

Bugs & Wish list

Updated items should have permissions checking | Tiki Wiki CMS Groupware :: Development

Updated items should have permissions checking

Status

✖ Closed

Subject

Updated items should have permissions checking

Version

1.9.x

Category

- Error

Feature

Wiki (page view, edit, history, rename, etc)

Modules

Resolution status

Fixed or Solved

Submitted by

mrish

Volunteered to solve

mrish

Lastmod by

mrish

Rating

★★★★★ (0) ?

Description

The last updated pages mod shows pages that the user does not have a right to view. This is a bug and could be serious security. The code should only show pages that the user has a right to view.

Solution

The issue was with category views. Here is code I tweaked in tikilib that fixes it. Can someone modify and check in the code?

```
// Function that checks for:
// - tiki_p_admin
// - the permission itself
// - individual permission
// - category permission
// if O.K. this function shall replace similar constructs in list_pages and other functions above.
// $categperm is the category permission that should grant $perm. if none, pass 0
function
user_has_perm_on_object($user,$object,$objtype,$perm,$categperm='tiki_p_view_categories') {
global $feature_categories;
global $userlib;
// superadmin

if($userlib->user_has_permission($user, 'tiki_p_admin')) {
return(TRUE);
}
```

```

//mod changed order
// no individual and no category perms. So has the user the perm itself?
if (is_array($perm)) {
    foreach($perm as $p) {
        if(!$userlib->user_has_permission($user, $p)) {
            return(FALSE);
        }
    }
} else {
    if(!$userlib->user_has_permission($user, $perm)) {
        return(FALSE);
    }
}

if ($userlib->object_has_one_permission($object, $objtype)) {
    // wiki permissions override category permissions
    //handle multiple permissions
    if(is_array($perm)) {
        foreach($perm as $p) {
            if(!$userlib->object_has_permission($user, $object, $objtype,$p)) {
                return(FALSE);
            }
        }
    } else {
        if (!$userlib->object_has_permission($user, $object, $objtype,$perm))
        {
            return(FALSE);
        }
    }
    return (TRUE);
} elseif ($feature_categories 'y' && $categperm ! 0) {

// no wiki permissions so now we check category permissions tiki_p_view_categories
global $cataglib;
if (!is_object($cataglib)) {
    include_once('lib/categories/cataglib.php');
}
unset($tiki_p_view_categories); // unset this var in case it was set previously
$perms_array = $cataglib->get_object_categories_perms($user, $objtype, $object);
if ($perms_array) {
    $is_categorized = TRUE;
    foreach ($perms_array as $p => $value) {
        $$p = $value;
    }
    if ($tiki_p_admin_categories 'y' && $tiki_p_view_categories 'n')
    $tiki_p_view_categories = 'y';
} else {
    $is_categorized = FALSE;
}

if ($is_categorized && !empty($categperm) && $$categperm == 'y') {
    //
    return(TRUE);
}

```

```
} else {  
return(FALSE);  
}  
// if it has no category perms or the user does not have  
// the perms, continue to check individual perms!  
}  
  
return(TRUE);  
}
```

Importance

4

Priority

20

Demonstrate Bug (Tiki 19+)

Please demonstrate your bug on show2.tiki.org

Version: trunk ▼

Demonstrate Bug (older Tiki versions)

Ticket ID

742

Created

Friday 02 June, 2006 21:21:40 GMT-0000

by Unknown

LastModif

Wednesday 07 June, 2006 18:44:21 GMT-0000

Comments

Attachments

filename	created	hits	comment	version	filetype
----------	---------	------	---------	---------	----------

No attachments for this item

The original document is available at

<https://dev.tiki.org/item742-Updated-items-should-have-permissions-checking>