DATABASE & SYSTEM SECURITY

LAB-12

12. Hashing Data in Transit 2

Date of the Session:____/___/____ **Time of the Session:______to_______**

Learning Outcomes:

- **To understand and implement the concept of hashing using Oracle.**
- **To understand and implement the concept of hashing data in transit in Oracle.**

Pre-Lab:

Q1.What are temporal data types in Oracle?

Sol)

Oracle provides the following categories of data types to represent temporal data inside an Oracle database:

The DATE data type.

The TIMESTAMP data types: TIMESTAMP. TIMESTAMP WITH TIME ZONE. TIMESTAMP WITH LOCAL TIME ZONE.

The INTERVAL data types: INTERVAL YEAR TO MONTH. INTERVAL DAY TO SECOND.

Q2. What is VArray?

Sol) The varray (variable size array) is one of the three types of collections in PL/SQL (associative array, nested table, varray). The varray's key distinguishing feature is that when you declare a varray type, you specify the maximum number of elements that can be defined in the varray.

Q3. What is the difference between rename and alias?

Sol) Rename is actually changing the name of an object whereas Alias is giving another name (additional name) to an existing object. Rename is a permanent name given to a table or column whereas Alias is a temporary name given to a table or column which do not exist once the SQL statement is executed.

Q4. Can we store pictures in the database and if so, how it can be done?

Sol) A database gives you the opportunity to store photos and other small images in a database table. You can create such a database table for example when you want to create an online photo album with descriptions of your photos. Storing images in a database table is not recommended.

Q5. What is hash cluster?

Sol) A hash cluster provides an alternative to a non-clustered table with an index or an index cluster. With an indexed table or index cluster, Oracle Database locates the rows in a table using key values that the database stores in a separate index. To use hashing, you create a hash cluster and load tables into it.

In-Lab:

Q1. You are a database security consultant for a company. The company has given you the task of creating a page which takes username, message, gender and place as inputs and stores the hashed value of the message, gender, place in a database table. You plan to store the hash values of the message, gender, place in the database. The hashing is done using MD5. You are to implement this using Javascript.

First, create a html page with the username, message, genderand place fields. Once the details are given as input and submit button is pressed, the javascript program in the background will hash the message, gender, place and store it in the database along with the username and original value of message, gender, place.

Create a table called 'dbusers22' to store the credentials. ***Sol)***

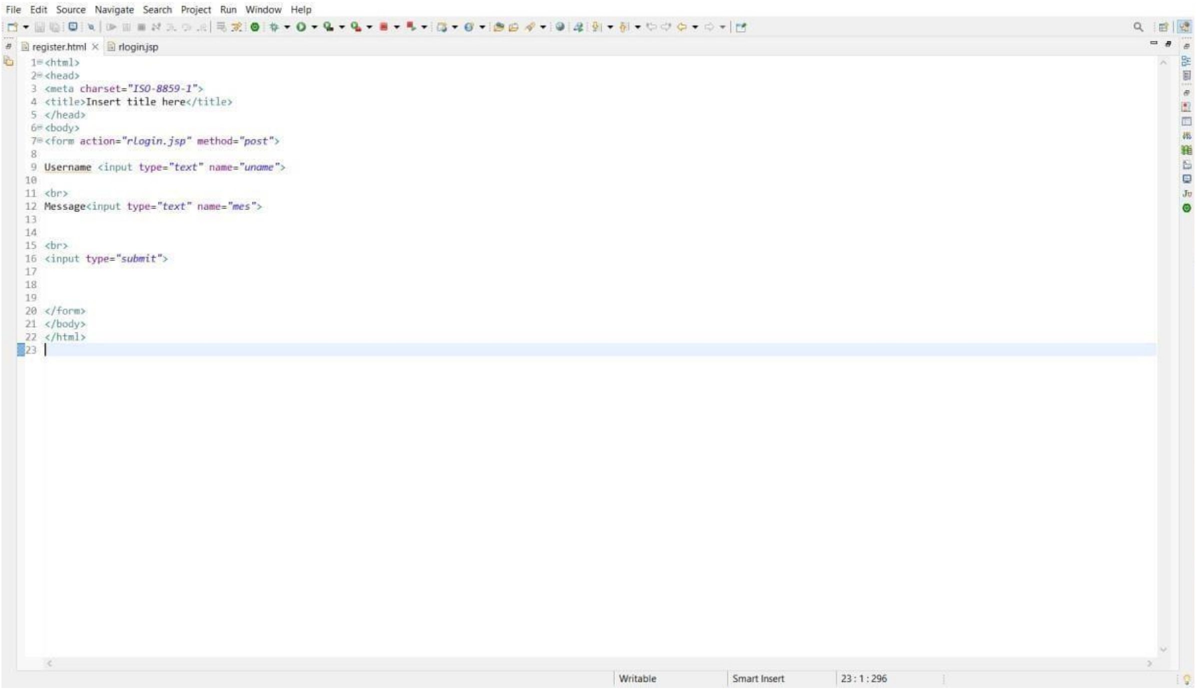
1. Connect as system to sqlplus and create the 'dbusers10' table. **create table dbusers10(username varchar2(20), message varchar2(20), emsg varchar2(50), euser varchar2(50));**
2. Switch on the Eclipse IDE.

   Go to 'File' → New → Other → Scroll down to 'Web' → Expand the folder and choose 'Dynamic Web Project'.
3. Set project name as something of your choice.
4. Choose 'Dynamic web module version' as 2.5.
5. Click Finish.
6. Then expand the project file in 'Project Explorer'. Expand 'WebContent' → WEB-INF → Right click on 'lib' → Build Path… → Configure Build Path… → Click on 'Classpath' → Click 'Add External JARs…' → Navigate to the 'ojdbc14.jar' and add it.
7. Then right click on 'WebContent'. This is where you make your html and jsp files.

   Right click on 'WebContent' → New → HTML File.

