

Admidio / **admidio** Public

<> **Code** Issues 156 Pull requests 3 Actions Projects Security and qua

Commit 707171c



Fasse committed last week

Merge commit from fork
implement csrf-token check for all registration functions


v5.0 · v5.0.8

1 parent [00494b9](#) commit 707171c

7 files changed +32 -7 lines changed

[↑ Top](#)

- ∨ modules
 - ∨ profile
 - profile_new.php
 - registration.php
- ∨ src
 - ∨ Session/Entity
 - Session.php
 - ∨ UI/Presenter
 - RegistrationPresenter.php
- ∨ system/classes
 - ModuleContacts.php
- ∨ themes/simple/templates
 - ∨ modules
 - contacts.assign.tpl
 - ∨ sys-template-parts

 card.information.button.tpl

 **7 files changed** +32 -7 lines changed



modules/profile/profile_new.php



@@ -52,6 +52,11 @@

```

52 52         foreach ($getUserUuids as $userUuid) {
53 53             // read user data
54 54             if (!$gValidLogin || $getAcceptRegistration) {
55 +                 if ($getAcceptRegistration) {
56 +                     // check the CSRF token of the form against the session token
57 +                     SecurityUtils::validateCsrfToken($_POST['adm_csrf_token']);
58 +                 }
59 +
55 60             // create a user registration object and set requested organization
56 61             $user = new UserRegistration($gDb, $gProfileFields);
57 62             $user->readDataByUuid($userUuid);

```



modules/registration.php



@@ -88,6 +88,9 @@

```

88 88         $page->createContentAssignUser($registrationUser, true);
89 89         $page->show();
90 90     } elseif (in_array($getMode, array('assign_member', 'assign_user'))) {
91 +         // check the CSRF token of the form against the session token
92 +         SecurityUtils::validateCsrfToken($_POST['adm_csrf_token']);
93 +
91 94         $registrationService = new RegistrationService($gDb, $getUserUUID);
92 95         $message = $registrationService-
>assignRegistration($getUserUUIDAssigned, $getMode === 'assign_member');
93 96
91 94         $registrationService = new RegistrationService($gDb, $getUserUUID);
92 95         $message = $registrationService-
>assignRegistration($getUserUUIDAssigned, $getMode === 'assign_member');
93 96
104 107         exit();
105 108     } elseif ($getMode === 'create_user') {
106 109         // accept a registration, assign necessary roles and send a
notification email
110 +
111 +         // check the CSRF token of the form against the session token

```

```

112 + SecurityUtils::validateCsrfToken($_POST['adm_csrf_token']);
113 +
107 114 $registrationUser->acceptRegistration();
108 115
109 116 // if current user has the right to assign roles then show roles dialog

```

src/Session/Entity/Session.php

```

@@ -150,12 +150,12 @@ protected function clearUserData()
150 150
151 151 /**
152 152 * Returns a CSRF token from the session. If no CSRF token exists a new one
will be
153 - * generated and stored within the session. The next call of the method
will than
153 + * generated and stored within the session. The next call of the method
will then
154 154 * return the existing token. The CSRF token has 30 characters. A new token
could
155 155 * be forced by the parameter **$newToken**
156 156 * @param bool $newToken If set to true, always a new token will be
generated.
157 157 * @return string Returns the CSRF token
158 - * @throws Exception
158 + * @throws \Exception
159 159 */
160 160 public function getCsrftoken(bool $newToken = false): string
161 161 {

```

src/UI/Presenter/RegistrationPresenter.php

```

@@ -89,8 +89,14 @@ public function createRegistrationList(): void
89 89 'name' => $gl10n->get('SYS_ASSIGN_REGISTRATION')
90 90 );
91 91 } else {
92 + if ($gCurrentUser->isAdministratorUsers() {
93 + $url = SecurityUtils::encodeUrl(ADMIDIO_URL .
FOLDER_MODULES.'/profile/profile_new.php', array('accept_registration' => true,
'user_uuid' => $row['usr_uuid']));

```

```

94 +         } else {
95 +             $url = SecurityUtils::encodeUrl(ADMIDIO_URL .
FOLDER_MODULES.'/registration.php', array('mode' => 'create_user', 'user_uuid'
=> $row['usr_uuid']));
96 +         }
92 97             $templateRow['buttons'][] = array(
93 -                 'url' => ($gCurrentUser->isAdministratorUsers() ?
SecurityUtils::encodeUrl(ADMIDIO_URL .
FOLDER_MODULES.'/profile/profile_new.php', array('accept_registration' => true,
'user_uuid' => $row['usr_uuid'])) : SecurityUtils::encodeUrl(ADMIDIO_URL .
FOLDER_MODULES.'/registration.php', array('mode' => 'create_user', 'user_uuid'
=> $row['usr_uuid'))),
98 +                 'csrfToken' => $gCurrentSession->getCsrftoken(),
99 +                 'url' => $url,
94 100                 'name' => $gL10n->get('SYS_CONFIRM_REGISTRATION')
95 101             );
96 102         }

