Assignment 6 - 10 ECTS

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.

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 product WHERE category_id = \$category_id;
```

Solution. I would something like the following into the URL,

```
?category=1 OR 1=1; -
```

When this is passed to the SQL query, the first statement might fail, but the OR statement always evaluates to true. This results in all products being retrieved. We have abused the fact, that the developer didn't expect an `OR` statement in the URL.

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);
```

Solution. The following SQL injection will probably results in all the comments being deleted,

```
"hello"); DROP TABLE comments; -.
```

Assuming that the comment a user leaves is inserted on the `comments` fields in `VALUES`, my code terminates the tuple, and then deletes the table with the `DROP` command. The added `-` comments out any code there might be at the end.

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.

Solution. I use the following command,

`GRANT INSERT, SELECT ON Users TO "Ira" WITN GRANT OPTION;.`

`INSERT, SELECT` gives read and write privileges, while `GRANT OPTION` allows Ira to pass her privileges on. To remove privileges from Cheng I use the following command,

`REVOKE INSERT ON Reports FROM "Cheng";`

This removes his permission to add data, and should not affect 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 name and address from 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.

Solution. We establish the role using `CREATE ROLE`,

`CREATE ROLE "Data_analyst";`

We can add privileges in the same way we add privileges to users,

```
GRANT SELECT ON Sales_data TO "Data_analyst";
```

To grant access to part of the Customer_info table we can create a view,

```
CREATE VIEW Data_analyst_customer_info AS
SELECT name, address
FROM Customer_info;
GRANT SELECT ON Data_analyst_customer_info TO "Data_analyst";
```

We could actually also have done the following,

```
GRANT SELECT (name, address) ON Customer_info TO "Data_analyst";
```

Having hired Pernille we can create a user for here and grant her the role of Data_analyst,

```
CREATE USER "Pernille";
GRANT ROLE "Data_analyst" TO "Pernille";
```

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

Solution. I use the following command,

```
db.supporter.find({
  "NGO_name": "KDG"
})
```

b. Retrieve only the name and email of all supporters who are volunteers.

Solution. I use the following command,

```
db.supporter.find({
  "volunteer": true
},
{
  "name": 1,
  "email": 1
})
```

c. Update the NGO_name for the supporter with `sid = 1` to Amnesty International

Solution. And for this one I use the following `update` command,

```
db.supporter.update({
  "sid": "1"
},
{
  $set: {
    "NGO_name": "Amnesty International"
  }
})
```

d. We here reconsider the previously used Movie dataset, this time in a graph based model in the NoSQL DBMS Neo4j. Please write 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.

Solution. And lastly I use this command,

```
MATCH (n:Person)-[r:DIRECTED]->(m:Movie) RETURN n.name as Director, m.
    title as Movie
```

This commands for relations `person -> directed -> movie` in the graph, and then returns the name of the person and the title of the movie.