CVE-2024-43425 - Remote Code Execution Risk in Moodle's Calculated Question Types

What Is CVE-2024-43425?

CVE-2024-43425 is a vulnerability in Moodle’s implementation of “calculated question types”. Moodle uses PHP to process user-submitted formulas for these questions. Due to loose input validation, a specially crafted formula input can break out of intended restrictions and inject PHP code, especially if the add/update capability is accessible to untrusted users.

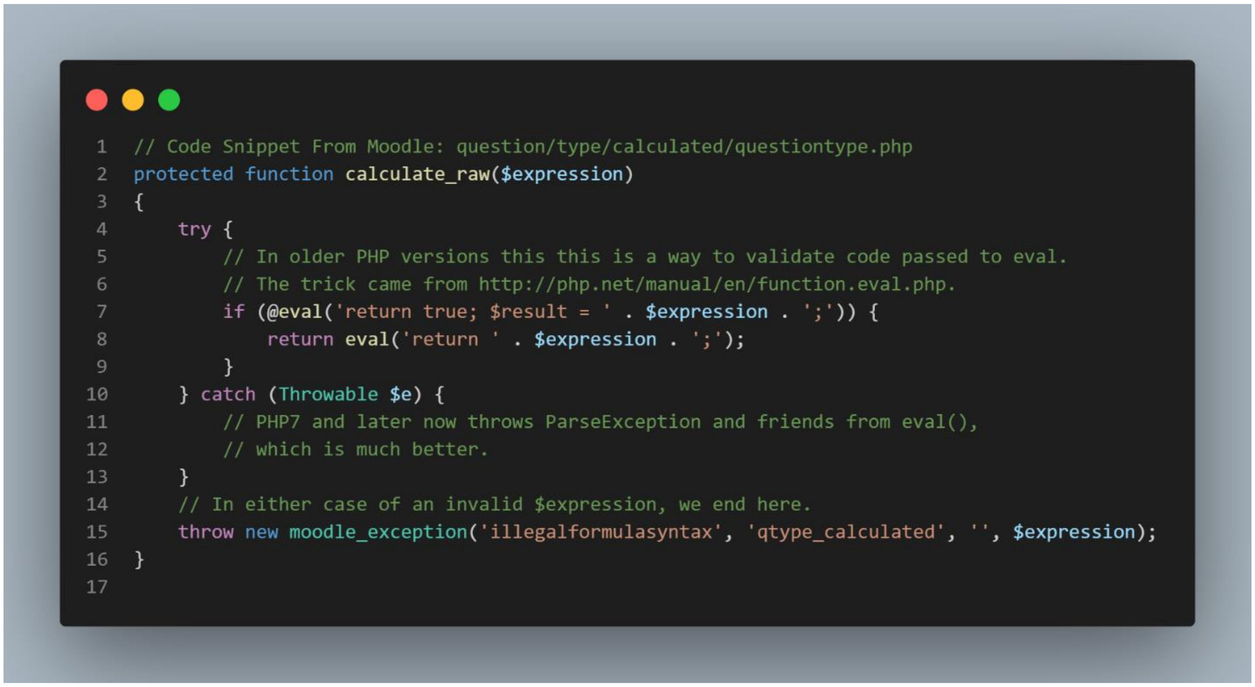
Who Is Affected?

Moodle sites/configurations where untrusted users (teachers, assistants) can create or edit calculated questions.

Technical Details

The core issue lies in how Moodle evaluates formulas in calculated questions. Before the patch, untrusted input wasn't fully sanitized before execution. The vulnerable code can be found in files handling question formulas, especially in ***/question/type/calculated/question.php***.

Vulnerable Source Code



```
1   // Code Snippet From Moodle: question/type/calculated/questiontype.php
2   protected function calculate_raw($expression)
3   {
4       try {
5           // In older PHP versions this this is a way to validate code passed to eval.
6           // The trick came from http://php.net/manual/en/function.eval.php.
7           if (@eval('return true; $result = ' . $expression . ';')) {
8               return eval('return ' . $expression . ';');
9           }
10      } catch (Throwable $e) {
11          // PHP7 and later now throws ParseException and friends from eval(),
12          // which is much better.
13      }
14      // In either case of an invalid $expression, we end here.
15      throw new moodle_exception('illegalformulasyntax', 'qtype_calculated', '', $expression);
16  }
17
```

The vulnerability is in line number 8. The user input passed to eval without any sanitized before execution.

This bug affects all versions before the fix in **4.4.2** version.

References:

- Blog 1
- Blog 2
- PHP Vulnerable Source Code