

Forum:[Hack Forums](#)

Thread: [\[TUT\]Make your own SQLI Lab and and practice \[TUT\]](#)

Aakash Choudhary - June 12, 2015, 9:39 am

Hi friends i am CodeNinja a.k.a. Aakash Choudhary. Today i will help you to make your own sqli lab where you can practice sql injection in your localhost.

Requirement :-

1. XAMPP/LAMPP
2. Basic knowledge of PHP & MySQL

NOTE: Save all this files in you localhost folder.

Step 1:- Here is my code of sql --->

PHP Code

```
<?php
```

```
-- phpMyAdmin SQL Dump
```

```
-- version 4.2.11
```

```
-- http://www.phpmyadmin.net
```

```
--
```

```
-- Host: localhost
```

```
-- Generation Time: Jun 12, 2015 at 05:22 PM
```

```
-- Server version: 5.6.21
```

```
-- PHP Version: 5.6.3
```

```
SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
```

```
SET time_zone = "+00:00";
```

```
/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
```

```
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
```

```
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
```

```
/*!40101 SET NAMES utf8 */;
```

```
--
```

```
-- Database: `webtest`
```

```
--
```

```
-- -----
```

```
--
```

```
-- Table structure for table `students`
```

```
--
```

```
CREATE TABLE IF NOT EXISTS `students` (
```

```
  `id` int(6) NOT NULL,
```

```
  `firstname` varchar(30) NOT NULL,
```

```
  `lastname` varchar(30) NOT NULL,
```

```
  `email` varchar(50) DEFAULT NULL,
```

```
`password` varchar(20) NOT NULL
) ENGINE=InnoDB AUTO_INCREMENT=7 DEFAULT CHARSET=latin1;
```

```
--
-- Dumping data for table `students`
--
```

```
INSERT INTO `students` (`id`, `firstname`, `lastname`, `email`, `password`) VALUES
(1, 'Mak', 'Man', 'makman@gmail.com', 'pass1'),
(2, 'Code', 'Ninja', 'code@gmail.com', 'pass2'),
(3, 'Aakash', 'Choudhary', 'aakash@gmail.com', 'pass3'),
(4, 'Anil', 'Kid', 'anil@gmail.com', 'pass4'),
(5, 'Saqu', 'Brother', 'saqu@gmail.com', 'pass5'),
(6, 'Zen', 'Javanicus', 'zen@gmail.com', 'pass6');
```

```
--
-- Indexes for dumped tables
--
```

```
--
-- Indexes for table `students`
--
```

```
ALTER TABLE `students`
ADD PRIMARY KEY (`id`);
```

```
--
-- AUTO_INCREMENT for dumped tables
--
```

```
--
-- AUTO_INCREMENT for table `students`
--
```

```
ALTER TABLE `students`
MODIFY `id` int(6) NOT NULL AUTO_INCREMENT,AUTO_INCREMENT=7;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
```

Save this file as "webtest.sql"

If you want to create database, tables, columns and insert data yourself with code then here is some codes but always remind that it is only for to increase your knowledge in MySQL ?

Some commands for Basic of mysql with example :-

1. Create Database :-

Code CREATE DATABASE webtest; This will create database.

2. Create Tables :-

Code CREATE TABLE `students` (
`id` int(6) NOT NULL AUTO_INCREMENT PRIMARY KEY,
`firstname` varchar(30) NOT NULL,

```
`lastname` varchar(30) NOT NULL,
`email` varchar(50) DEFAULT NULL,
`password` varchar(20) NOT NULL
)
```

Here i create "student" table and 5 columns -----> "id","firstname","lastname","email","password"

& int(6) mean id is integer value with 6 length

& varchar(30) mean we take name with 30 length

& AUTO_INCREMENT mean it will increment id value automatic like 1,2,3 etc etc

& PRIMARY KEY mean id is our primary key (main key)

3.Insert our data in those columns :-

Code INSERT INTO `students` (`id`, `firstname`, `lastname`, `email`, `password`) VALUES

(1, 'Mak', 'Man', 'makman@gmail.com', 'pass1'),

(2, 'Code', 'Ninja', 'code@gmail.com', 'pass2'),

(3, 'Aakash', 'Choudhary', 'aakash@gmail.com', 'pass3'),

(4, 'Anil', 'Kid', 'anil@gmail.com', 'pass4'),

(5, 'Saqu', 'Brother', 'saqu@gmail.com', 'pass5'),

(6, 'Zen', 'Javanicus', 'zen@gmail.com', 'pass6'); So we insert our data in student table with those values.

So this is all which we can do manually but i have given you my sql file to save your time. ?

