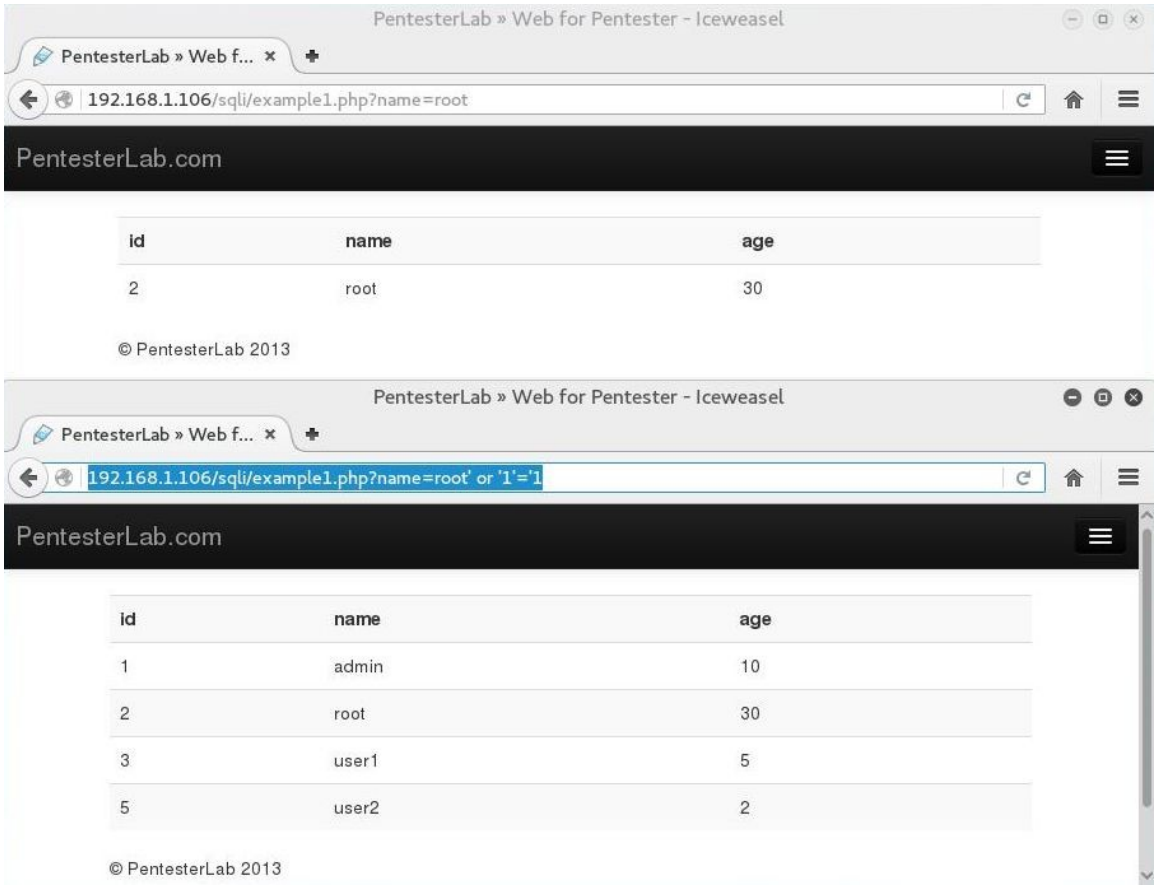
SQL Injection Solutions for "Web For Pentester"

