from Juvan Thavalingam, Tim Müller, Christian Graber

Task 1:

1. start Burp
2. open website Schoggi
3. go to the login page
4. send a request with any USER ID and any password,
5. in Burp under Proxy History send the API Rest Request to the Reapter,
6. try a SQL injection.
7. username: ' OR 1=1#

the ' closes the first statement, and OR 1=1 enables a Boolean, which is always true.

The # comments everything after that for the SQL statment.

8. password: doesn't matter
9. enter this information in the login page and you will automatically log in as user alice.
10. for the admin use burp again with the repeater.
11. password doesn't matter again.
12. username: ' OR 1=1 LIMIT 0,1#

The LIMIT keyword is new. Limit a,b. b is the number of the table. 1 is the table of employees.

a is the offset starting with 0, which goes through the rows of employees.

13. the replayer always shows the role in the request, i.e. user or admin.
14. if you now rotate through the username ' OR 1=1 LIMIT 0,1# from 0 to 6 you will find admins.

It also fits, if you click on community at alice you will see 7 members.

The admins are: victor, peggy