Step 2 :- Make a php file and save following codes in that

PHP Code

```
<?php
```

```
include("connection.php"); // This is your connection file
```

```
if(isset($_GET["id"])) {
```

```
    $id = $_GET["id"];
```

```
    $query = $conn->query("SELECT * FROM students WHERE id=$id
```

```
"); // Here student is our database name
```

```
    if(!$query) { // If this query is not running then you will see error
```

```
        echo "Error: " . mysqli_error($conn);
```

```
    } else {
```

```
        $data = mysqli_fetch_assoc($query);
```

```
        echo "<h3 style='text-align:center; -webkit-background-clip: text, border;
```

```
background-clip: text, border;
```

```
-webkit-text-stroke: 5px rgba(101, 86, 65, 0.2);font-size:40px;color:#436b95;'> " . $data["firstname"]
."<br><br>". $data["lastname"] . "</h3>";
```

```
/*Here we are fetching data from query like firstname and lastname.It is your wish what you want to fetch data whether it is email,password or something else.*/
```

```
    }
```

```
    } else {
```

```
        echo "<p>Please input the ID as parameter with numeric value like -> ?id=1</p>";
```

```
    }
```

```
?>
```

Save this php file as "integer.php"

Step 3 :- Make another php file and save following codes in php file

PHP Code

```
<?php
```

```
$servername = "localhost";  
$username = "root";  
$password = "You Password Here"; //Set your password here if have  
$database = "webtest"; // This is our database name.
```

```
//create connection  
$conn = new mysqli($servername,$username,$password,$database);
```

```
//check connection  
if ($conn->connect_error){  
    die("Connection failed: " . $conn->connect_error);  
}
```

```
?>
```

Save this file as "connection.php" .

Now browse your localhost in your browser ---> <http://localhost/lab/integer.php?id=1>

and you will see page.

Now if you want practice string based sql injection then just change following line :-

PHP Code

```
<?php
```

```
$query = $conn->query("SELECT * FROM students WHERE id=$id");
```

with this

PHP Code

```
<?php
```

```
$query = $conn->query(" SELECT * FROM students WHERE id= '$id' ");
```

Notice :- id = ' \$id ' <===== I use quoted to make it string based.

So when you type :- id=1' order by 100--+ then you will see error by putting ' so it is string based.

Now if you want to practice with double quation (") instead of single (') then here is the code :-

PHP Code

```
<?php
```

```
$id = "" . $_GET["id"] . "";
```

```
$query = $conn->query(" SELECT * FROM students WHERE id= ($id) ");
```

Here if you type :- id=1") order by 100--+ then you will see error otherwise not if you use id=1') order by 100--+

So this is small tutorial for you so enjoy this.

Also if you have any question, problem and if i have done any mistake then tell me. Next time i will tell about putting WAF when i learn it completely. Thanks ? ?

Hope you like it.

Th3PonyWizard - June 12, 2015, 10:23 am

A very nice tutorial. However, I don't want people taking this as an excuse to avoid learning PHP / SQL.

saheenshoukath - June 13, 2015, 12:29 am

N9c tut CodeNinja.Thanks for sharing ur knowledge :)

ketankul.2010 - June 14, 2015, 12:57 am

setting dis lab in my arch <3 .thnx buddy.

•^v^-[bLacKn3x]-^v^• - June 21, 2015, 1:04 pm

when i open localhost/integer.php?id=1 i get only white page .what is my problem?

Dum De Dum - June 21, 2015, 7:11 pm

Nice tut, it's a nice easy way to practice for all new people.

Aakash_Choudhary - June 22, 2015, 12:03 am

(Jun 21, 2015 01:04 PM)Blacknex158 Wrote: [\[CITE\]](#) when i open localhost/integer.php?id=1 i get only white page .what is my problem?

PM me for get my skype. Then i will help you live

NIIGHT HAWKE - June 24, 2015, 11:10 am

Nice tutorial, keep the good work upcoming.

•^v^-[bLacKn3x]-^v^• - June 24, 2015, 12:43 pm

okay now i got it .you forgot in your code include("connection.php") .

Thanks for that it helps me a lot for understanding this more

xx 0x0 xx - June 24, 2015, 6:10 pm

this is good tutorial for who wanna be injector i like it nice work dude

zoombierobo - September 19, 2015, 7:50 am

Thank you very much for this. I got idea to make vulnerable web application now. :D

Aakash_Choudhary - April 8, 2016, 2:07 am

Posting so that many beginners learn from my tutorial

Thanks

indianehacker - April 17, 2017, 3:55 am

good job.....

mutybyte - July 24, 2017, 3:55 am

Wow thank you for this tutorial. Once i learn php and mysql i will use this tutorial. Bookmarked it.

My mentor told me to learn php and mysql and then build vulnerable application so i searched in forum and got this awesome tutorial. Don't know why he is no active ?

ronnyprice - July 24, 2017, 11:09 am

Thanks for this! Trying to learn PHP and SQL but this definitely helps me feel like I can actually use my skills, in the interim.