Emre ÖVÜNÇ
İntern – İnnovera
info@emreovunc.com

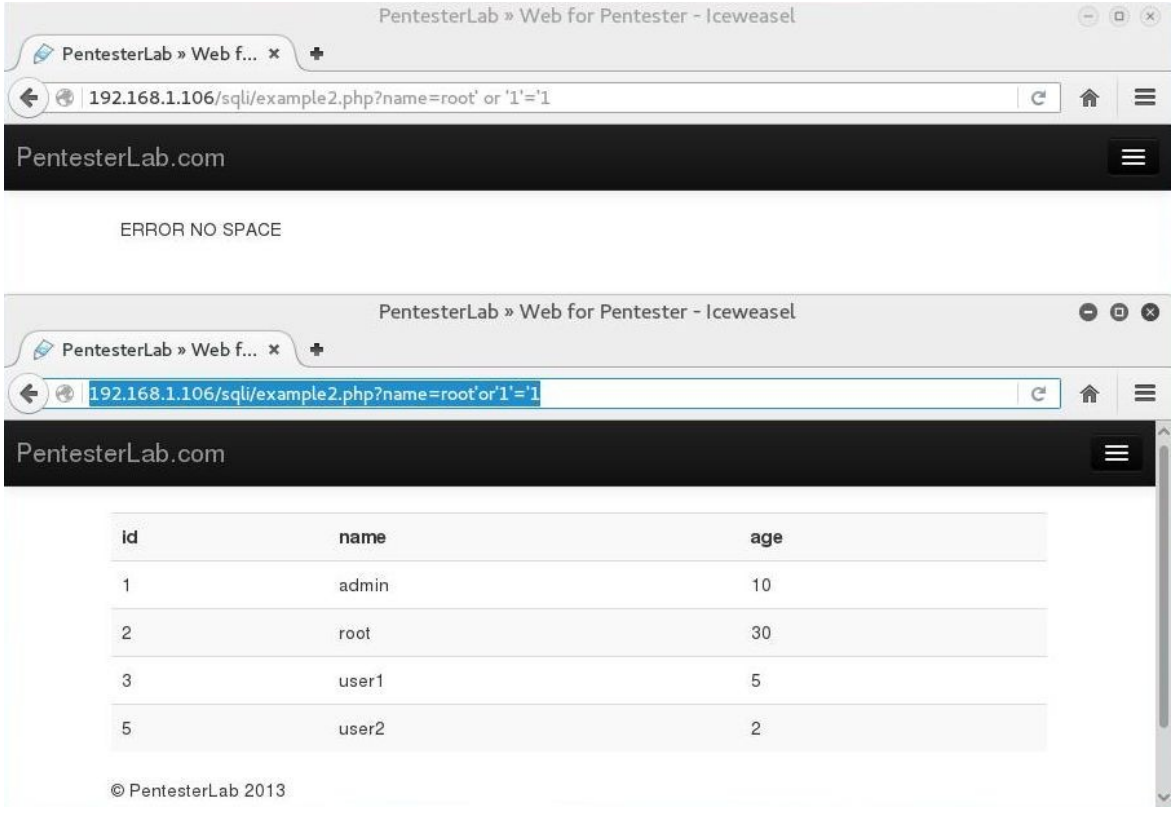
SQL Example #1:

