Cách sửa bug của Wordpress

# Lỗi điền giá trị bất kì vào bảng wp\_postmeta (commit 8d463ab)

Các fields trong param $post\_data được lọc bằng hàm \_wp\_get\_allowed\_postdata() (dòng 266), trở thành $translated. Cụ thể, hàm này sẽ bỏ các field meta\_input, file, guid của array là argument được truyền vào (dòng 195).

Text

Description automatically generated with medium confidence

Param $translated sau đó được truyền vào hàm wp\_update\_post() thay vì param $post\_data

Graphical user interface, text, application

Description automatically generated

Như vậy ta sẽ không thể thực hiện sửa bảng wp\_postmeta thông qua việc gửi POST request với param meta\_input[…]

# Lỗi Path Traversal và LFI

Mình đã thử tìm xem có path nào khắc phục được lỗi này không nhưng không thấy. Nếu tìm được cách khác để sửa bất kì tên file trong bảng wp\_postmeta (thông qua plugin lỗi,…) thì attacker vẫn có thể thực hiện Path Traversal vào folder themes và LFI to RCE.

Ở commit 2fc33ef, Wordpress đã thêm đoạn chống Path Traversal ở hàm wp\_mkdir\_p(), trả về false nếu tên string cần check có các kí tự ../

Chart

Description automatically generated with medium confidence

A computer screen capture

Description automatically generated with medium confidence

Tuy nhiên tác dụng của hàm này là tạo folder để lưu ảnh trong trường hợp các folder mẹ không tồn tại. Do đó khi ta lưu ảnh vào folder themes (đã tồn tại) thì đoạn chống Path Traversals không có tác dụng.