore put all dependencies in package.json

YOUR PROJECT TASK

What will you do?	Your task is to create a blog. In the blog you can see the blog posts of different users. All users should see in their feed the various blog posts and who has created them. The blog posts only contain text and a title. Requirement [G] Each user can log in with a unique username and password. [G] The password is saved hashed and salted in the database. [G] The page should remember who you are - if you open the page again, you should still be logged in. Within a reasonable time frame of course. It should also say up in the right corner "logged in as {username}". [G] The application can be started without problems. [G] The blog posts are in a database and not hardcoded. [G] Each blog entry must state who wrote it. [G] Each blog post must have a date and time attached to it. [G] The app stores any session data in a database, not in memory. [G] The application uses appropriate methods and status codes. [G] There is an admin login. The admin login must have permission to remove all posts from the platform. [G] New users should be able to register. [G] A user can login/register via GitHub (OAuth 2.0). [G] Each user can post blog posts themselves via a form. [VG] Each user can delete their own posts. [VG] Users can comment on each other's posts. In the comment field, the user must be able to use HTML to format their posts. example becomes **example.** [VG] The site uses several methods to secure itself against XSS and CSRF. [VG] In your submission, please specify some code changes and instruct how one could perform an XSS attack with the protections removed. It is enough to inject an alert(), [Bonus] Users can “like” each other's posts. It must then appear in all posts who/who liked the post. If you are inside the page when someone likes your post, you get a notification, without having to refresh the page (use WebSockets for this). A well-implemented bonus feature will give four bonus points on the exam.

SUBMISSION AND ACCOUNTING

Submission	Submission takes place via Learn Point **15 January 23.59**

JENSEN yrkeshögskola
TRÄNING FÖR VERKLIGHETEN

ASSESSMENT AND FEEDBACK

Assessment takes place against the following grading criteria:	The grading criteria for Pass and Pass with Distinction are: Passed (G) To receive the grade Passed (G), the student must have completed the course and achieved all course objectives. Well Passed (VG) In order to receive the grade Well Passed (VG), the student must have completed the course and achieved all course objectives. The student must also be able to conduct well-founded and nuanced reasoning and be able to make well-founded and nuanced assessments regarding the application of the methods and tools included in this course. **Approved** • All G requirements from the requirements specification are met. **Well approved** • All VG requirements from the requirements specification are met.
Feedback	The groups receive written feedback via the learning platform LearnPoint **by the 29th at the latest January**