0-DAY NO CVE MEDIUM PUBLIC

Moodle, core_grades_get_gradeitems hidden catalogue

Moodle 5.2.3 core_grades_get_gradeitems has no require_capability. Sibling get_grade_tree already requires grade:viewall. An enrolled student AJAX-reads hidden grade-item names the student gradebook UI still hides. No CVE yet.

NAME Moodle, core_grades_get_gradeitems hidden catalogue	TYPE 0-day analysis
CVE n/a	CVE RISK medium
DISCLOSURE STATUS public	VENDOR Moodle
AFFECTED Moodle LMS 5.2.3 tag v5.2.3 (344232c). Enrolled student. ajax plus official mobile service. Live install lab.	PUBLISHED 12 Oct 2026
UPDATED 12 Oct 2026	TAGS 0-day, moodle, idor, grades, cwe-862, cwe-200, authenticated

TL;DR

Lab files and proof-of-concept here.

01 the student UI hid it. the AJAX catalogue did not

I am @abraxas_null. The proof of concept is on GitHub: **abraxas/moodle-grades-gradeitems** (loopback client). The lab stack is `lab/`: Dockerfile, docker-compose.yml, run.sh, poc.py, seed.php. Authorized lab only. It talks to loopback.

This is **Moodle LMS 5.2.3** (`344232c15336c71b80f9aca8359ce0e0a9f3d116`). No CVE yet. CWE-862 / CWE-200. 4.3 Medium (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N`). Remote IDOR. Enrolled student. Catalogue leak, not scores. Not RCE.

`core_grades_get_gradeitems` is ajax plus the official mobile service, with no `capabilities` key in `lib/db/services.php`. `validate_context` is the only gate. Then `grade_item::fetch_all` dumps every item in the course. The filter drops `GRADE_TYPE_NONE`, category items, and the course item. Hidden is not in that filter. Sibling `core_grades_get_grade_tree` already requires `moodle/grade:viewall`.

Same pin: Blackboard img file read, enrol_database SQLi, grades feedback IDOR.

02 Why this service

Grade web services were in the MSA-26-0016 window. I was already in `public/grade/classes/external/` for the feedback leftover. `get_gradeitems.php` has no `require_capability` at all. That is a different class of miss: not a forgotten group check, a forgotten cap.

I only wanted Critical or High, with Medium if a student could see structure the UI hid. Hidden extra-credit items, unpublished assignments, the names of things the teacher is still writing: that is a catalogue leak. The return schema has no scores. I am not inflating it.

03 Pinning v5.2.3

Same tag. `public/lib/db/services.php` 1099-1105 registers the method as ajax + `MOODLE_OFFICIAL_MOBILE_SERVICE` and does not name a capability. `get_grade_tree.php` 65-68 already does `require_capability('moodle/grade:viewall', $context)`. Incomplete sibling **inside** `core_grades`.

04 The skip list

Same MSA-26 list. Do not re-file group checks that landed. Do not re-file XML grade CSRF. This post is the service with no cap.

05 Surfaces that returned nothing

Unauthenticated AJAX is `servicerequireslogin`. A logged-in user who is not enrolled is `requireloginerror`. Those are closed. The student gradebook UI already hides the item. If AJAX matched the UI, this leftover would not exist.

I also looked at whether the return included grades. It does not. Keys are `id`, `itemname`, `category`. That is why the class is catalogue IDOR, not a score read.

06 The handler

`public/grade/classes/external/get_gradeitems.php`:

PHP Copy

```php
$warnings = [];
$context = context_course::instance($params['courseid']);
parent::validate_context($context);

$allgradeitems = grade_item::fetch_all(['courseid' => $params['courseid']]);
$gradeitems = array_filter($allgradeitems, function($item) {
    $item->itemname = $item->get_name();
```

```
    $item->category = $item->get_parent_category()->get_name();
    return $item->gradetype != GRADE_TYPE_NONE && !$item->is_category_item() &&
});

return [
    'gradeItems' => $gradeitems,
    'warnings' => $warnings,
];
```

Sibling `get_grade_tree.php`:

PHP Copy

```php
$context = \context_course::instance($params['courseid']);
parent::validate_context($context);
// Make sure that the user has the capability to view the full grade tree in the
require_capability('moodle/grade:viewall', $context);
```

Service registration:

PHP Copy

```php
'core_grades_get_gradeitems' => [
    'classname' => 'core_grades\external\get_gradeitems',
    'description' => 'Get the gradeitems for a course',
    'type' => 'read',
    'ajax' => true,
    'services' => [MOODLE_OFFICIAL_MOBILE_SERVICE],
],
```

No `capabilities` key.