   Give a filename and end it with '.html' extension. Press Finish. **register.html**

```
<html>
<head>
<meta charset="ISO-8859-1">
<title>Insert title here</title>
</head>
<body>
<form action="rlogin.jsp" method="post">

Username <input type="text" name="uname">

<br>
Message<input type="text" name="mes">


<br>
<input type="submit">


</form>
</body>
        </html>
```



```
<html>
<head>
<meta charset="ISO-8859-1">
<title>Insert title here</title>
</head>
<body>
<form action="rlogin.jsp" method="post">

Username <input type="text" name="uname">

<br>
Message<input type="text" name="mes">


<br>
<input type="submit">



</form>
</body>
</html>

```

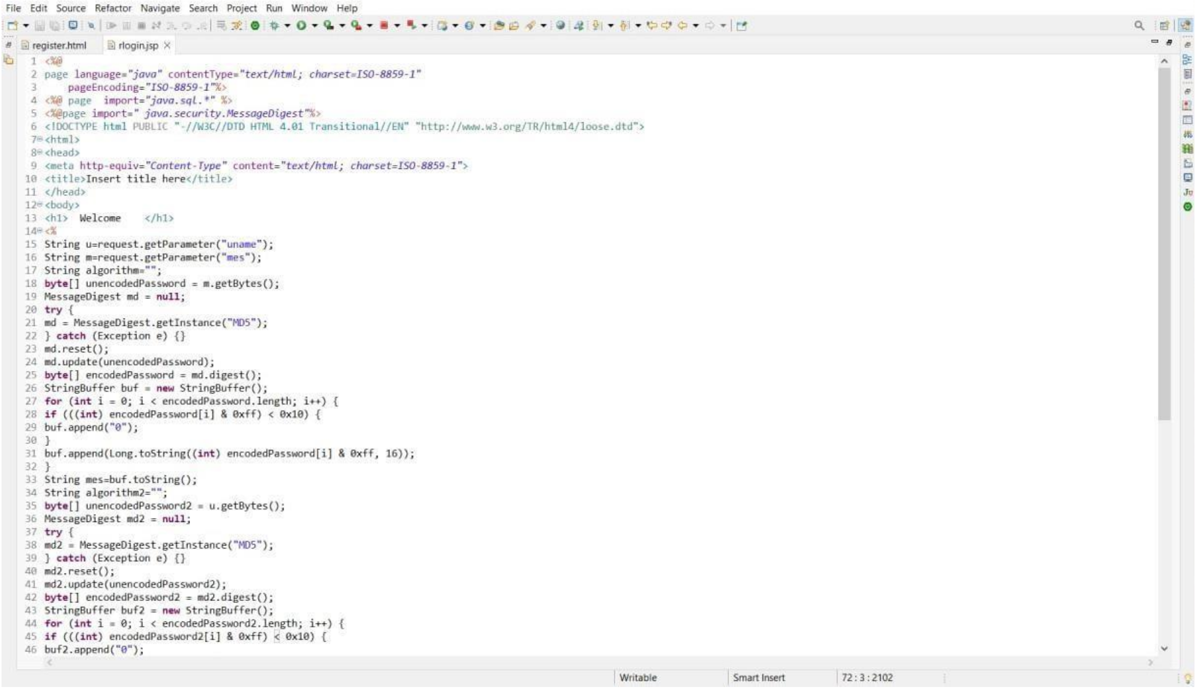
---Save

the file.

8. Right click on ‘WebContent’ → New → JSP File.

Give a filename and end it with ‘.jsp’ extension. Press Finish. **rlogin.jsp**

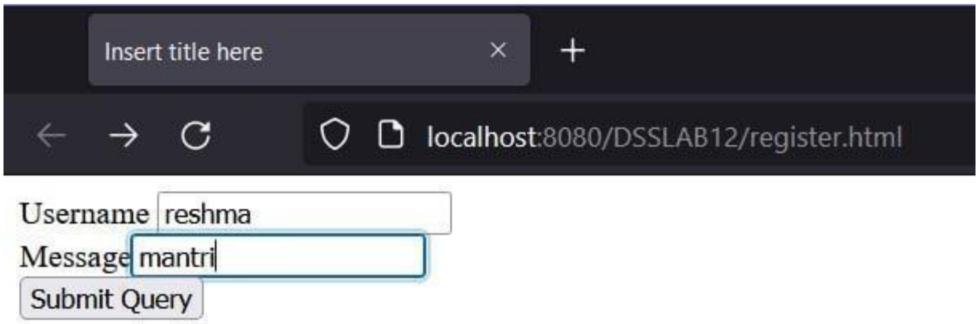
```
----------------------------

<%@
page language="java" contentType="text/html; charset=ISO-8859-1"
pageEncoding="ISO-8859-1"%>

<%@ page  import="java.sql.*" %>
<%@page import=" java.security.MessageDigest"%>

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<title>Insert title here</title>
</head>
<body>
<h1>  Welcome    </h1>

<%



String u=request.getParameter("uname");

String m=request.getParameter("mes");

String algorithm="";
byte[] unencodedPassword = m.getBytes();
MessageDigest md = null; try
{
md = MessageDigest.getInstance("MD5");
} catch (Exception e) {} md.reset();
md.update(unencodedPassword); byte[]
encodedPassword = md.digest(); StringBuffer buf =
new StringBuffer(); for (int i = 0; i <
encodedPassword.length; i++) { if (((int)
encodedPassword[i] & 0xff) < 0x10) {
buf.append("0");
} buf.append(Long.toString((int) encodedPassword[i] & 0xff,
16));
}
String mes=buf.toString();

String algorithm2="";
byte[] unencodedPassword2 = u.getBytes();
MessageDigest md2 = null; try
{
md2 = MessageDigest.getInstance("MD5");
} catch (Exception e) {} md2.reset();
md2.update(unencodedPassword2); byte[]
encodedPassword2 = md2.digest(); StringBuffer buf2
= new StringBuffer(); for (int i = 0; i <
encodedPassword2.length; i++) { if (((int)
encodedPassword2[i] & 0xff) < 0x10) {
buf2.append("0");
}
buf2.append(Long.toString((int) encodedPassword2[i] & 0xff, 16)); }
String usern=buf2.toString();

out.println(u +"----"+m); try
{

          Class.forName("oracle.jdbc.driver.OracleDriver");



          Connection
con=DriverManager.getConnection("jdbc:oracle:thin:@localhost:1521:xe","system","syste
m");

          PreparedStatement ps=con.prepareStatement("insert into dbusers10
values(?,?,?,?)");           ps.setString(1,u);        ps.setString(2,m);
   ps.setString(3,mes);      ps.setString(4,usern);
int a=ps.executeUpdate();

out.println(a+ "  Record Inserted Successfully");
}
catch(Exception e)
{
       out.println(e);

}

%>

</body>
</html>
```