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



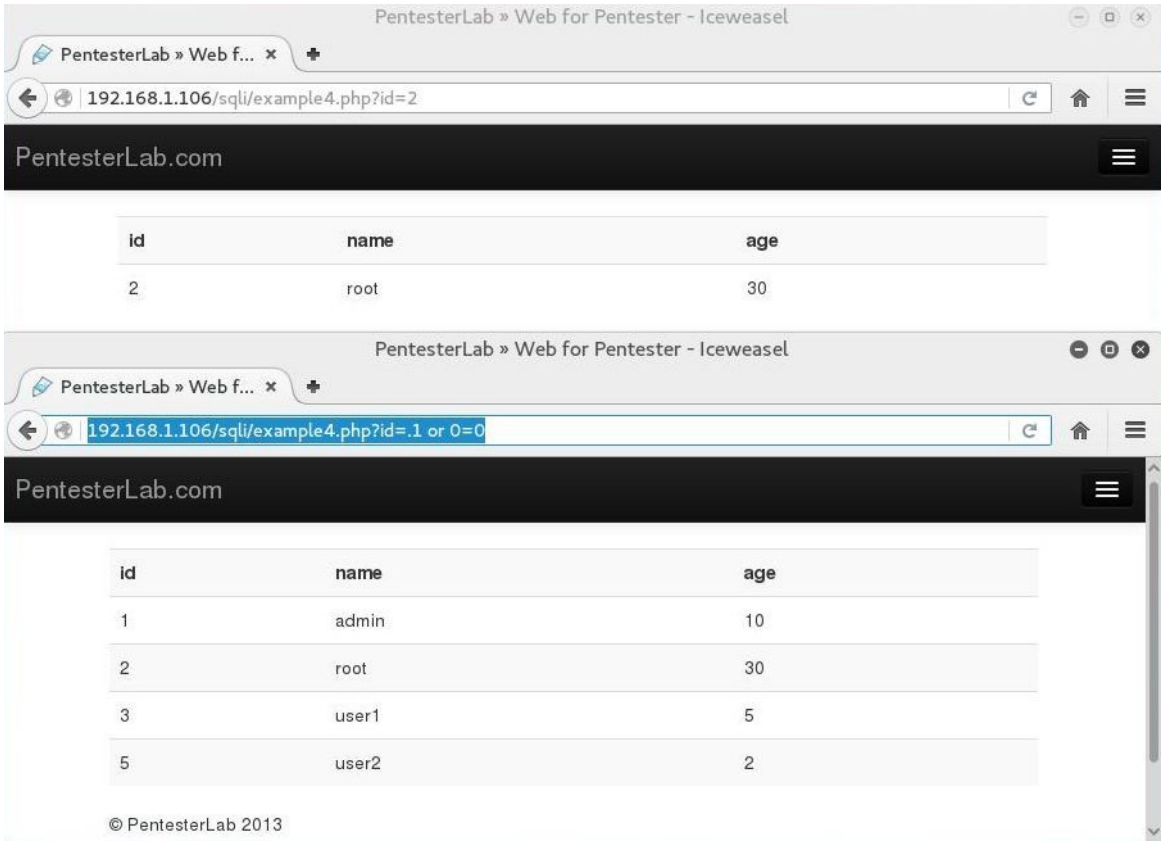
SQL Example #2 - #3:

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.



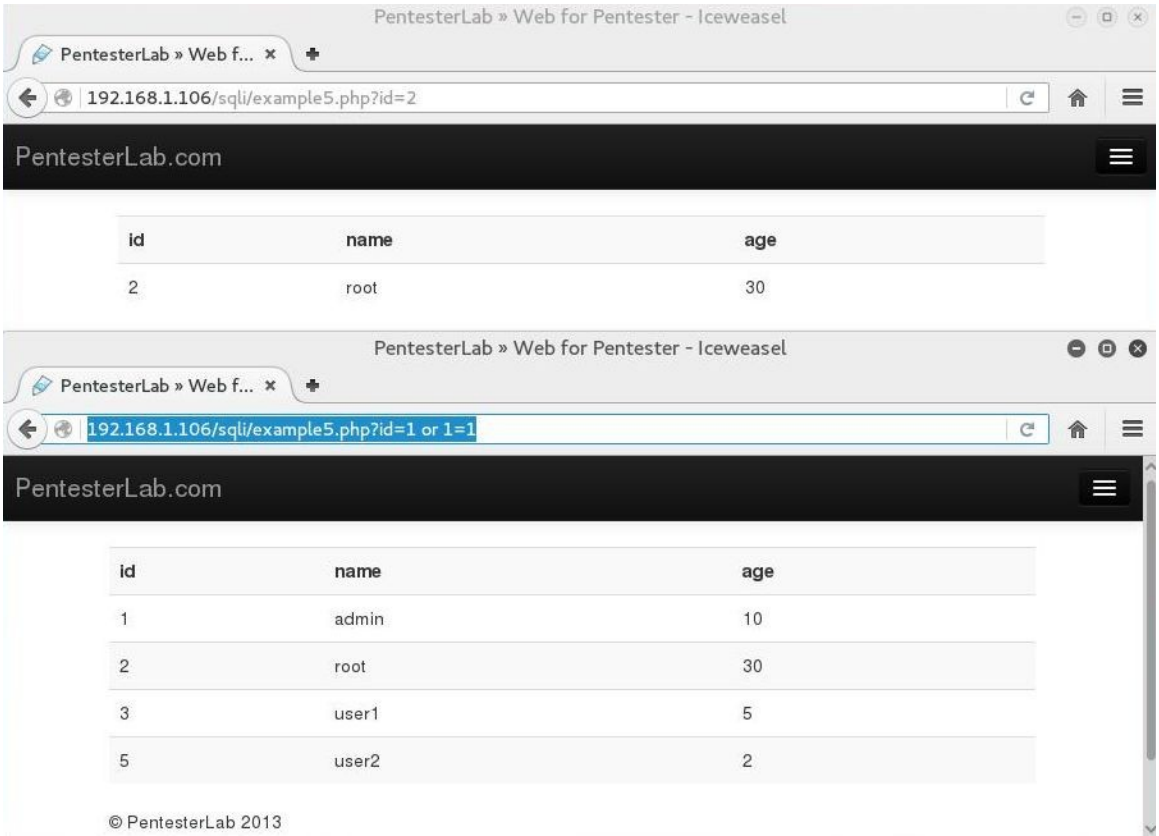
SQL Example #4:

