DB 25 Handin-6 **Database Security and NoSQL** **Deadline 21.3 18:00**

The purpose of this hand-in is to demonstrate that you know how to avoid SQL injection attacks, authorize access to a database, and work with NoSQL databases.

Please make sure to make yourself familiar with the reading material and lectures, and work with the presentation exercises before doing your hand-in. As detailed in "the road to success" on the course homepage, this benefits your learning and your understanding of what this hand-in asks you to do. The criteria for evaluation are detailed in the rubrics for this hand-in on Brightspace.

Important formality:
On the top of the first page in your hand-in,

1) You must state the name of all **contributors**, and of nobody but contributors.
2) You must state if your group are following the 10 ECTS course, or the 5 ECTS course, as this has an impact on how you are accessed in the course. Please also state which study program you are from (CS, Informatic, ...)
3) **Statement on Generative AI:** You must include one of the following statements on GenAI depending on which one applies to your hand-in:
    a. We have not used any Generative Artificial Intelligence tools in doing this assignment.
    b. We have used Generative Artificial Intelligence tools in doing this assignment, for the following legitimate use cases only: to get background information or understand the topic / problem, to improve writing of own text, to find gaps in our knowledge. The solution of the assignment is entirely our own.

*Please note: You do **NOT** have to use MySQL, MongoDB or Neo4j in order to solve this hand-in, and you only need to hand in your statements in a readable format, but we expect that it is very helpful for you to try it out in your MySQL workbench or in the MongoDB or Neo4j sandboxes as described below.*

---

1. SQL injection attacks

a. A product page displays items for sale based on a category ID passed in the URL as a query parameter (e.g., `?category=1`). The SQL query used to retrieve the data from the database is given below. Can you use SQL injection to retrieve all products, regardless of their category? Please give the SQL injection statement and explain how it works.

```
SELECT * FROM products WHERE category_id = $category_id;
```

b. Your website features an article commenting system that allows users to leave comments on articles. All your comments are stored in a database in the Comments table. These comments are inserted into the database using the following SQL command. Can you exploit an SQL injection vulnerability to execute an additional SQL command to remove the entire Comments table? Please give the SQL injection statement and explain how it works.

```
INSERT INTO comments (article_id, user_id, comments) VALUES (article_id, user_id, comments);
```

2. Authorization

Please write SQL authorization statements to solve the following tasks.

a. You have a database for a web application that includes a table named Users and a table named Reports.
    1. You want to grant the user Ira permission to read from and add data into table Users and allow her to pass on this permission to other users.
    2. After a security review, you've decided that a certain user, Cheng, should no longer be allowed to add data into the Reports table, but you also want to make sure that this decision does not have an impact on other users.

b. You are managing a large database with multiple users who need similar permissions. To simplify permission management, you decide to use roles. You want to create a role named Data_analyst that can read from the Sales_data and part of the Customer_info tables.
    1. Establish a Data_analyst role.
    2. Make sure any Data_analyst can read from Sales_data, and name and address from Customer_info tables.
    3. We hire a new Data_analyst named Pernille who should have the corresponding role.

3. NoSQL systems

We want to create a database on NGO supporters using a NoSQL database, specifically MongoDB. If you wish to test your code interactively you can use https://mongoplayground.net/, else you are welcome to write them in an editor of your choice. You insert data in the leftmost pane, write a query in the middle pane and the result is shown in the rightmost pane. We provide a json file 'supporter.json' with the necessary data for the supporters. Please provide MongoDB queries that do the following:

a. Retrieve all the supporters of KDG
b. Retrieve only the name and email of all supporters who are volunteers.
c. Update the NGO_name for the supporter with sid = 1 to Amnesty International
d. We here reconsider the previously used Movie dataset, this time in a graph based model in the NoSQL DBMS Neo4j. You can use the Neo4j sandbox if you would like to test

interactively: https://sandbox.neo4j.com/, else you are welcome to use an editor of your choice.. Please write a query to find the name of directors and the title of movies they directed, by using PERSON and MOVIE nodes, and the DIRECTED relationship between them.

Please handin your report as a **single pdf file**. Present your code in a **copyable format** (then your TA can try it out), i.e. avoid screenshots. If you write in Latex then you can use the **verbatim** package.
We encourage you to discuss any questions you may have in the discussion forum, but do not share solutions or solution attempts in the forum.
Please note that late hand-ins will **not** count towards the grade.