**File Disclosure: J2EE Development Mitigation SOP**

A file disclosure occurs when data enters a program from an untrusted source. The data is then used to dynamically construct a path.

**Defense Against File Disclosure**

Do not use untrusted data to direct requests to server-side resources. Instead, use a level of indirection between locations and paths.

**Example**

String returnURL = request.getParameter("returnURL");

RequestDispatcher rd = request.getRequestDispatcher(returnURL);

rd.forward();

**Explanation**

The preceding code takes untrusted data and uses it to build a path which is used in a server side forward.

**Recommendation**

Instead of the following:

< a href="http://www.yourcorp.com/webApp/logic?nextPage=WEB-INF/signup.jsp">New Customer

Use the following:

< a href="http://www.yourcorp.com/webApp/logic?nextPage=newCustomer">New Customer

The server-side logic would have a map keyed by logical names to server-side paths such that the path stored under the key "newCustomer" would be "/WEB-INF/signup.jsp".

**References**

1. Ryan Berg and Dinis Cruz, Two Security Vulnerabilities in the Spring Framework's MVC, 2008, http://o2platform.files.wordpress.com/2011/07/ounce\_springframework\_vulnerabilities.pdf
2. INPUT-1: Validate inputs, Oracle, http://www.oracle.com/technetwork/java/seccodeguide-139067.html#5
3. Standards Mapping - Common Weakness Enumeration, CWE ID 552