Practical Lab 6

Student ID: _____ Student Name: _____

Q1. Test the following codes to hash a message.

Test demo1 here: Demo 1

1. Download **sha256.js** from the here and put under your student folder.
2. Link **sha256.js** file, see first highlight part
3. Call **sha256 hash function** and hash the user input, see second highlight part

```
<html>
	<body>

	<h1>Lab 6 Demo 1</h1>

	<input name="input" id="input" type="text" >
	<br/><br/>
	<button type="button" onclick="hash()">Hash</button>
	<br/><br/>

	<h3>Hash value</h3>
	<p name="hash_value" id="hash_value"></p>


	<!-- refer to the js file, which contains sha256 hash function-->
	<script src="js/sha256.js"></script>

	<script type="text/javascript">
		// Demo code
		function hash() {
			// get user input
			var input = document.getElementById('input').value;

			// call sha256 hash function
			var hash = SHA256.hash(input);

			// print on the screen
			document.getElementById('hash_value').innerHTML = hash;
		}
	</script>

	</body>
</html>
```

Think: 1. refer a js file in different folder.
2. Try different messages and see the hash results
   2.1. When you enter the same messages, the hash value must be the same
   2.2. When you enter different messages, the hash values must be different

Q2. Test the following codes to save a **hash value** into the "database".

Based on the answers of previous lab (Lab 5), test Demo2 here: Demo 2

1. Create an empty txt file named: database.txt, set the permission as 777
2. Copy and paste the below code to create a HTML file as client.html, permission as 755
3. Copy and paste the below code to create a PHP file as server.php, permission as 755
4. Go to titan.csit.rmit.edu.au/~sXXXXXXX/…/client.html

client.html

```
<html>
<body>
    <h2>Lab 6 Demo 2</h2>
    <form action="../server/server.php" method="POST">

    Enter: <input type="text" name="input" id="input">
    <br/><br/>
    <button type="submit" onclick="hash()">Submit</button>
    </form>

    <script src="js/sha256.js"></script>
    <script type="text/javascript">
        function hash() {
            var input = document.getElementById('input').value;
            var hash = SHA256.hash(input);
            document.getElementById("input").value = hash;
        }
    </script>
</body>
</html>
```

server.php

```
<html>
<body>
    <?php
        //Receive user input from clint side
        $user_input = $_POST['input'];

        //open the database file named "database.txt"
        $file = fopen("../database/database.txt","a");
        //insert $user_input into the database.txt
        fwrite($file, $user_input."\n");
        //close the "$file"
        fclose($file);

        echo "The hash value has been added to the
    database/database.txt";
    ?>
</body>
</html>
```

Q3. Based on Q1, Q2, update the answers of Lab 5, which contains register.html, register.php, login.html, login.php, users.txt and sha256.js to achieve the following:

Expected outcome: users' passwords have been hashed before saved in the database

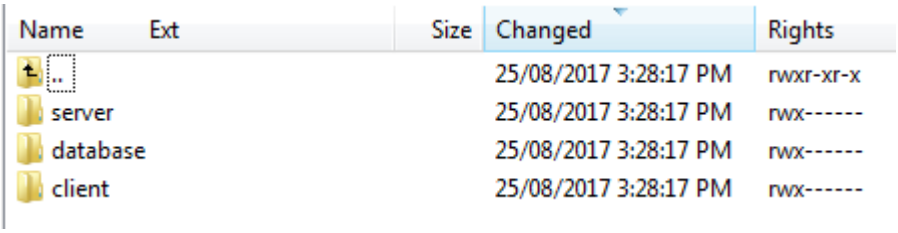
Register:

1. Go to register.html, and enter username and password
2. Go back to check users.txt, the password has been hashed.
3. Username is remained as plaintext, and also do not allow the same user (with same username) to register.

Login:

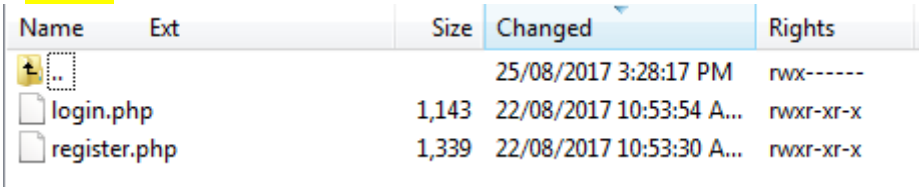
1. Go to login.html
2. Enter the username and password
3. Entered password is hashed before submitted the form
4. Compare the hash values to verify the user

According to Q2, create the folders/files as below:



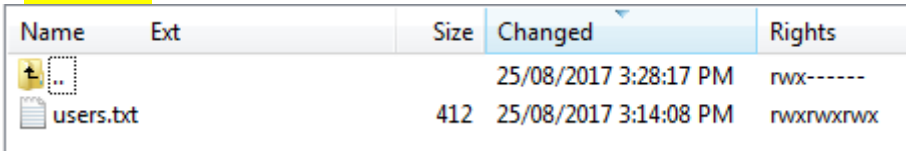
Name	Ext	Size	Changed	Rights
..			25/08/2017 3:28:17 PM	rwxr-xr-x
server			25/08/2017 3:28:17 PM	rwx------
database			25/08/2017 3:28:17 PM	rwx------
client			25/08/2017 3:28:17 PM	rwx------

in the folder server:



