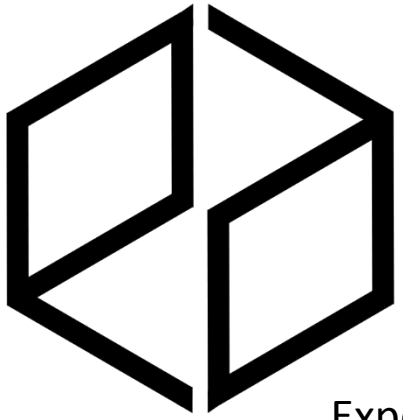

www.pandoralabs.net
PANDORA
SECURITY LABS
Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.



PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

www.pandoralabs.net

We are a Security-as-a-Service company

Providing businesses with on-demand IT security controls for them to meet their 24x7 security strategies & requirements.

We Make IT Secure

Developing Secure Applications

Quick Tips

Use Parameterized Queries

Use Parameterized Queries

- Injection happens when data is supplied from one component to another
- Hackers "inject" their code to run instead of yours
  - Example: SQL injection attack String query = "SELECT * FROM products WHERE name='" + request.getParameter("id") +"'";
- Code expects a nice parameter in the URL
  - http://example.com/products?id=123
  - Hacker could instead supply this: http://example.com/products?id=';+DROP+TABLE+'products';

Use Parameterized Queries

String prodId= request.getParameter(“productId");

String query = "SELECT product_status FROM product_data WHERE product_id = ? ";

PreparedStatement pstmt = connection.prepareStatement(query);

pstmt.setString(1, prodId);

ResultSet results = pstmt.executeQuery( );

Validate User Input

#6 Sanitize and Validate User Input

- Always assume the data is “evil”
- Always sanitize input! (at the backend not front end!)
- Encode all user input before using it
- Clean up quotes, semi-colons, parentheses, etc.

#6 Sanitize and Validate User Input

Data should be:

- Strongly Typed at all times
- Length Checked and Fields Length Minimized
- Ranged check if numeric
- Unsigned unless required to be signed
- Syntax or grammar should be checked prior to first use or inspection
- Sanitized

#6 Sanitize and Validate User Input

- Coding guidelines should use some form of visible tainting on input from the client or untrusted sources, such as third party connectors to make it obvious that the input is unsafe:

```
taintedPostcode = getParameter(“postCode”);
validation = New Validation();
postCode = validation.isPostcode(taintPostcode);
```


www.pandoralabs.net
PANDORA
SECURITY LABS
Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.