**Resource Injection Development Mitigation SOP**

Resource injection vulnerabilities occur when the application allows user input to control resource identifiers, which could enable an attacker to access or modify otherwise protected resources. The first way this vulnerability could occur is if an attacker can specify the identifier used to access a system resource, for example, if an attack can specify a port number used to connect to a network resource. The second way is if the attacker is able to gain a capability that would be otherwise permitted by allowing them to specify the resource. For example, if the program gives the attacker the ability to transmit sensitive information to a third-party server.

**Defense Against Resource Injection**

The best way to prevent resource injection vulnerabilities is to make sure user inputs are being validated by only allowing the user to choose options from a validated drop down list. If a user is allowed to specify a port number, be sure to check their input with a list of allowed port numbers before using it without validation.

While blacklisting can help avoid insecure inputs, whitelisting is the better option because this allows the programmer to specify the allowed characters that can appear in the resource name. All inputs can be accepted in they are composed exclusively of characters in the approved set.

**Example**

String rPort = request.getParameter(“remotePort”);

…

ServerSocket srvr = new ServerSocket(rPort);

Socket skt = srvr.accept();

…

**Explanation**

The code above shows an application that receives a port number from an HTTP request, then creates a socket from the input without any validation. This is vulnerable to allowing a user to modify the port using a proxy and obtain a direct connection with the server.

**References**

1. [HP Enterprise Security – Resource Injection](http://www.hpenterprisesecurity.com/vulncat/en/vulncat/php/resource_injection.html)
2. [OWASP – Resource Injection](https://www.owasp.org/index.php/Resource_Injection)