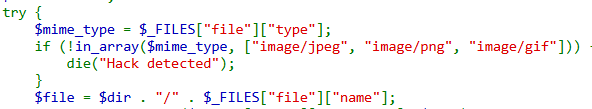
Ở level 5 này ta thấy được nó không còn kiểm tra bằng đuôi file nữa mà kiểm tra bằng kiểu dữ liệu của file   
và ta thấy nó chỉ nhận những ảnh.

Nhưng ta lại nhận ra rằng Trong PHP, $\_FILES là một siêu toàn cục được sử dụng để xử lý việc tải lên tệp. Cụ thể, $\_FILES["file"]["type"] chứa loại MIME (MIME type) của tệp tải lên. Giá trị này được trình duyệt tự động thiết lập trong quá trình tải tệp lên và được gửi kèm theo khi gửi biểu mẫu. Nó sẽ tự động thiêt lập khi gửi các phương thức nên suy ra mình có thể fake content type để fake kiểu dữ liệu cho 1 file php thành 1 file ảnh

Chứng minh giả thiết ta có sau khi fake ta được

A screenshot of a computer

Description automatically generated

Ta đã gửi thành công 1 file php lên server ta sẽ xem kết quả

A screenshot of a computer

Description automatically generated

Tấn công thành công