**System Information Leak: HTML Comment in JSP Development Mitigation SOP**

Comments throughout the code helps developers understand the process and give insight to those unfamiliar with the code. Any information that can be viewed by the user and could provide any insight that would be help an attack a plan of attack would be considered a system information leak.

**Defense Against System Information Leak: HTML Comment in JSP**

To prevent would be attackers from gaining knowledge of the system via comments, remove all HTML comments before promoting to the production environment. If comments need to be available to the developers then use JSP comments. The JSP Engine will remove all of the comments at the translation phase and the compilation unit doesn’t contain them.

**Example**

<!-- Hidden form to submit a delete -->

**Explanation**

This comment lets the user know how forms are handles and can be viewed from any browser.

**Recommendation**

These comments are available within the source code and are readable to the developers only.

<%-- Hidden form to submit a delete --%>

**References**

1. [OWASP – Information Leakage](https://www.owasp.org/index.php/Top_10_2007-Information_Leakage_and_Improper_Error_Handling)