File Edit Source Refactor Navigate Search Project Run Window Help
register.html
rlogin.jsp
Writable
Smart Insert
72 : 3 : 2102

```
<%@
page language="java" contentType="text/html; charset=ISO-8859-1"
    pageEncoding="ISO-8859-1"%>
<%@ page  import="java.sql.*" %>
<%@page import=" java.security.MessageDigest"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<title>Insert title here</title>
</head>
<body>
<h1>  Welcome    </h1>
<%
String u=request.getParameter("uname");
String m=request.getParameter("mes");
String algorithm="";
byte[] unencodedPassword = m.getBytes();
MessageDigest md = null;
try {
md = MessageDigest.getInstance("MD5");
} catch (Exception e) {}
md.reset();
md.update(unencodedPassword);
byte[] encodedPassword = md.digest();
StringBuffer buf = new StringBuffer();
for (int i = 0; i < encodedPassword.length; i++) {
if (((int) encodedPassword[i] & 0xff) < 0x10) {
buf.append("0");
}
buf.append(Long.toString((int) encodedPassword[i] & 0xff, 16));
}
String mes=buf.toString();
String algorithm2="";
byte[] unencodedPassword2 = u.getBytes();
MessageDigest md2 = null;
try {
md2 = MessageDigest.getInstance("MD5");
} catch (Exception e) {}
md2.reset();
md2.update(unencodedPassword2);
byte[] encodedPassword2 = md2.digest();
StringBuffer buf2 = new StringBuffer();
for (int i = 0; i < encodedPassword2.length; i++) {
if (((int) encodedPassword2[i] & 0xff) < 0x10) {
buf2.append("0");
```

Save the file.

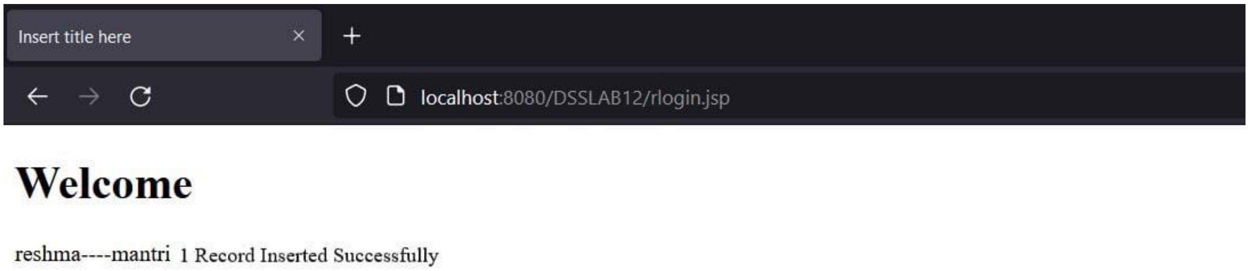
9. Right click on the html file and press 'Run As' → 1 Run on Server → (The Tomcat server should already be selected) → Press Finish.



Username reshma
Message mantri
Submit Query

10. Give your username and password.

The inputs I am giving are 'kumar' as username and 'secret' as message.

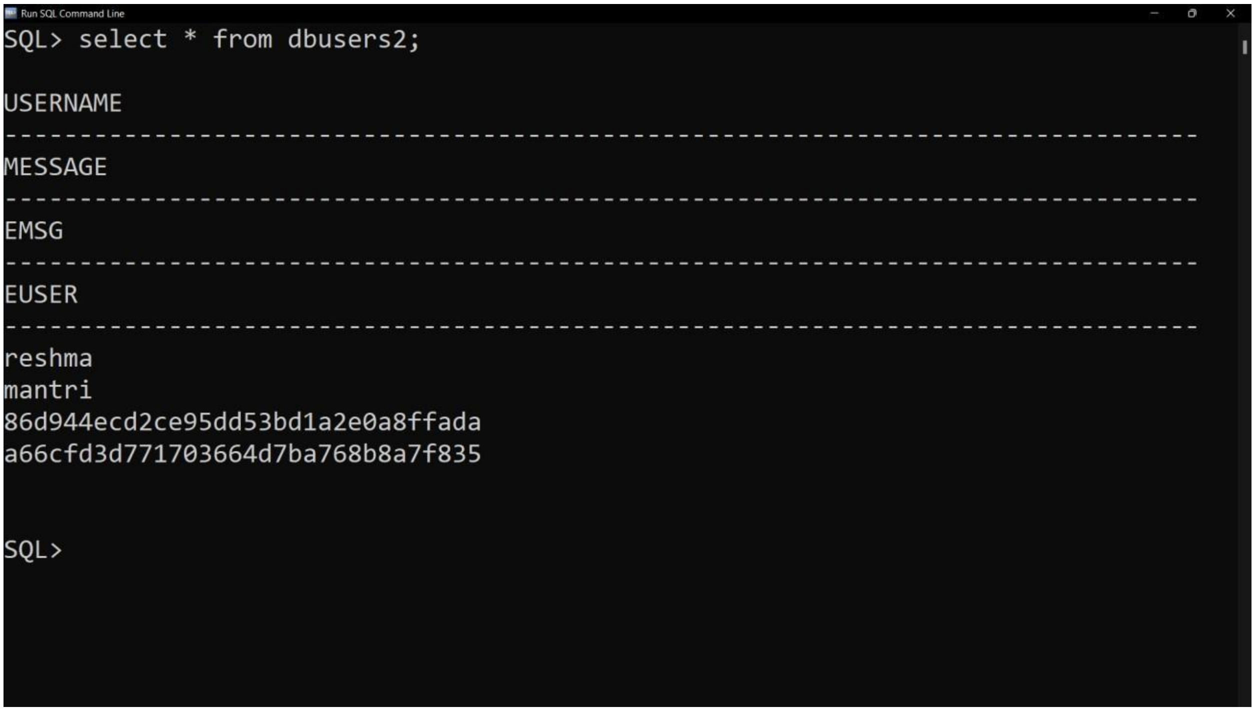


Welcome

reshma----mantri 1 Record Inserted Successfully

11. The hashed message and username must be stored in the table ‘dbusers2’ now.

Display the table using ‘**select * from dbusers2;**’.



```
SQL> select * from dbusers2;

USERNAME
--------------------------------------------------------------------------------
MESSAGE
--------------------------------------------------------------------------------
EMSG
--------------------------------------------------------------------------------
EUSER
--------------------------------------------------------------------------------
reshma
mantri
86d944ecd2ce95dd53bd1a2e0a8ffada
a66cfd3d771703664d7ba768b8a7f835


SQL>
```

<u>Post-Lab:</u>

Q1. You are a database security consultant for a company. The company has given you the task of creating a registration page which takes username, password, gender and place as inputs and stores the hashed value of the password, gender, placein a database table. You plan to store the hash values of the password, gender, place in the database. The hashing is done using MD5. You are to implement this using Javascript.