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.



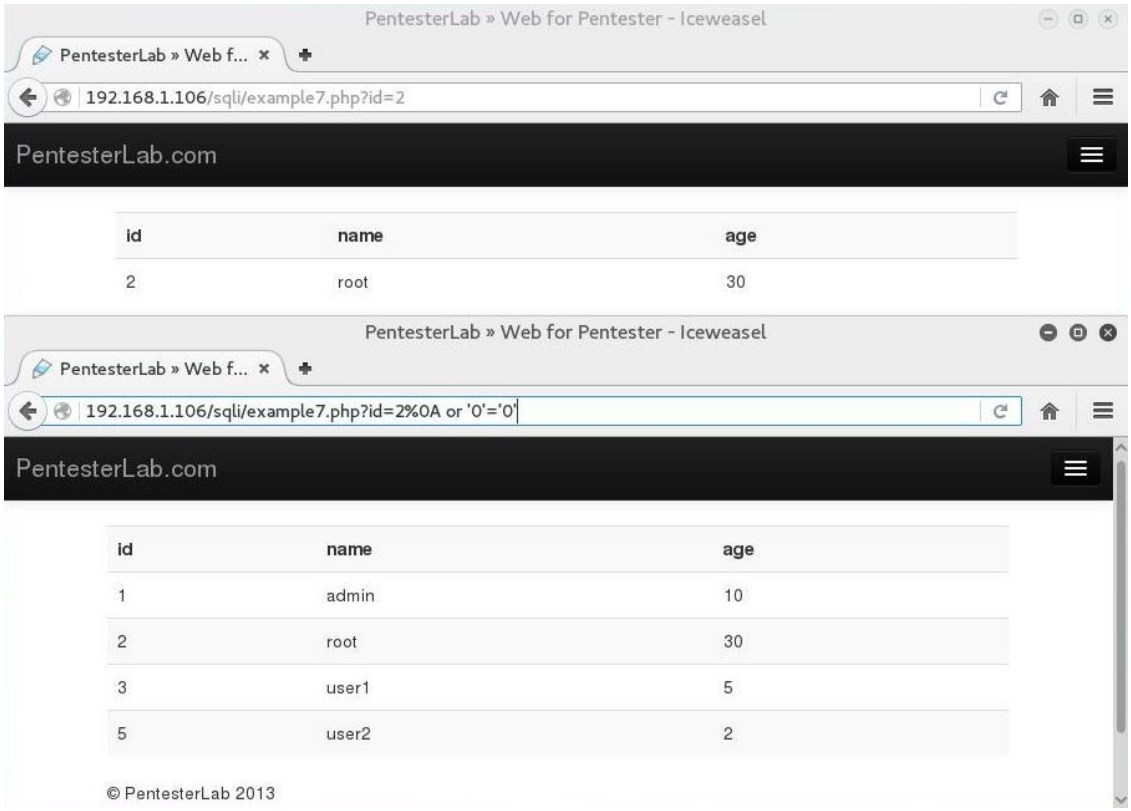
SQL-Example #5 - #6:

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.



