

Commit 317ec91



Fasse committed 4 days ago

Merge commit from fork
implement csrf-token check on deleting mylists

v5.0 · v5.0.8

1 parent [5f770c1](#) commit 317ec91

1 file changed +9 -9 lines changed

Top

modules/groups-roles

mylist_function.php

1 file changed +9 -9 lines changed



modules/groups-roles/mylist_function.php



@@ -38,6 +38,12 @@

```

38 38          throw new Exception('SYS_MODULE_DISABLED');
39 39      }
40 40
41 + // check the CSRF token of the form against the session token
42 + $myListForm = $gCurrentSession->getFormObject($_POST['adm_csrf_token']);
43 + if ($_POST['adm_csrf_token'] !== $myListForm->getCsrftoken()) {
44 +     throw new Exception('Invalid or missing CSRF token!');
45 + }
46 +
41 47      // At least one field should be assigned (has a non-empty value)
42 48      if (
43 49          empty($_POST['column']) ||

```

```

@@ -77,12 +83,6 @@
77 83
78 84     // save list
79 85     if (in_array($getMode, array('save', 'save_as', 'save_temporary'))) {
80 -         // check the CSRF token of the form against the session token
81 -         $categoryReportConfigForm = $gCurrentSession-
>getFormObject($_POST['adm_csrf_token']);
82 -         if ($_POST['adm_csrf_token'] !== $categoryReportConfigForm-
>getCsrftoken()) {
83 -             throw new Exception('Invalid or missing CSRF token!');
84 -         }
85 -
86 86         $globalConfiguration = admFuncVariableIsValid($_POST,
'cbx_global_configuration', 'bool', array('defaultValue' => false));
87 87
88 88         // go through all existing columns
@@ -98,22 +98,22 @@ function ($col, $sort = null, $cond = null) use ($list,
$gProfileFields, &$scolumn
98 98             $list->deleteColumn($columnNumber, false);
99 99             return null;
100 100         }
101 -
101 +
102 102         // Add column (profile fields usr_/mem_ stay as-is, others map
to usf_id)
103 103         if (StringUtil::strStartsWith($col, 'usr_') ||
StringUtil::strStartsWith($col, 'mem_')) {
104 104             $list->addColumn($col, $columnNumber, $sort ?? '', $cond ??
'');
105 105         } else {
106 106             $list->addColumn($gProfileFields->getProperty($col,
'usf_id'), $columnNumber, $sort ?? '', $cond ?? '');
107 107         }
108 -
108 +
109 109             $columnNumber++;
110 110             return null; // return value unused
111 111         },
112 112         $columns,

```

```
113 113          $sorts,  
114 114          $conditions  
115 115      );  
116 116      -  
116 116      +  
117 117          // Remove potentially deleted columns at the end  
118 118          $list->deleteColumn($columnNumber, true);  
119 119
```

Comments 0



Please [sign in](#) to comment.