First, create a html page with the username, password, genderand place fields. Once the details are given as input and submit button is pressed, the javascript program in the background will hash the password, gender, place and store it in the database along with the username and original value of gender, place.

Create a table called 'dbusers22' to store the credentials. ***Sol)***

1. Connect as system to sqlplus and create the 'dbusers22' table.
2. **create table dbusers22(username varchar2(20), message varchar2(20), gender varchar2(10), place varchar2(10), emsg varchar2(40), egen varchar2(40), eplace varchar2(40));**
3. Switch on the Eclipse IDE.

   Go to 'File' → New → Other → Scroll down to 'Web' → Expand the folder and choose 'Dynamic Web Project'.
4. Set project name as something of your choice.
5. Choose 'Dynamic web module version' as 2.5. Click Finish.
6. Then expand the project file in 'Project Explorer'. Expand 'WebContent' → WEB-INF → Right click on 'lib' → Build Path… → Configure Build Path… → Click on 'Classpath' → Click 'Add External JARs…' → Navigate to the 'ojdbc14.jar' and add it.
7. Then right click on 'WebContent'. This is where you make your html and jsp files.

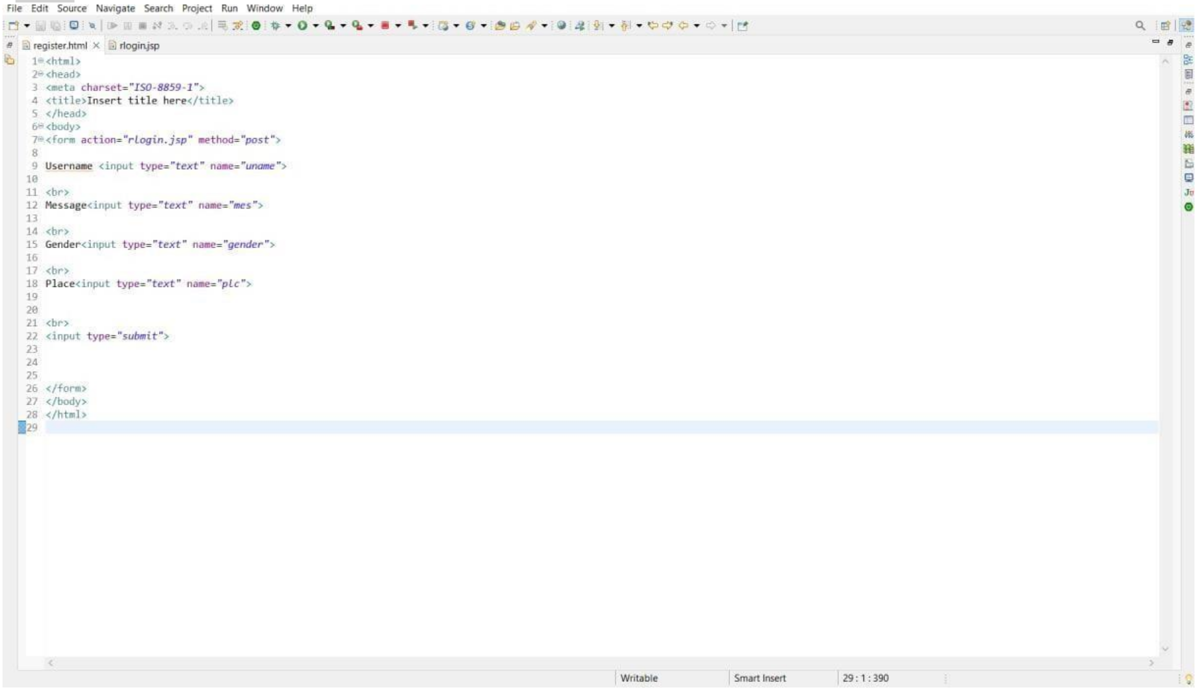
   Right click on 'WebContent' → New → HTML File.

   Give a filename and end it with '.html' extension. Press Finish. **register.html**

   --

```
<html>
<head>
<meta charset="ISO-8859-1">
<title>Insert title here</title>
</head>
<body>
<form action="rlogin.jsp" method="post">
Username <input type="text" name="uname">

<br>
```

```
Message<input type="text" name="mes">

<br>
Gender<input type="text" name="gender">

<br>
Place<input type="text" name="plc">

<br>
<input type="submit">


</form>
</body>
</html>
```



```
<html>
<head>
<meta charset="ISO-8859-1">
<title>Insert title here</title>
</head>
<body>
<form action="rlogin.jsp" method="post">

Username <input type="text" name="uname">

<br>
Message<input type="text" name="mes">

<br>
Gender<input type="text" name="gender">

<br>
Place<input type="text" name="plc">


<br>
<input type="submit">



</form>
</body>
</html>

```

--Save

the file.

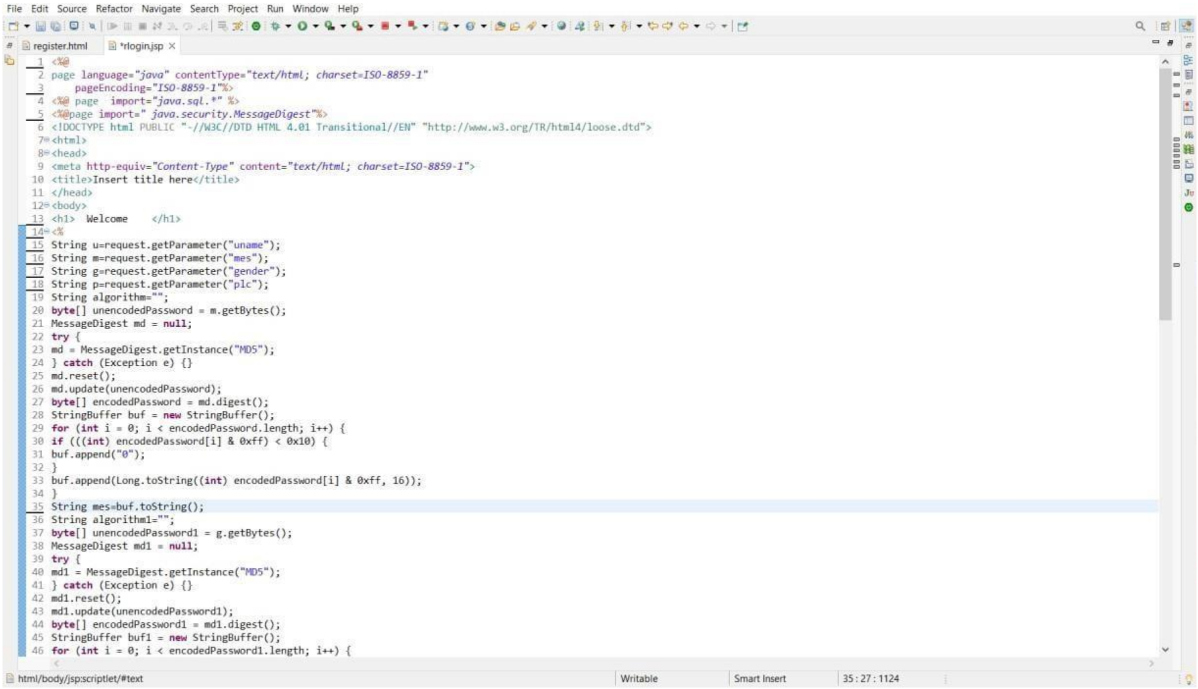
8. Right click on ‘WebContent’ → New → JSP File.

