

Dolibarr / dolibarr Public

- <> Code
- Issues 837
- Pull requests 296
- Actions
- Projects
- Security 3

Commit 743c22e



eldy committed 29 days ago · ✓ 2 / 2

Sec: Fix #GHSA-2mfj-r695-5h9r

develop · 23.0.1 23.0.0

1 parent [4bfe5d2](#) commit 743c22e

2 files changed +11 -9 lines changed

[↑ Top](#)

Filter files...

- htdocs/core
 - ajax
 - selectobject.php
 - lib
 - functions.lib.php

2 files changed +11 -9 lines changed



htdocs/core/ajax/selectobject.php



	↑...		@@ -18,8 +18,9 @@
18	18		*/
19	19		
20	20		/**
21	-	*	\file htdocs/core/ajax/selectobject.php
22	-	*	\brief File to return Ajax response on a selection list request
	21	+	\file htdocs/core/ajax/selectobject.php
	22	+	\brief File to return Ajax response on a selection list request
	23	+	Used by selectForForms(). See code comment in this function to find how it is used by modulebuilder fields or by extrafields.

```

23 24 */
24 25
25 26 if (!defined('NOTOKENRENEWAL')) {
  @@ -40,19 +41,19 @@
40 41
41 42 // Load Dolibarr environment
42 43 require '.././main.inc.php';
43 - require_once DOL_DOCUMENT_ROOT.'/core/class/html.form.class.php';
44 - require_once DOL_DOCUMENT_ROOT.'/core/class/extrafields.class.php';
45 44 /**
46 45 * @var Conf $conf
47 46 * @var DoliDB $db
48 47 * @var HookManager $hookmanager
49 48 * @var Translate $langs
50 49 * @var User $user
51 50 */
51 + require_once DOL_DOCUMENT_ROOT.'/core/class/html.form.class.php';
52 + require_once DOL_DOCUMENT_ROOT.'/core/class/extrafields.class.php';
52 53
53 54 $extrafields = new ExtraFields($db);
54 55
55 - $objectdesc = GETPOST('objectdesc', 'alphanohml', 0, null, null, 1);
56 + $objectdesc = GETPOST('objectdesc', 'alphanohml', 0, null, null, 1); //
  Deprecated. Do not use this anymore. Use param 'objectfield' instead.
56 57 $htmlname = GETPOST('htmlname', 'aZ09');
57 58 $outjson = (GETPOSTINT('outjson') ? GETPOSTINT('outjson') : 0);
58 59 $id = GETPOSTINT('id');
  @@ -107,7 +108,8 @@
107 108 $InfoFieldList[3] = preg_replace('/:\\w*$/', '', $vartmp); // take the
  filter field
108 109
109 110 $classname = $InfoFieldList[0];
110 - $classpath = $InfoFieldList[1];
111 + $classpath = dol_sanitizePathName($InfoFieldList[1]);
112 +
111 113 //$addcreatebuttonornot = empty($InfoFieldList[2]) ? 0 : $InfoFieldList[2];
112 114 $filter = empty($InfoFieldList[3]) ? '' : $InfoFieldList[3];
113 115 $sortfield = empty($InfoFieldList[4]) ? '' : $InfoFieldList[4];
  @@ -116,7 +118,7 @@

```

```

116 118     $objecttmp = fetchObjectByElement(0, strtolower($InfoFieldList[0]));
117 119
118 120     // Fallback to another solution to get $objecttmp
119 -     if (empty($objecttmp) && !empty($classpath)) {
121 +     if (empty($objecttmp) && !empty($classpath) &&
    preg_match('/\.class\.php$/', $classpath)) {
120 122         dol_include_once($classpath);
121 123
122 124         if ($classname && class_exists($classname)) {
    ↓
    ↑
    @@ -151,7 +153,7 @@
151 153     if ($objecttmp !== null && !empty($objecttmp->module) && !in_array($objecttmp->
    >module, $allowModules)) {
152 154         restrictedArea($user, $objecttmp->module, $id, $objecttmp->table_element,
    $objecttmp->element);
153 155     } else {
154 -     restrictedArea($user, $objecttmp !== null ? $objecttmp->element : '', $id);
156 +     restrictedArea($user, $objecttmp !== null ? $objecttmp->element :
    'unknownobject', $id); // If object is unknown, we force to 'unknownobject'
    instead of '' to be sure access is forbidden
155 157     }
156 158
157 159
    ↓

```

```

▼ htdocs/core/lib/functions.lib.php ...
    ↑
    @@ -1595,7 +1595,7 @@ function dol_getprefix($mode = '')
1595 1595     * To link to a module file from a module file, use include
    './mymodulefile';
1596 1596     * To link to a module file from a core file, then this function can be used
    (call by hook / trigger / speciales pages)
1597 1597     *
1598 -     * @param string $relpath    Relative path to file (Ie: mydir/myfile,
    ./myfile, ...)
1598 +     * @param string $relpath    Relative path to file (Ie: mydir/myfile,
    ./myfile, ...)
1599 1599     * @param string $classname  Class name (deprecated)
1600 1600     * @return bool              True if load is a success, False if it fails
1601 1601     */
    ↓

```

Comments 0



Please [sign in](#) to comment.