Admidio / **admidio** Public

Code Issues 158 Pull requests 2 Actions Projects Security and qua

Commit `00494b9`

Fasse committed 4 days ago

```
Merge commit from fork

fix: CSRF and Form Validation Bypass in Inventory Item Save via 'impo…
```

v5.0 · v5.0.8

1 parent 317ec91 commit 00494b9

4 files changed +16 -9 lines changed

Top

Filter files…

- src
  - Inventory/Service
    - ImportService.php
    - ItemService.php
  - UI/Presenter
    - InventoryImportPresenter.php
- themes/simple/templates/modules
  - inventory.import.assign-fields.tpl

4 files changed +16 -9 lines changed

Search within code

src/Inventory/Service/ImportService.php

```
@@ -451,10 +451,12 @@ public function importItems(): array
451 451                     $itemModule->save();
452 452
453 453                     $importSuccess = true;
454     -                   unset($_POST);
```

```
455  454              }
456  455          }
457  456
     457  +       // cleanup the post data after the import
     458  +       unset($_POST);
     459  +
458  460          // Send notification to all users
459  461          $items->sendNotification($importedItemData);
460  462
     @@ -463,7 +465,6 @@ public function importItems(): array
463  465              $returnMessage['message'] = $gL10n->get('SYS_SAVE_DATA');
464  466          } else {
465  467              $returnMessage['message'] = $gL10n->get('SYS_INVENTORY_NO_NEW_IMPORT_DATA');
466       -
467  468          }
468  469
469  470          return $returnMessage;
```

src/Inventory/Service/ItemService.php

```
     @@ -101,12 +101,8 @@ public function save(bool $multiEdit = false): void
101  101          global $gCurrentSession, $gL10n, $gSettingsManager;
102  102
103  103          // check form field input and sanitized it from malicious content
104       -        if (!$this->postImported) {
105       -            $itemFieldsEditForm = $gCurrentSession->getFormObject($_POST['adm_csrf_token']);
106       -            $formValues = $itemFieldsEditForm->validate($_POST, $multiEdit);
107       -        } else {
108       -            $formValues = $_POST;
109       -        }
     104  +       $itemFieldsEditForm = $gCurrentSession->getFormObject($_POST['adm_csrf_token']);
     105  +       $formValues = $itemFieldsEditForm->validate($_POST, $multiEdit);
110  106
111  107          $startIdx = 1;
112  108          if ($this->postCopyField > 0) {
```

src/UI/Presenter/InventoryImportPresenter.php

```
@@ -311,11 +311,19 @@ public function createAssignFieldsForm(): void
311 311                         'class' => 'admidio-import-field'
312 312                     )
313 313                 );
    314 +
    315 +             // hidden input field for import validation (security check if the form payload includes unexpected fields)
    316 +             $form->addInput(
    317 +                 'INF-' . $itemField->GetValue('inf_name_intern'),
    318 +                 $itemField->GetValue('inf_name'),
    319 +                 '',
    320 +                 array('hidden' => true, 'property' => FormPresenter::FIELD_HIDDEN)
    321 +             );
314 322             }
315 323
316 324             $form->addSubmitButton('btn_forward', $gL10n->get('SYS_IMPORT'), array('icon' => 'fa-upload'));
317 325
318 326             $form->addToHtmlPage();
319 327             $gCurrentSession->addFormObject($form);
320 328         }
321     - }
    329 + }
```

.../modules/inventory.import.assign-fields.tpl

```
@@ -23,6 +23,8 @@
23 23                         <div class="card-body">
24 24                 {/if}
25 25                 {include 'sys-template-parts/form.select.tpl' data=$itemField}
    26 +         {elseif {string_contains haystack=$key needle="INF-"}}
    27 +             {include 'sys-template-parts/form.input.tpl' data=$itemField}
26 28             {/if}
27 29         {/foreach}
28 30         </div></div>
```

Comments 0

Please sign in to comment.