Subject: workflow security issue.
Posted by ljkbrost on Sun, 04 Apr 2010 23:30:30 GMT
View Forum Message <> Reply to Message

Hi,

I'm using a workflow and having trouble when the rdcaccount_id != 1. I'm using an 'AUTO' transition and when the workflow system goes to update the record I get a silent failure. The workflow is not executed, I get no error message, and I'm returned to the previous screen.

In my tracing of the problem I think it's related to wf_workitem.class.inc and the _cm_pre_getData function. Inside this function it sets the following:

```
$this->sql_select = 'user_id, role_id, wf_workitem.workflow_id, case_id, workitem_id,
wf_workitem.task_id, transition_trigger, w\
orkitem_status, enabled_date, cancelled_date, finished_date, deadline, context, workflow_name,
task_desc';
```

Later in std.table.class.inc the function updateRecord checks the rdcaccount_id below:

```
if ($fieldarray['rdcaccount_id'] != $_SESSION['rdcaccount_id']) {
 $this->errors['rdcaccount_id'] = getLanguageText('sys0189');
} // if
```

Because of the sql_select statment above the rdcaccount_id is not pulled from the wf_workitem table and the subsequent std.table.class.inc code fails. When I change the sql_select statment to:

```
$this->sql_select = 'user_id, role_id, wf_workitem.workflow_id, case_id, workitem_id,
wf_workitem.task_id, transition_trigger, w\
orkitem_status, enabled_date, cancelled_date, finished_date, deadline, context, workflow_name,
task_desc, rdcaccount_id';
```

Everything works as expected.