Give a filename and end it with ‘.jsp’ extension. Press Finish. **rlogin.jsp**

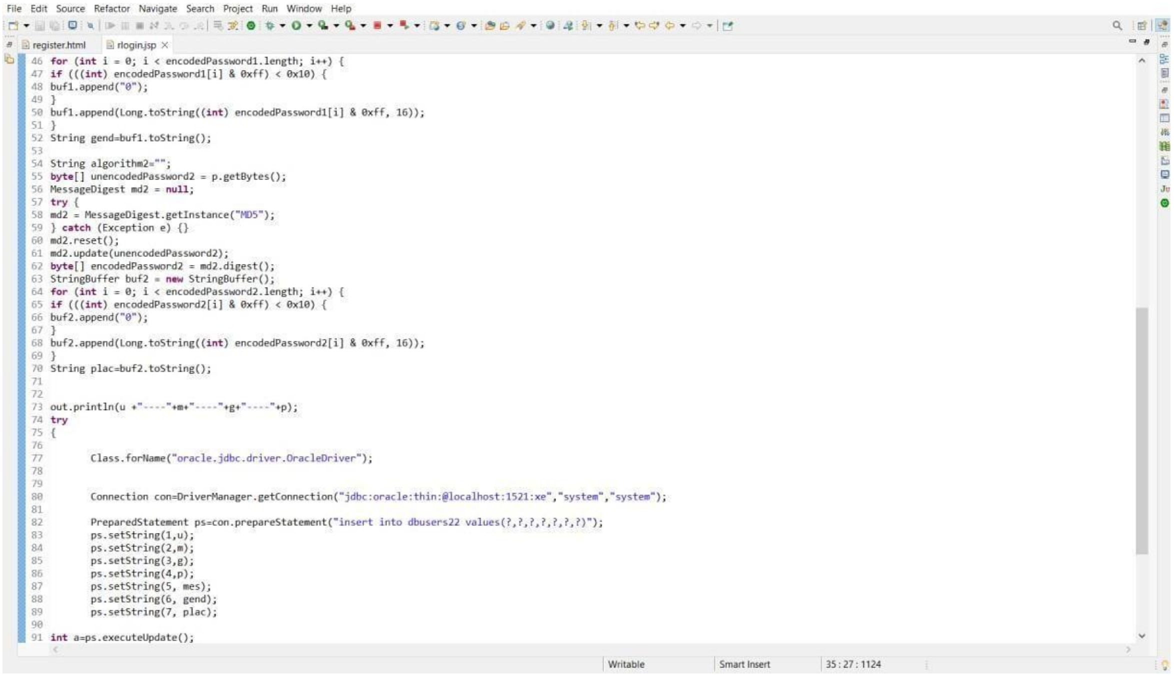
```
<%@
page language="java" contentType="text/html; charset=ISO-8859-1"
pageEncoding="ISO-8859-1"%>

<%@ page  import="java.sql.*" %>
```

```
<%@page import=" java.security.MessageDigest"%>

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html> <head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<title>Insert title here</title>
</head>
<body>
<h1>  Welcome    </h1>

<%


String u=request.getParameter("uname");

String m=request.getParameter("mes");

String g=request.getParameter("gender");

String p=request.getParameter("plc");

String algorithm="";
byte[] unencodedPassword = m.getBytes();
MessageDigest md = null; try
{
md = MessageDigest.getInstance("MD5");
} catch (Exception e) {} md.reset();
md.update(unencodedPassword); byte[]
encodedPassword = md.digest(); StringBuffer buf =
new StringBuffer(); for (int i = 0; i <
encodedPassword.length; i++) { if (((int)
encodedPassword[i] & 0xff) < 0x10) {
buf.append("0");
}
buf.append(Long.toString((int) encodedPassword[i] & 0xff, 16));
}
String mes=buf.toString();

String algorithm1="";
byte[] unencodedPassword1 = g.getBytes();
MessageDigest md1 = null; try
{
md1 = MessageDigest.getInstance("MD5");
} catch (Exception e) {} md1.reset();
md1.update(unencodedPassword1);
byte[] encodedPassword1 = md1.digest();
StringBuffer buf1 = new StringBuffer(); for (int i
= 0; i < encodedPassword1.length; i++) { if (((int)
encodedPassword1[i] & 0xff) < 0x10) {
buf1.append("0");
}
buf1.append(Long.toString((int) encodedPassword1[i] & 0xff, 16)); }
String gend=buf1.toString();

String algorithm2="";
byte[] unencodedPassword2 = p.getBytes();
MessageDigest md2 = null; try
{
md2 = MessageDigest.getInstance("MD5");
} catch (Exception e) {} md2.reset();
md2.update(unencodedPassword2); byte[]
encodedPassword2 = md2.digest(); StringBuffer buf2
= new StringBuffer(); for (int i = 0; i <
encodedPassword2.length; i++) { if (((int)
encodedPassword2[i] & 0xff) < 0x10) {
buf2.append("0");
}
buf2.append(Long.toString((int) encodedPassword2[i] & 0xff, 16)); }
String plac=buf2.toString();

out.println(u +"----"+m+"----"+g+"----"+p); try
{

          Class.forName("oracle.jdbc.driver.OracleDriver");



          Connection
con=DriverManager.getConnection("jdbc:oracle:thin:@localhost:1521:xe","system","syste
m");

          PreparedStatement ps=con.prepareStatement("insert into dbusers22
values(?,?,?,?,?,?,?)");     ps.setString(1,u);        ps.setString(2,m);
   ps.setString(3,g);        ps.setString(4,p);        ps.setString(5,
mes);           ps.setString(6, gend);           ps.setString(7, plac);

int a=ps.executeUpdate();

out.println(a+ "  Record Inserted Successfully");
}
catch(Exception e)
{
       out.println(e);

}

%>

</body>
```

```
</html>
```


