chamilo / **chamilo-lms** Public

Code | Issues 415 | Pull requests 12 | Discussions | Actions | Projects

Commit `f03f681`

AngelFQC committed last month Verified

```
Security: Strengthen evaluation editing logic by adding course ownership and ID
validation to prevent unauthorized access.

See advisory GHSA-9h22-wrg7-82q6
```

`master` · v2.0.0-RC.3

1 parent `740f5a6` commit `f03f681`

2 files changed +25 -12 lines changed

Top

Filter files…

- public/main/gradebook
  - gradebook_edit_eval.php
  - lib/be
    - evaluation.class.php

2 files changed +25 -12 lines changed

Search within code

public/main/gradebook/gradebook_edit_eval.php

```
@@ -12,9 +12,21 @@
12 12   GradebookUtils::block_students();
13 13
14 14   $evaledit = Evaluation::load($_GET['editeval']);
15    - if ($evaledit[0]->is_locked() && !api_is_platform_admin()) {
16    -     api_not_allowed();
   15 + if (empty($evaledit[0])) {
   16 +     api_not_allowed(true);
17 17   }
```

```
+ if (!api_is_platform_admin()) {
+     $currentCourseId = api_get_course_int_id();
+
+     if ($evaledit[0]->getCourseId() && $evaledit[0]->getCourseId() !=
  $currentCourseId) {
+         api_not_allowed(true);
+     }
+
+     if ($evaledit[0]->is_locked()) {
+         api_not_allowed(true);
+     }
+ }
+
  $form = new EvalForm(
      EvalForm::TYPE_EDIT,
      $evaledit[0],
  @@ -28,12 +40,13 @@

      $entityManager = Database::getManager();

-     $evaluationId = $values['hid_id'];
-     if ($evaluationId) {
-         $evaluation = $entityManager->getRepository(GradebookEvaluation::class)-
  >find($evaluationId);
-     } else {
-         $evaluation = new GradebookEvaluation();
-         $entityManager->persist($evaluation);
+     $evaluationId = (int) $values['hid_id'];
+     if ($evaluationId !== (int) $evaledit[0]->get_id()) {
+         api_not_allowed(true);
+     }
+     $evaluation = $entityManager->getRepository(GradebookEvaluation::class)-
  >find($evaluationId);
+     if (!$evaluation) {
+         api_not_allowed(true);
      }

      $evaluation->setTitle($values['name']);
```

.../main/gradebook/lib/be/evaluation.class.php

```
@@ -226,7 +226,7 @@ public function set_locked($locked)
226 226          * @param ?int  $visible Whether it is visible or not
227 227          * @param ?int  $locked  Whether it is locked or not
228 228          *
229     -        * @return array
    229 +        * @return array<int, Evaluation>
230 230          * @throws Exception
231 231          */
232 232         public static function load(
@@ -236,7 +236,7 @@ public static function load(
236 236             ?int $categoryId = 0,
237 237             ?int $visible = -1,
238 238             ?int $locked = -1
239     -    ) {
    239 +    ): array {
240 240             $table = Database::get_main_table(TABLE_MAIN_GRADEBOOK_EVALUATION);
241 241             $sql = 'SELECT * FROM '.$table;
242 242             $parametersCount = 0;
@@ -950,9 +950,9 @@ public function setCourseId(?int $courseId = null):
Evaluation
950 950         /**
951 951          * @param array $result
952 952          *
953     -        * @return array
    953 +        * @return array<int, Evaluation>
954 954          */
955     -    private static function create_evaluation_objects_from_sql_result($result)
    955 +    private static function create_evaluation_objects_from_sql_result($result):
array
956 956         {
957 957             $alleval = [];
958 958             $allow = ('true' ===
api_get_setting('gradebook.allow_gradebook_stats'));
```

Comments 0

Please sign in to comment.