**Hidden Field**

The program creates a hidden form field.

**Classic Example**

Hidden hidden = new Hidden(element);

Programmers often trust the contents of hidden fields, expecting that users will not be able to view them or manipulate their contents. Attackers will violate these assumptions. They will examine the values written to hidden fields and alter them or replace the contents with attack data.

**Example**

<input type="hidden" name="trackedItems[<c:out value="${newTrackedItemIndex}"/>].standardDevelopmentAction.stdDvlpmtActionId" value="<c:out value="${stdDevActionId}"/>"/>

**Defense Against *Specific Vulnerability***

*If hidden fields carry sensitive information, this information will be cached the same way the rest of the page is cached. This can lead to sensitive information being tucked away in the browser cache without the user's knowledge*.

**Specific Explanation**

In general, using hidden fields should be avoided. Another alternative might be to disable fields. If the usage of hidden fields can’t be avoided, make sure you are validating all the data.

**References**

[1] Input Validation and Representation, Micro Focus Fortify, https://vulncat.fortify.com/

[2] Standards Mapping - Common Weakness Enumeration, CWE ID 472, CWE ID 642

[3] Standards Mapping - OWASP Mobile Top 10 Risks 2014, M4 Unintended Data Leakage