07 The lab

Live Moodle **v5.2.3** on php:8.3-apache + MariaDB 11.4. Compose project `moodle-grades-gradeitems`. Loopback `:19590`. Seed enrols `labstudent`, leaves

`laboutsider` out of the course, and creates a visible manual item plus a hidden item whose name is the witness. `run.sh` copies a local pin or clones tag `v5.2.3`. The Moodle tree is not in the pack.

Unauth AJAX: HTTP 200, error, `servicerequireslogin`. Outsider: `requireloginerror`. Student AJAX names: `Visible Lab Assignment` and `MOODLE-GRADES-GRADEITEMS-WITNESS`. Same session's gradebook UI: hidden name absent, visible name present.

PLAIN TEXT Copy

```
SUCCESS moodle-grades-gradeitems student-ajax=200 hidden-in-ajax=yes hidden-in-ui
```

PLAIN TEXT Copy

```
python3 moodle-grades-gradeitems-Abraxas-Labs.py
```

or `cd lab && ./run.sh`. Target only `http://127.0.0.1:19590`. Stack tears down after the run.

08 Wrong turns, in the order I made them

Treating unauth AJAX 200 as the leak. Body is `servicerequireslogin`. HTTP 200 with `error: true` is Moodle's AJAX envelope, not success.

Calling this a score IDOR because the method name has `grade`. Schema is names, ids, categories. No scores.

Expecting `get_grade_tree` to be the same leftover. It already requires `viewall`. That is the control.

Mobile-only. The service is ajax plus mobile. Lab used AJAX. The registration is the inferred mobile path.

A reverse shell. Theatre. The oracle is the hidden name in AJAX and its absence in the student UI.

09 What an attacker can do

Writer: an enrolled student in the course. They POST the AJAX service with `{courseid}`. The response is names, IDs, and categories.

Class: IDOR. **Reach:** Remote.

PRIVILEGE	METHOD / SINK
Read hidden grade-item name, id, and category	POST `/lib/ajax/serv` `sesskey=` `core_grades_get_gra` `{courseid}`
Read visible grade-item name, id, and category	Same response
Same catalogue over the official mobile service	Same class, `MOODLE_OFFICIAL_MOB`
Walk sequential `courseid` values for courses the student can enter	Same method, guesse
See the hidden item in the student gradebook UI	GET `/grade/report/user/` `id=`
Call without a session	AJAX with a dummy se

PRIVILEGE	METHOD / SINK
Call as a logged-in user who is not enrolled	outsider AJAX, same c
Read other students' scores or write grades	n/a
PHP RCE / OS LPE	n/a

A teacher or manager who already has `moodle/grade:viewall` already sees the catalogue.

10 The fix

After `validate_context`, require the same cap as `get_grade_tree`: `require_capability('moodle/grade:viewall', $context)`. Also drop hidden items unless the caller has `moodle/grade:viewhidden`. Add a Behat/PHPUnit case: enrolled student, hidden manual item, `core_grades_get_gradeitems` must omit that item (or 403). Student gradebook UI already hides it.

I am not going to print an AJAX POST you can paste at someone else's course. The missing cap is the useful part. If you own the site, run the proof of concept against loopback.

11 References

- Proof of concept: abraxas/moodle-grades-gradeitems · moodle-grades-

gradeitems-Abraxas-Labs.py

- Lab: `lab/` · Dockerfile · docker-compose.yml · run.sh · poc.py · seed.php
- @abraxas_null · github.com/abraxas · abraxaslabs.tech · abraxas.null@proton.me
- CWE-862 · CWE-200
- Tree: moodle/moodle v5.2.3 (`344232c`) · `get_gradeitems.php` · `get_grade_tree.php` · `services.php`
- Same pin: moodle-blackboard-img · moodle-enrol-database-sqli · moodle-grades-feedback-idor

Independent research. Private analysis by arrangement. No ads. abraxas.null@proton.me · For defensive awareness and authorized testing only.

© 2026 Abraxas Labs