```

system/classes/ModuleContacts.php

```

@@ -45,7 +45,7 @@ public function __construct(string $id, string $headline =
'')
45 45         */
46 46         public function createContentAssignUser(User $user, bool
$assignRegistration = false)
47 47         {
48 -             global $gL10n, $gSettingsManager, $gCurrentUser, $gDb, $gProfileFields,
$gCurrentOrganization;
48 +             global $gL10n, $gSettingsManager, $gCurrentUser, $gDb, $gProfileFields,
$gCurrentOrganization, $gCurrentSession;
49 49
50 50             $templateData = array();
51 51             $userUuid = $user->getValue('usr_uuid');
@@ -127,11 +127,13 @@ public function createContentAssignUser(User $user,
bool $assignRegistration = f
127 127                 $button['icon'] = 'bi-person-check-fill';
128 128                 $button['url'] = SecurityUtils::encodeUrl(ADMIDIO_URL .
FOLDER_MODULES . '/registration.php', array('user_uuid' => $userUuid,
'user_uuid_assigned' => $similarUser->getValue('usr_uuid'), 'mode' =>
'assign_member'));

```

```

129 129         }
130 130 +         $button['csrfToken'] = $gCurrentSession->getCsrfToken();
130 131     }
131 132     } else {
132 133         // found user is NOT a member of this organization yet
133 134         $button['label'] = $gL10n->get('SYS_ASSIGN_MEMBERSHIP');
134 135         $button['icon'] = 'bi-person-check-fill';
136 136 +         $button['csrfToken'] = $gCurrentSession->getCsrfToken();
135 137
136 138         if($assignRegistration) {
137 139             $button['url'] = SecurityUtils::encodeUrl(ADMIDIO_URL .
FOLDER_MODULES . '/registration.php', array('user_uuid' => $userUuid,
'user_uuid_assigned' => $similarUser->getValue('usr_uuid'), 'mode' =>
'assign_user'));
@@ -156,6 +158,7 @@ public function createContentAssignUser(User $user, bool
$assignRegistration = f
156 158         $templateData[] = $templateRow;
157 159     }
158 160
161 161 +     $this->smarty->assign('csrfToken', $gCurrentSession->getCsrfToken());
159 162     $this->smarty->assign('similarUsers', $templateData);
160 163     $this->smarty->assign('l10n', $gL10n);
161 164     $this->pageContent .= $this->smarty-
>fetch('modules/contacts.assign.tpl');

```

```

...imple/templates/modules/contacts.assign.tpl
@@ -19,7 +19,7 @@
19 19         {if {array_key_exists array=$similarUser key='button'}}
20 20             <br />
21 21             <p>{$similarUser.button.description}</p>
22 22 -             <button class="btn btn-primary"
onclick="window.location.href='{$similarUser.button.url}'">
22 22 +             <button class="btn btn-primary"
onclick="redirectPost('{$similarUser.button.url}',{ adm_csrf_token:
'{$similarUser.button.csrfToken}' });">
23 23             <i class="bi {$similarUser.button.icon}"></i>
{$similarUser.button.label}</button>
24 24             {/if}
25 25         </li>

```

```

@@ -32,7 +32,7 @@
32 32     <div class="card-body">
33 33         <p>{{110n->get('SYS_CONTACT_NOT_FOUND_CREATE_NEW')}}</p>
34 34
35 35 -         <button class="btn btn-primary"
           onclick="window.location.href='{{createNewUserUrl}}'">
35 35 +         <button class="btn btn-primary"
           onclick="redirectPost('{{createNewUserUrl}}', { adm_csrf_token: '{{csrfToken}}'
           });">
36 36         <i class="bi bi-plus-circle-fill"></i>{{110n->
           get('SYS_CREATE_CONTACT')}}</button>
37 37     </div>
38 38 </div>

```

```

...-template-parts/card.information.button.tpl
@@ -22,7 +22,11 @@
22 22     </ul>
23 23     {if {array_key_exists array=$card key="buttons"} &&
           count($card.buttons) > 0}
24 24     {foreach $card.buttons as $buttonItem}
25 25 -         <a class="btn btn-primary mt-auto" href="{{buttonItem.url}}">
           {{buttonItem.name}}</a>
25 25 +         {if isset($buttonItem.csrfToken)}
26 26 +         <a class="btn btn-primary mt-auto"
           onclick="redirectPost('{{buttonItem.url}}', { adm_csrf_token:
           '{{buttonItem.csrfToken}}' });">{{buttonItem.name}}</a>
27 27 +         {else}
28 28 +         <a class="btn btn-primary mt-auto" href="
           {{buttonItem.url}}">{{buttonItem.name}}</a>
29 29 +         {/if}
26 30     {/foreach}
27 31     {/if}
28 32 </div>

```

Comments 0



Please [sign in](#) to comment.