File Edit Source Refactor Navigate Search Project Run Window Help
register.html
*rlogin.jsp
html/body/jsp:scriptlet/#text
Writable
Smart Insert
35 : 27 : 1124

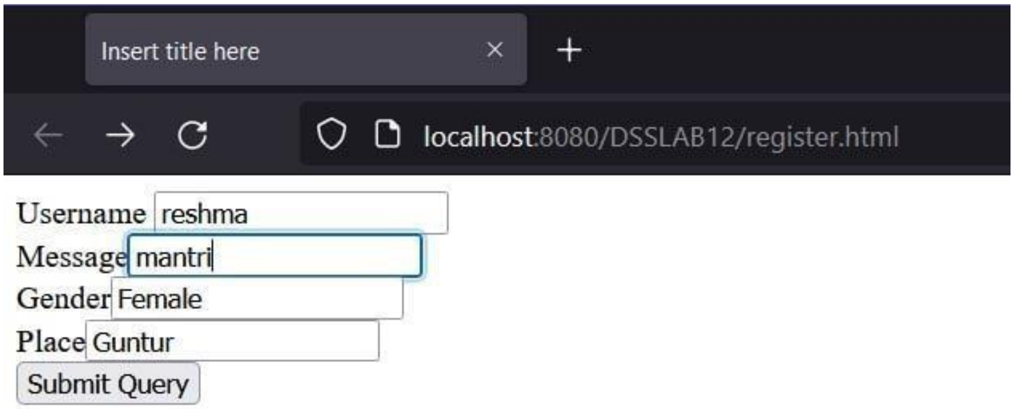
```
<%@
page language="java" contentType="text/html; charset=ISO-8859-1"
    pageEncoding="ISO-8859-1"%>
<%@ page  import="java.sql.*" %>
<%@page import=" java.security.MessageDigest"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<title>Insert title here</title>
</head>
<body>
<h1>  Welcome    </h1>
<%
String u=request.getParameter("uname");
String m=request.getParameter("mes");
String g=request.getParameter("gender");
String p=request.getParameter("plc");
String algorithm="";
byte[] unencodedPassword = m.getBytes();
MessageDigest md = null;
try {
md = MessageDigest.getInstance("MD5");
} catch (Exception e) {}
md.reset();
md.update(unencodedPassword);
byte[] encodedPassword = md.digest();
StringBuffer buf = new StringBuffer();
for (int i = 0; i < encodedPassword.length; i++) {
if (((int) encodedPassword[i] & 0xff) < 0x10) {
buf.append("0");
}
buf.append(Long.toString((int) encodedPassword[i] & 0xff, 16));
}
String mes=buf.toString();
String algorithm1="";
byte[] unencodedPassword1 = g.getBytes();
MessageDigest md1 = null;
try {
md1 = MessageDigest.getInstance("MD5");
} catch (Exception e) {}
md1.reset();
md1.update(unencodedPassword1);
byte[] encodedPassword1 = md1.digest();
StringBuffer buf1 = new StringBuffer();
for (int i = 0; i < encodedPassword1.length; i++) {
```


File Edit Source Refactor Navigate Search Project Run Window Help
register.html
rlogin.jsp
Writable
Smart Insert
35 : 27 : 1124

```
for (int i = 0; i < encodedPassword1.length; i++) {
if (((int) encodedPassword1[i] & 0xff) < 0x10) {
buf1.append("0");
}
buf1.append(Long.toString((int) encodedPassword1[i] & 0xff, 16));
}
String gend=buf1.toString();

String algorithm2="";
byte[] unencodedPassword2 = p.getBytes();
MessageDigest md2 = null;
try {
md2 = MessageDigest.getInstance("MD5");
} catch (Exception e) {}
md2.reset();
md2.update(unencodedPassword2);
byte[] encodedPassword2 = md2.digest();
StringBuffer buf2 = new StringBuffer();
for (int i = 0; i < encodedPassword2.length; i++) {
if (((int) encodedPassword2[i] & 0xff) < 0x10) {
buf2.append("0");
}
buf2.append(Long.toString((int) encodedPassword2[i] & 0xff, 16));
}
String plac=buf2.toString();


out.println(u +"----"+m+"----"+g+"----"+p);
try
{

        Class.forName("oracle.jdbc.driver.OracleDriver");


        Connection con=DriverManager.getConnection("jdbc:oracle:thin:@localhost:1521:xe","system","system");

        PreparedStatement ps=con.prepareStatement("insert into dbusers22 values(?,?,?,?,?,?,?)");
        ps.setString(1,u);
        ps.setString(2,m);
        ps.setString(3,g);
        ps.setString(4,p);
        ps.setString(5, mes);
        ps.setString(6, gend);
        ps.setString(7, plac);

int a=ps.executeUpdate();
```

Save the file.

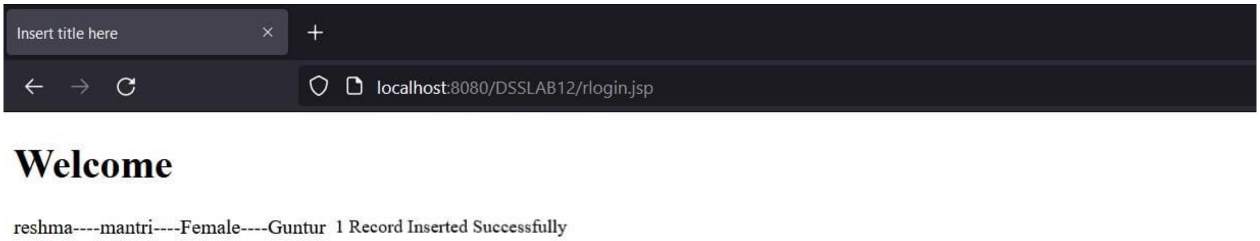
9. Right click on the html file and press ‘Run As’ → 1 Run on Server → (The Tomcat server should already be selected) → Press Finish.