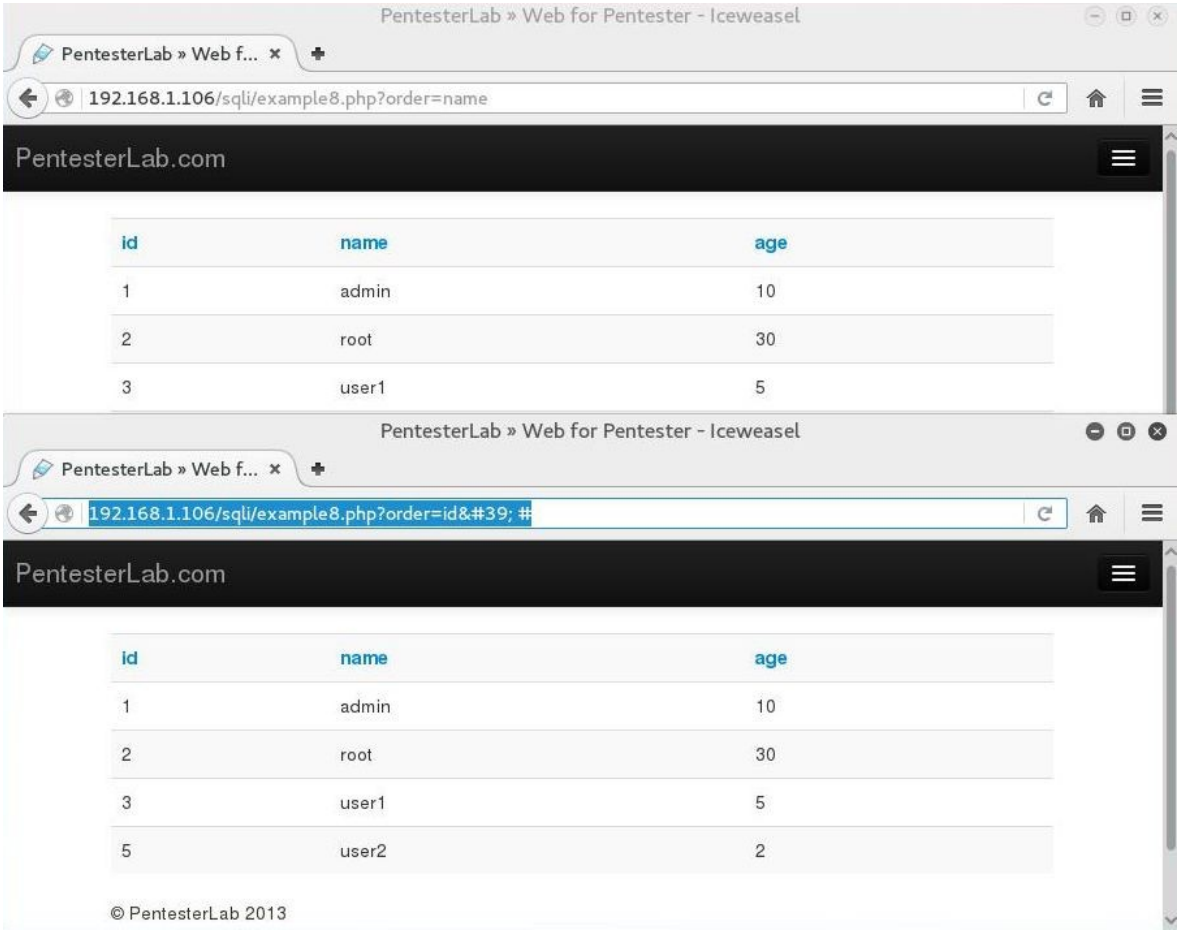
SQL-Example #7:

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 O**RDER 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.