Plugin Forminator 1.24.6 - Unauthenticated Remote Command Execution

- Plugin : Forminator

- Phiên bản lỗi: 1.24.6

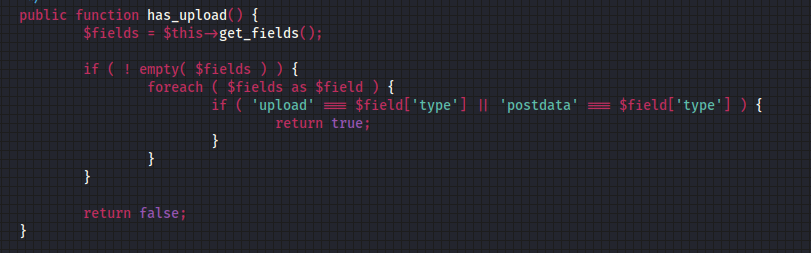
- Lỗi : Unauthenticated Remote Command Execution

a) Mô tả

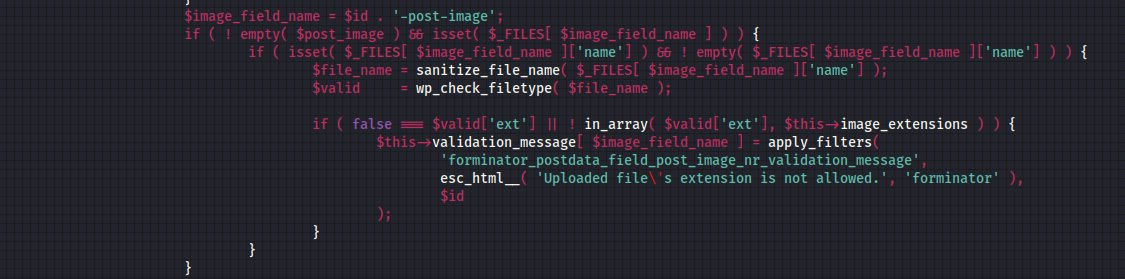
Forminator là plugin tạo biểu mẫu WordPress dễ sử dụng cho mọi trang web và mọi tình huống. Đây là cách dễ dàng nhất để tạo bất kỳ biểu mẫu nào – biểu mẫu liên hệ, biểu mẫu đặt hàng, biểu mẫu thanh toán, biểu mẫu email, tiện ích phản hồi, cuộc thăm dò tương tác với kết quả theo thời gian thực, câu đố “không trả lời sai” theo phong cách buzzfeed, công cụ ước tính dịch vụ và biểu mẫu đăng ký có thanh toán các tùy chọn bao gồm PayPal và Stripe.

b) Hàm xử lý bị lỗi

- Source code : */forminator/library/modules/custom-forms/front/front-render.php*

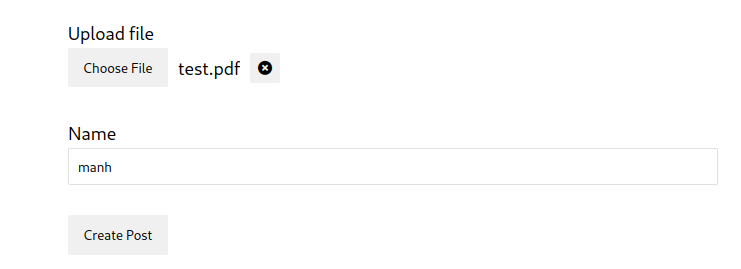


- Source code: */forminator/library/fields/postdata.php*

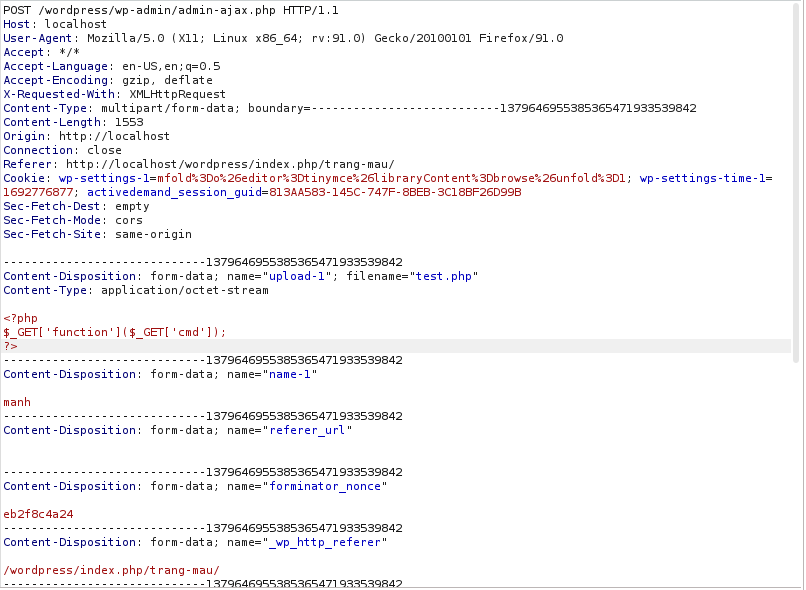


c)khai thác

- Tải 1 tệp lên bắt yêu cầu gửi lên

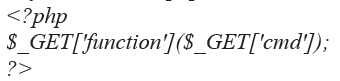


Chỉnh sửa yêu cầu gửi lên

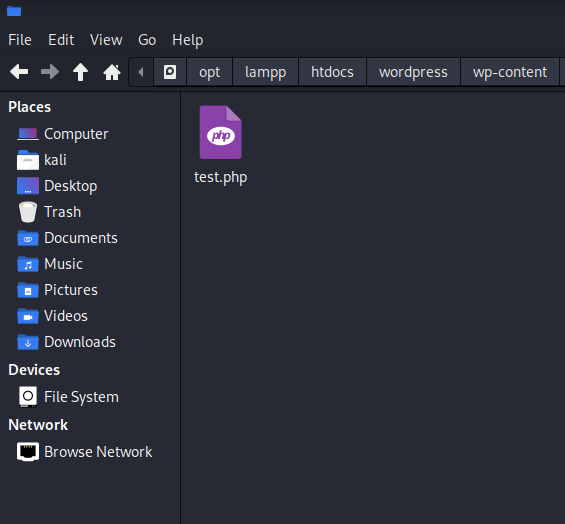


Payload

Payload file: test.php

**

Kiểm tra thư mục upload, ta thấy thư mục đã có trong thư mục



Chạy test.php

