Vulnerable Java Code

```
String DRIVER = "com.ora.jdbc.Driver";
String DataURL = "jdbc:db://localhost:5112/users";
String LOGIN = "admin";  String PASSWORD = "admin123";
Class.forName(DRIVER);

//Make connection to DB Connection
connection = DriverManager.getConnection(DataURL, LOGIN, PASSWORD);
String Username = request.getParameter("USER"); // From HTTP request
String Password = request.getParameter("PASSWORD"); // From HTTP request
int iUserID = -1;
String sLoggedUser = "";
String sel = "SELECT User_id, Username FROM USERS WHERE Username = '" +Username + "' AND Password = '" +
Password + "'";
Statement selectStatement = connection.createStatement ();
ResultSet resultSet = selectStatement.executeQuery(sel);

if (resultSet.next()) {
          iUserID = resultSet.getInt(1);
          sLoggedUser = resultSet.getString(2);
}

PrintWriter writer = response.getWriter ();
if (iUserID >= 0) {
          writer.println ("User logged in: " + sLoggedUser);
} else {
          writer.println ("Access Denied!");
}
```

1. What does this code have to do with security?

2. What is the vulnerability?

3. What does the vulnerability allow the attacker to do?

4. The next page: code to blacklist bad inputs…

```vb
Imports Microsoft.VisualBasic

Namespace Sample
    Public Class SampleSqlInjectionScreeningModuleVB
        Implements IHttpModule

        'Defines the set of characters that will be checked.
        Public Shared blackList As String() = {"/*", "*/", "@@", _
                                               "nchar", "nvarchar", "alter", _
                                               "begin", "cast", "create", "cursor", "declare", "delete", _
                                               "drop", "end", "execute", "fetch", "insert", _
                                               "kill", "open", "select", "sys", "sysobjects", "syscolumns", _
                                               "table", "update"}

        Public Sub Dispose() Implements IHttpModule.Dispose
            'no-op
        End Sub

        'Tells ASP.NET that there is code to run during BeginRequest
        Public Sub Init(ByVal app As HttpApplication) Implements IHttpModule.Init
            AddHandler app.BeginRequest, AddressOf app_BeginRequest
        End Sub

        'For each incoming request, check the query-string, form and cookie values for suspicious values.
        Private Sub app_BeginRequest(ByVal sender As Object, ByVal e As EventArgs)
            Dim Request As HttpRequest = TryCast(sender, HttpApplication).Context.Request

            For Each key As String In Request.QueryString
                CheckInput(Request.QueryString(key))
            Next
            For Each key As String In Request.Form
                CheckInput(Request.Form(key))
            Next
            For Each key As String In Request.Cookies
                CheckInput(Request.Cookies(key).Value)
            Next
        End Sub

        'The utility method that performs the blacklist comparisons
        'You can change the error handling and error redirect location to whatever makes sense for your site.
        Private Sub CheckInput(ByVal parameter As String)
            For i As Integer = 0 To blackList.Length - 1
                If (parameter.IndexOf(blackList(i), StringComparison.OrdinalIgnoreCase) >= 0) Then
                    'Handle the discovery of suspicious Sql characters here
                    'generic error page on your site
                    HttpContext.Current.Response.Redirect("~/Error.aspx")
                End If
            Next
        End Sub

    End Class
End Namespace
```