**CSRF Changes in XPEDX**

**What we need to do to enable CSRF check?**

Add the below context params in web.xml

<context-param>

<param-name>scui-request-validator-10</param-name>

<param-value>com.sterlingcommerce.ui.web.platform.security.SCUICSRFTokenValidator</param-value>

</context-param>

<context-param>

<param-name>scui-csrf-validator-request-method</param-name>

<param-value>ALL</param-value>

</context-param>

The OOTB code assigns a csrf token for each session which is in session attribute **SCUI\_CSRF\_SECURITY\_TOKEN**. This is expected in every call reaching server. This is monitored by a filter.

**What is taken care by OOTB?**

1. All Ext Ajax calls with proper href url will be appended with csrf token.
2. All href or struts tag for url (<s:url…) will be appended with csrf token.

**What not to do?**

1. Hard code the url inside Ajax will not work

Ext.Ajax.request({

url: '/swc/catalog/setSelectedView.action?sfId=xpedx&amp;scFlag=Y’,

params: {

selectedView: document.getElementById("selectedView").value

},

method: 'GET',

callback: **function** () {

svg\_classhandlers\_decoratePage();

}

});

**The right way to do this is**

<s:url id=*'selectedViewURL'* action=*'setSelectedView'* namespace=*'/catalog'* />

…

**var** url = "<s:property value='#selectedViewURL'/>";

url = ReplaceAll(url,"&amp;",'&');

Ext.Ajax.request({

url: url,

params: {

selectedView: document.getElementById("selectedView").value

},

method: 'GET',

callback: **function** () {

svg\_classhandlers\_decoratePage(); }

});

**What to do?**

The below method is added in header jsp. In xpedx case XPEDXPrepareHeader.jsp

**function** addCSRFToken(o, type)

{

**var** csrfToken='<%=session.getAttribute("SCUI\_CSRF\_SECURITY\_TOKEN") %>';

**if**(csrfToken != 'null')

{

**if** (type == 'link')

{

**var** url= o + '&scCSRFToken=' +csrfToken;

url = ReplaceAll(url,"&amp;",'&');

**return** url;

}

//otherwise the o is assumed to be of form type.

**var** el = document.createElement("input");

el.type = "hidden";

el.name = "scCSRFToken";

el.id = "scCSRFToken";

el.value = csrfToken;

o.appendChild(el);

}

**return** o;

}

**Where do we use it?**

1. Form’s submit url need to use this method before the form is submitted.

**Example:**

addCSRFToken(form.dom, 'form');

form.dom.submit();

1. URL defined as var in js that need csrf token added.

**Example:**

**var** linkUrl="/swc/xpedx/jsp/common/XPEDXWebtrends.jsp?...”

linkUrl=addCSRFToken(linkUrl, 'link');

1. If <s:url is accessed using <s:property in javascript, then the url formed is incorrect. We need to replace the &amp; with actual ‘&’.

**Example:**

**var** url = '<s:property value="#ResetPasswordURL" />';

url = ReplaceAll(url,"&amp;",'&');

**XPEDX Files Modified with the changes**

\WebChannel\main\webapp\xpedx\jsp\catalog\XPEDXCatalogExt.jsp

\WebChannel\main\webapp\xpedx\jsp\catalog\XPEDXproductComparisonExt.jsp

\WebChannel\main\webapp\xpedx\jsp\common\XPEDXPrepareHeader.jsp

\WebChannel\main\webapp\xpedx\jsp\profile\user\XPEDXUserList.jsp

\WebChannel\main\webapp\swc\js\MyItems\XPEDXAddToCartAndAvailability.js

\WebChannel\main\webapp\xpedx\js\webtrends\displayWebTag.js

\WebChannel\main\webapp\xpedx\jsp\catalog\XPEDXItemDetails.jsp

\WebChannel\main\webapp\xpedx\jsp\MyItems\XPEDXMyItemsList.jsp

\WebChannel\main\webapp\xpedx\jsp\MyItems\XPEDXMyItemsListDisplayAsSubMenu.jsp

\WebChannel\main\webapp\xpedx\jsp\profile\user\XPEDXUserProfile.jsp

\WebChannel\main\webapp\xpedx\jsp\order\XPEDXOrderDetail.jsp

\WebChannel\main\webapp\swc\js\order\XPEDXDraftOrderDetails.js

\WebChannel\main\webapp\xpedx\js\catalog\catalogExt.js