One vulnerability that exists in this code is SQL Injection. This code did not do an input validation for the username get from the client. To mitigate this vulnerability, he needs to do a input validation to filter hazardous characters from user input like the code below.

//Get the username

String username = request.getParameter(“username”)

String characterPattern = "[0-9a-zA-Z]";

If (! username. matches (characterPattern))

{

out.println (“Invalid Input”);

}

Else

{

//Prepare the connection

Statement statement = connection.createStatement();

String query = “SELECT secret FROM Users WHERE (username = ‘” + username+ “’ AND NOT role = ‘admin’)”;

//Execute query and return the results

ResultSet result = statement.executeQuery(query);

}