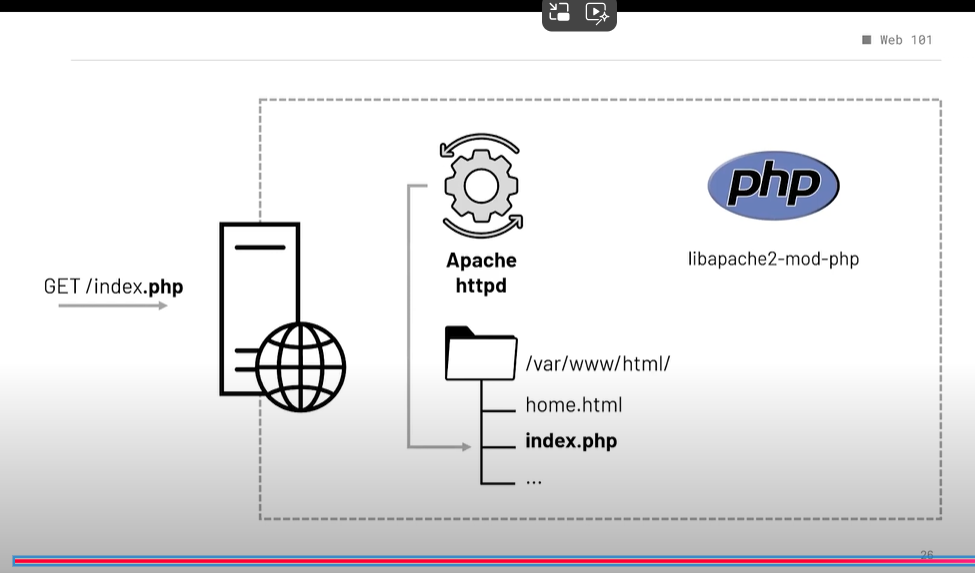
Kiến thức: Sau khi người dùng có yêu cầu request đến server thì http sẽ tiếp nhận và truy cập vào Document Roor (var/www/html) để lấy ra các file cần thiết. Httpd sẽ căn cứ vào đuôi file để quyết định xem có trả về trực tiếp hay cần phải sử lí xong mới trả về. Httpd sẽ không thể nào sử lí được file có đuôi .php nên nó sẽ đưa cho mod-php sử lí trước khi trả về cho người dùng.



Ở bài này ta sẽ tấn công server bằng lỗ hổng fileupload. Khi ta mở trang web lên ta sẽ thấy dao diện như sau: A screen shot of a computer

Description automatically generated

Ở đây ta thấy có tải file vào server và sử lí.

Sẽ như thế nào nếu ta tải 1 file bất kì cho httpd sử lí ? Trang web sẽ trả cho mình những gì?

A white background with black text

Description automatically generated

ở đây sau khi tải 1 file bất kì nó sẽ hiện ra 2 link 1 link là xe file đã tải và 1 link là xem vị trí của file.

Sẽ như thế nào nếu ta gửi lên 1 file để cho httpd xử lí và nó chuyển cho file cho mod\_php xử lí. Vậy file đó là file gì và khi sử lí xong thì nó trả về những gì.

Ở đây ta sửa gói tin thay gói tin bằng tên 1 gói tin bất kì có đuổi php để cho mod-php xử lí. Ta sẽ thay gói tin bằng 1 gói tin php vô hại để kiểm tra xem ta có thực sự tải được 1 gói tin php vào server Document root được hay không A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

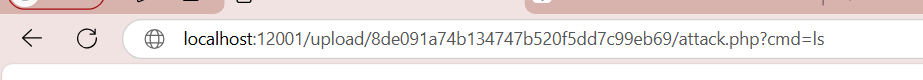
Sau khi toi dùng 1 file test để xác nhận được rằng máy chủ đã cho tôi thông qua vậy có nghĩa là tôi sẽ cho được các file khác thông qua.

Sẽ như thế nào tôi cho 1 file có câu lệnh thao tác với hệ thống như câu lệnh system, liệu rằng ta có thể kiếm soát được hệ thông hay không?

Ta sẽ dùng 1 file php có câu lệnh A screen shot of a computer

Description automatically generated

Lúc này ta gửi file đồng thời ta truyền giá trị của cmd lên trên param như sau



Lúc này ta sẽ được kết quả

A screenshot of a computer

Description automatically generated

Vậy ta thấy được hệ thống thực sự có thể bị kiểm soát bằng các thay đổi giá trị của cmd.

Đây chính là 1 bug.