Username reshma
Message mantri
Gender Female
Place Guntur
Submit Query

10. Give your username, message, gender an place.

The inputs I am giving are 'kumar' as username, 'singh' as message and 'male' as gender and 'vjw' as place.

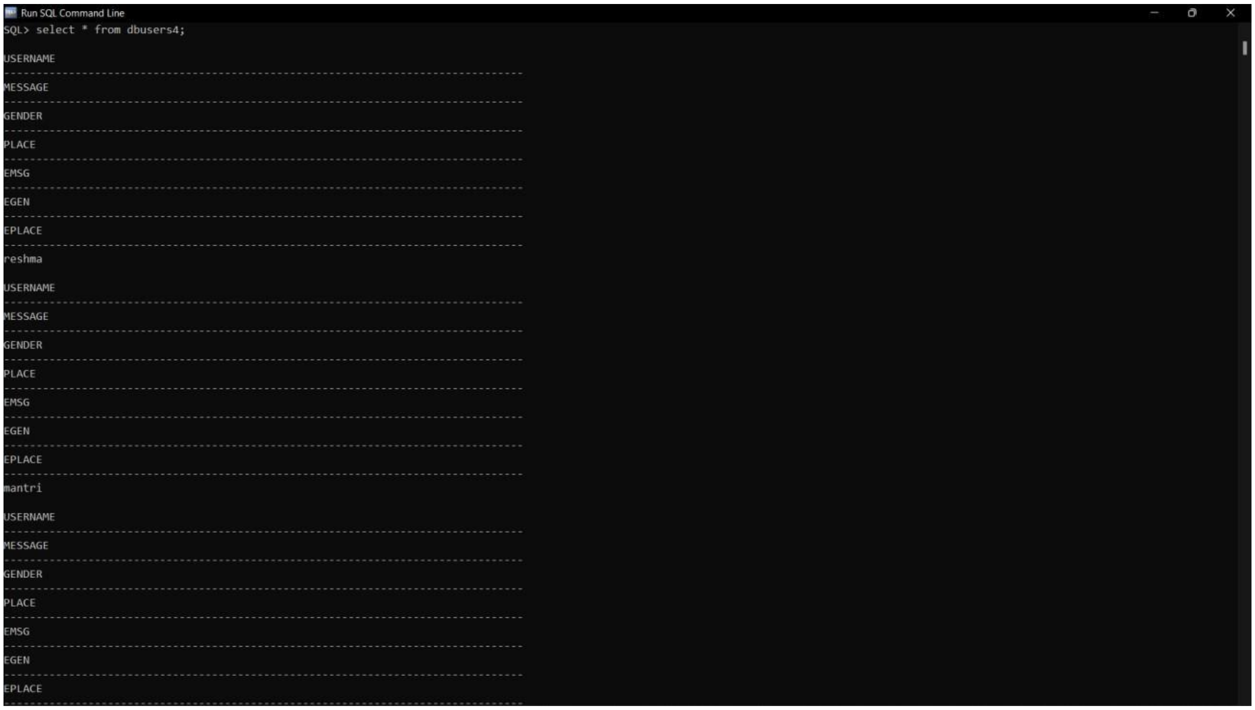


Welcome

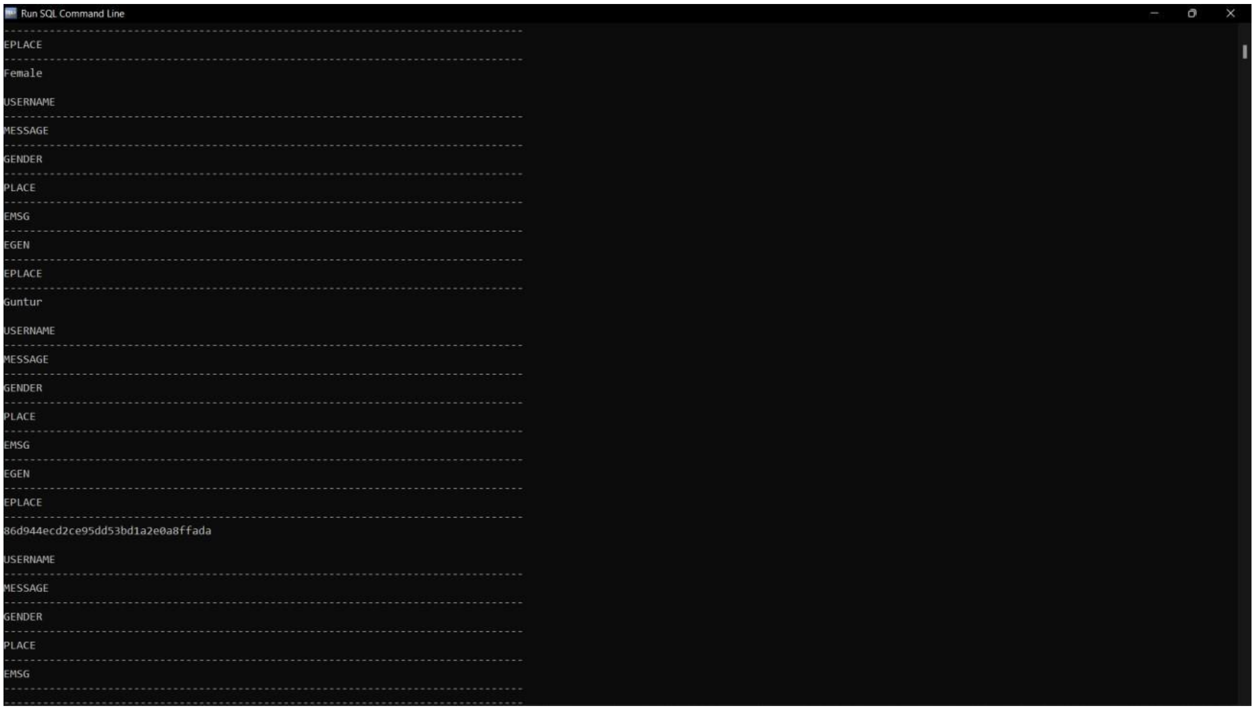
reshma----mantri----Female----Guntur 1 Record Inserted Successfully

