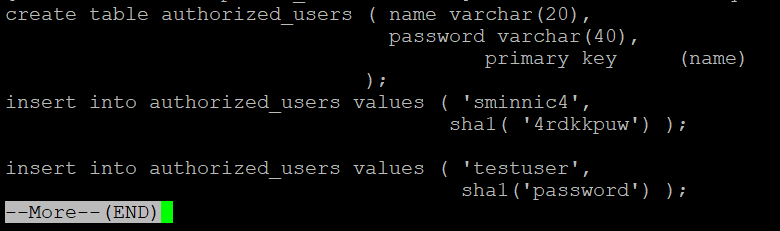
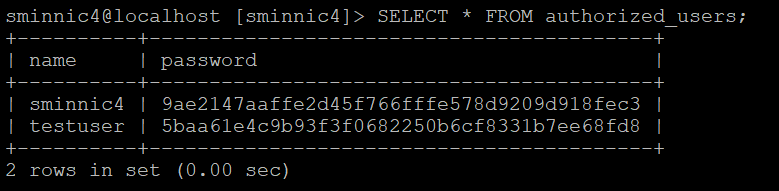


<http://et791.ni.utoledo.edu/~sminnic4/cset3300/secretdb.php>

sminnic4  
4rdkkpuw  
  
  


<?php

$name = $\_POST['name'];

$password = $\_POST['password'];

if ((!isset($name)) || (!isset($password))) {

//Visitor needs to enter a name and password

?>

<h1>Please Log In</h1>

<p>This page is secret.</p>

<form method="post" action="secretdb.php">

<p>Username: <input type="text" name="name"></p>

<p>Password: <input type="text" name="password"></p>

<p><input type="submit" name="submit" value="Log In"></p>

</form>

<?php

} else {

// connect to mysql

$mysql = mysqli\_connect("localhost", "sminnic4", "4rdkkpuw");

// $mysql = new mysqli("localhost", "sminnic4", "4rdkkpuw", "sminnic4");

if (mysqli\_connect\_errno()){

printf("Connect failed: %s/n", mysqli\_connect\_error());

exit();

}

if(!$mysql) {

echo "Cannot connect to database.";

exit;

}

// select the appropriate database

$selected = mysqli\_select\_db($mysql, "sminnic4");

// $selected = mysqli\_select\_db("sminnic4", $mysql);

if(!$selected) {

echo "Cannot select database.";

exit;

}

$password1=mysqli\_real\_escape\_string($mysql,$password);

// query the database to see if there is a record which matches

$query = "select count(\*) from authorized\_users where

name = '".$name."' and

password = sha1('".$password."')";

$result = mysqli\_query($mysql, $query);

if(!$result) {

echo "Cannot run query.";

exit;

}

$row = mysqli\_fetch\_row($result);

$count = $row[0];

if ($count > 0) {

// visitor's name and password combination are correct

echo "<h1>Here it is!</h1>

<p>I bet you are glad you can see this secret page.</p>";

} else {

// visitor's name and password combination are not correct

echo "<h1>Go Away!</h1>

<p>You are not authorized to use this resource.</p>";

}

}

?>