Ở level 2 ta đặt giả thiết, sẽ như thế nào nếu ta up 1 file có đuôi php để mod-php xử lí, liệu nó còn bị kiểm soát như level 1.

A screenshot of a phone

Description automatically generated

Nhưng ở đây hệ thống dường như đã bắt đầu quan tâm đến lỗi này và sửa chúng. Chúng ta sẽ không còn tận dụng được lỗi này nữa.

Tiếp theo ta quan sát và ấn váo debug source.

A screenshot of a computer

Description automatically generated

Dường như đây chính là source trang web

Ta để ý A computer code with text

Description automatically generated with medium confidenceTại đây ta thấy dường như hệ thống đã thông minh hơn bừng các tách tên của file ra bằng cách tách các cụm ở giữa dấu ‘,’ và kiểm tra xem ở vị trí index1 có là php hay không nếu có thì hệ thống sẽ không nhận file đó.

Sẽ như thế nào nếu ta up 1 file đuôi php nhưng php lại không nằm trong index 1?

Trong đây ta sẽ up 1 file test.html.php để test xem hệ thống có thực sự cho tôi thông qua hay không.

A screenshot of a computer

Description automatically generated

Ngay lập tức hệ thống sẽ cho tôi thông qua. Tiếp theo tôi sẽ tấn công 1 file có nội dung điều khiển hệ thống và có form file như trên và ta sẽ được kết quả như sau.

A screenshot of a phone

Description automatically generated

Thực sự hệ thống lại bị điểu khiển như level 1.