```
SELECT * FROM users WHERE username = 'input_username' AND password = 'input_password';
```

```
' OR '1'='1'; --
```

```
SELECT * FROM users WHERE username = '' OR '1'='1'; --' AND password = 'input_password';
```

Boolean Based SQL injection

```
// This is a simplified example for educational purposes only.
// Never use code like this in a real-world application.

import java.io.*;
import javax.servlet.*;
import javax.servlet.http.*;
import java.sql.*;

public class LoginServlet extends HttpServlet {

   protected void doPost(HttpServletRequest request, HttpServletResponse response) throws ServletException, IOException {
      String username = request.getParameter("username");
      String password = request.getParameter("password");

      // Vulnerable SQL query - Concatenating user inputs directly
      String query = "SELECT * FROM users WHERE username='" + username + "' AND password='" + password + "';";

      try {
         // Assuming you have a Connection object (conn) to your database
         Statement statement = conn.createStatement();
         ResultSet resultSet = statement.executeQuery(query);

         if (resultSet.next()) {
            // Authentication successful
            response.getWriter().println("Login successful");
         } else {
            // Authentication failed
            response.getWriter().println("Login failed");
         }
      } catch (SQLException e) {
         e.printStackTrace();
      }
   }
}
```

1) Use Parameterized Statements or Prepared Statements:

```
String query = "SELECT * FROM users WHERE username = ? AND password = ?";
PreparedStatement preparedStatement = connection.prepareStatement(query);
preparedStatement.setString(1, enteredUsername);
preparedStatement.setString(2, enteredPassword);
ResultSet resultSet = preparedStatement.executeQuery();
```

2) Input Validation

Username => character (0-9)(a-z)

```
If username matches character(0-9)(a-z)
  Run the sql query

Else

Input validation failed and enter correct format of username
```

http://testphp.vulnweb.com/artists.php?artist=1

Select artistinfo from artisttable where artistid = 1

Sqlmap => Opensource installed in KaliLinux
Retrive the Databases
Retrieve the Tables
Retrieve the columns
Retrieve the data