chamilo / **chamilo-lms** Public

Code Issues 415 Pull requests 12 Discussions Actions Projects

Commit 63e1e6d

AngelFQC committed last month · ✕ 1 / 3 · Verified

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

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

1.11.x · v1.11.38

1 parent 3b03306 commit 63e1e6d

2 files changed +23 -6 lines changed

Top

Filter files…

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

2 files changed +23 -6 lines changed

Search within code

main/gradebook/gradebook_edit_eval.php

```
@@ -10,8 +10,19 @@
10 10   GradebookUtils::block_students();
11 11
12 12   $evaledit = Evaluation::load($_GET['editeval']);
13    - if ($evaledit[0]->is_locked() && !api_is_platform_admin()) {
14    -     api_not_allowed();
   13 + if (empty($evaledit[0])) {
   14 +     api_not_allowed(true);
   15 + }
```

```
      16  + if (!api_is_platform_admin()) {
      17  +     $currentCourseCode = api_get_course_id();
      18  +
      19  +     if ($evaledit[0]->get_course_code() && $evaledit[0]->get_course_code() !=
          $currentCourseCode) {
      20  +         api_not_allowed(true);
      21  +     }
      22  +
      23  +     if ($evaledit[0]->is_locked()) {
      24  +         api_not_allowed(true);
      25  +     }
15    26    }
16    27    $form = new EvalForm(
17    28        EvalForm::TYPE_EDIT,
          @@ -23,6 +34,12 @@
23    34    );
24    35    if ($form->validate()) {
25    36        $values = $form->exportValues();
      37  +
      38  +     $evaluationId = (int) $values['hid_id'];
      39  +     if ($evaluationId !== (int) $evaledit[0]->get_id()) {
      40  +         api_not_allowed(true);
      41  +     }
      42  +
26    43        $eval = new Evaluation();
27    44        $eval->set_id($values['hid_id']);
28    45        $eval->set_name($values['name']);
```

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

```
          @@ -221,7 +221,7 @@ public function set_locked($locked)
221   221         * @param int    $category_id parent category
222   222         * @param int    $visible     visible
223   223         *
224       -       * @return array
      224   +     * @return array<int, Evaluation>
225   225         */
226   226        public static function load(
227   227            $id = null,
          @@ -230,7 +230,7 @@ public static function load(
```

```
230  230            $category_id = null,
231  231            $visible = null,
232  232            $locked = null
233       -      ) {
     233  +      ): array {
234  234            $table = Database::get_main_table(TABLE_MAIN_GRADEBOOK_EVALUATION);
235  235            $sql = 'SELECT * FROM '.$table;
236  236            $paramcount = 0;
     ↓ ↑   @@ -935,9 +935,9 @@ public function getSkillsFromItem(): string
935  935        /**
936  936         * @param array $result
937  937         *
938       -      * @return array
     938  +      * @return array<int, Evaluation>
939  939         */
940       -      private static function create_evaluation_objects_from_sql_result($result)
     940  +      private static function create_evaluation_objects_from_sql_result($result): array
941  941        {
942  942            $alleval = [];
943  943            $allow = api_get_configuration_value('allow_gradebook_stats');
     ↓
```

Comments 0

Please sign in to comment.