1. User puts in “MemberId” & Password
2. Password (on user end)
   1. PHP asks the database for salt  
      SELECT Salt FROM UserAccount WHERE MemberId = input.MemberId
   2. Database returns the salt (specifically for that member)
   3. PHP hashes input.Password  
      string $hash (“sha256”, input.Password, FALSE)
3. Password to DB
   1. PHP asks DB for public key  
      SELECT public FROM key
   2. $hash gets encrypted with public key (referred to as $message; Luis will get you algorithm)
   3. $message is sent to database (with public key encryption)  
      EXEC [command($message)]
4. DB returns true or false
   1. If true, password is correct; check if admin/reg
      1. If admin go to admin page
      2. If reg go to reg page
   2. If flase, password is incorrect

--------

TO CONNECT AND QUERY THE DB From PHP

**Connection** to the MARIADB database:

<?php

$servername = "localhost";

$username = "username";

$password = "password";

// Create connection

*//W3schools for mysql...*

$con = new mysqli($servername, $username, $password);

*//One.com suggests...*

$con = mysqli\_connect($servername, $username, $password);

// Check connection

if ($con->connect\_error) {

die("Connection failed: " . $con->connect\_error);

}

echo "Connected successfully";

?>

**To Query** the MARIADB database

(it’s for MYSQL; so, doublecheck it works for MariaDB):

$sql = "SELECT id, firstname, lastname FROM MyGuests";

$result = $con->query($sql);

if ($result->num\_rows > 0) {

// output data of each row

while($row = $result->fetch\_assoc()) {

echo "id: " . $row["id"]. " - Name: " . $row["firstname"]. " " . $row["lastname"]. "<br>";

}

} else {

echo "0 results";

}

$con->close();

?>