11. The hashed message, gender and place must be stored in the table 'dbusers4' now.

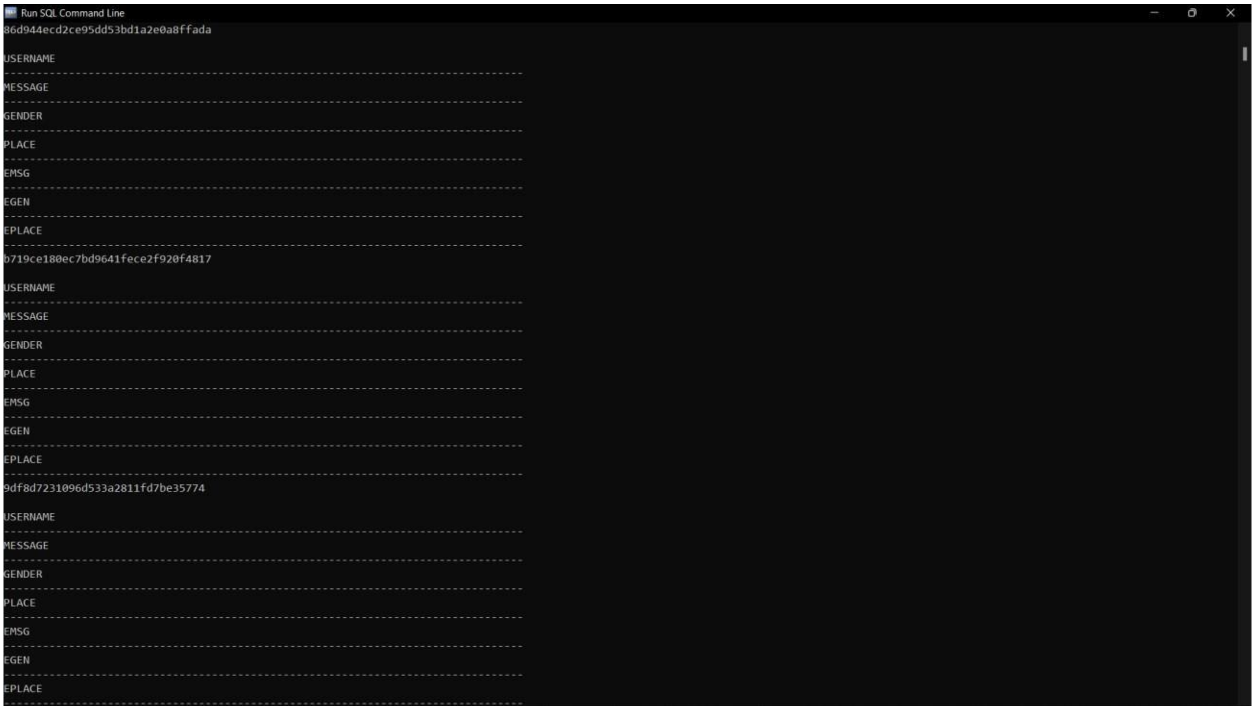
Display the table using '**select * from dbusers4;**'.



```
SQL> select * from dbusers4;

USERNAME
--------------------------------------------------------------------------------
MESSAGE
--------------------------------------------------------------------------------
GENDER
--------------------------------------------------------------------------------
PLACE
--------------------------------------------------------------------------------
EMSG
--------------------------------------------------------------------------------
EGEN
--------------------------------------------------------------------------------
EPLACE
--------------------------------------------------------------------------------
reshma

USERNAME
--------------------------------------------------------------------------------
MESSAGE
--------------------------------------------------------------------------------
GENDER
--------------------------------------------------------------------------------
PLACE
--------------------------------------------------------------------------------
EMSG
--------------------------------------------------------------------------------
EGEN
--------------------------------------------------------------------------------
EPLACE
--------------------------------------------------------------------------------
mantri

USERNAME
--------------------------------------------------------------------------------
MESSAGE
--------------------------------------------------------------------------------
GENDER
--------------------------------------------------------------------------------
PLACE
--------------------------------------------------------------------------------
EMSG
--------------------------------------------------------------------------------
EGEN
--------------------------------------------------------------------------------
EPLACE
--------------------------------------------------------------------------------
```



```
--------------------------------------------------------------------------------
EPLACE
--------------------------------------------------------------------------------
Female

USERNAME
--------------------------------------------------------------------------------
MESSAGE
--------------------------------------------------------------------------------
GENDER
--------------------------------------------------------------------------------
PLACE
--------------------------------------------------------------------------------
EMSG
--------------------------------------------------------------------------------
EGEN
--------------------------------------------------------------------------------
EPLACE
--------------------------------------------------------------------------------
Guntur

USERNAME
--------------------------------------------------------------------------------
MESSAGE
--------------------------------------------------------------------------------
GENDER
--------------------------------------------------------------------------------
PLACE
--------------------------------------------------------------------------------
EMSG
--------------------------------------------------------------------------------
EGEN
--------------------------------------------------------------------------------
EPLACE
--------------------------------------------------------------------------------
86d944ecd2ce95dd53bd1a2e0a8ffada

USERNAME
--------------------------------------------------------------------------------
MESSAGE
--------------------------------------------------------------------------------
GENDER
--------------------------------------------------------------------------------
PLACE
--------------------------------------------------------------------------------
EMSG
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
```



```
86d944ecd2ce95dd53bd1a2e0a8ffada

USERNAME
--------------------------------------------------------------------------------
MESSAGE
--------------------------------------------------------------------------------
GENDER
--------------------------------------------------------------------------------
PLACE
--------------------------------------------------------------------------------
EMSG
--------------------------------------------------------------------------------
EGEN
--------------------------------------------------------------------------------
EPLACE
--------------------------------------------------------------------------------
b719ce180ec7bd9641fece2f920f4817

USERNAME
--------------------------------------------------------------------------------
MESSAGE
--------------------------------------------------------------------------------
GENDER
--------------------------------------------------------------------------------
PLACE
--------------------------------------------------------------------------------
EMSG
--------------------------------------------------------------------------------
EGEN
--------------------------------------------------------------------------------
EPLACE
--------------------------------------------------------------------------------
9df8d7231096d533a2811fd7be35774

USERNAME
--------------------------------------------------------------------------------
MESSAGE
--------------------------------------------------------------------------------
GENDER
--------------------------------------------------------------------------------
PLACE
--------------------------------------------------------------------------------
EMSG
--------------------------------------------------------------------------------
EGEN
--------------------------------------------------------------------------------
EPLACE
--------------------------------------------------------------------------------
```