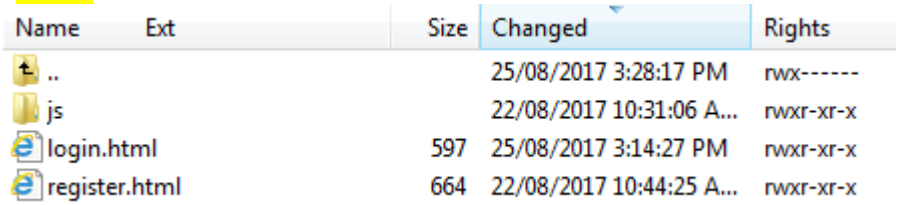
Name	Ext	Size	Changed	Rights
..			25/08/2017 3:28:17 PM	rwx------
login.php		1,143	22/08/2017 10:53:54 A...	rwxr-xr-x
register.php		1,339	22/08/2017 10:53:30 A...	rwxr-xr-x

in the folder database:



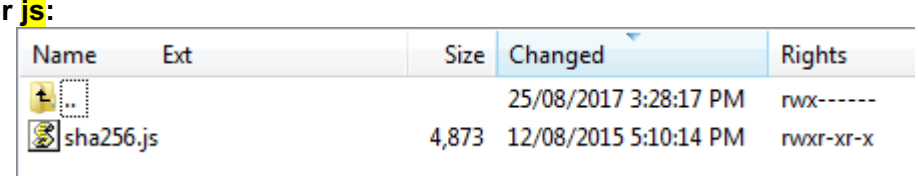
Name	Ext	Size	Changed	Rights
..			25/08/2017 3:28:17 PM	rwx------
users.txt		412	25/08/2017 3:14:08 PM	rwxrwxrwx

in the folder client:



Name	Ext	Size	Changed	Rights
..			25/08/2017 3:28:17 PM	rwx------
js			22/08/2017 10:31:06 A...	rwxr-xr-x
login.html		597	25/08/2017 3:14:27 PM	rwxr-xr-x
register.html		664	22/08/2017 10:44:25 A...	rwxr-xr-x

in the folder js:



Name	Ext	Size	Changed	Rights
..			25/08/2017 3:28:17 PM	rwx------
sha256.js		4,873	12/08/2015 5:10:14 PM	rwxr-xr-x

Step 1. Update register.html, enter the username and password, such as "**USER1**" and "**PASSWORD1**", "**USER2**" and "**PASSWORD2**" and "**USER3**" and "**PASSWORD3**".

Try

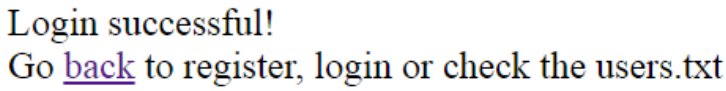
Check users.txt as below:

```
USER1,244f28ce3685167745ad3a7f1760fd4483bbbb3fd150b9087b95442d4d6fd905
USER2,0a7a1850dbb368d88236b608da9367c738f825b11dd9fc297c79303f468dd9b8
USER3,73712c8fc5cad6236491c625484b3338cacb7ba72cad941d6432d0ad8cb07f8c
```

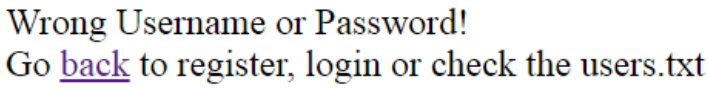
Please note: if you entered as "**USER1**" and "**PASSWORD1**", "**USER2**" and "**PASSWORD2**" and "**USER3**" and "**PASSWORD3**", it must be the same result as above in the users.txt.

Step 2. Update login.html to achieve previous login functions

Case 1: enter correct username and password



Case 2: enter incorrect username or password



Step 3. Update login.html and register.html the **action="..."** part (refer to highlight part 1 of **Q2**)
Update login.php and register.php the **fopen(…)** part (refer to highlight part 2 of **Q2**)

Answer of Q3:

register.html

```
<html>
<body>

<h2>Lab 6 Register</h2>

<form action="../server/register.php" method="POST">
Username: <input type="text" name="username" id="username">
<br/><br/>
Password: <input type="password" name="password" id="password">
<br/><br/>
<button type="submit" onclick="hashPassword()">Submit to register</button>
</form>

<script src="js/sha256.js"></script>
<script type="text/javascript">
		function hashPassword() {
			var input = document.getElementById('password').value;
			var hash = SHA256.hash(input);
			document.getElementById("password").innerHTML = hash;
			document.getElementById("password").value = hash;
		}
</script>
</body>
</html>
```

login.html

```
<html>
<body>

<h2>Lab 6 Login</h2>

<form action="../server/login.php" method="POST">
Username: <input type="text" name="username" id="username">
<br/><br/>
Password: <input type="password" name="password" id="password">
<br/><br/>
<button type="submit" onclick="hashPassword()">Submit to Login</button>
</form>

<script src="js/sha256.js"></script>
<script type="text/javascript">
		function hashPassword() {
			var input = document.getElementById('password').value;
			var hash = SHA256.hash(input);
			document.getElementById("password").value = hash;
		}
</script>
</body>
</html>
```