CVE-2017-18515

- plugin : wpstatistics

- Phiên bản lỗi: 12.0.7

- Lỗi: (Authenticated) Blind SQL Injection

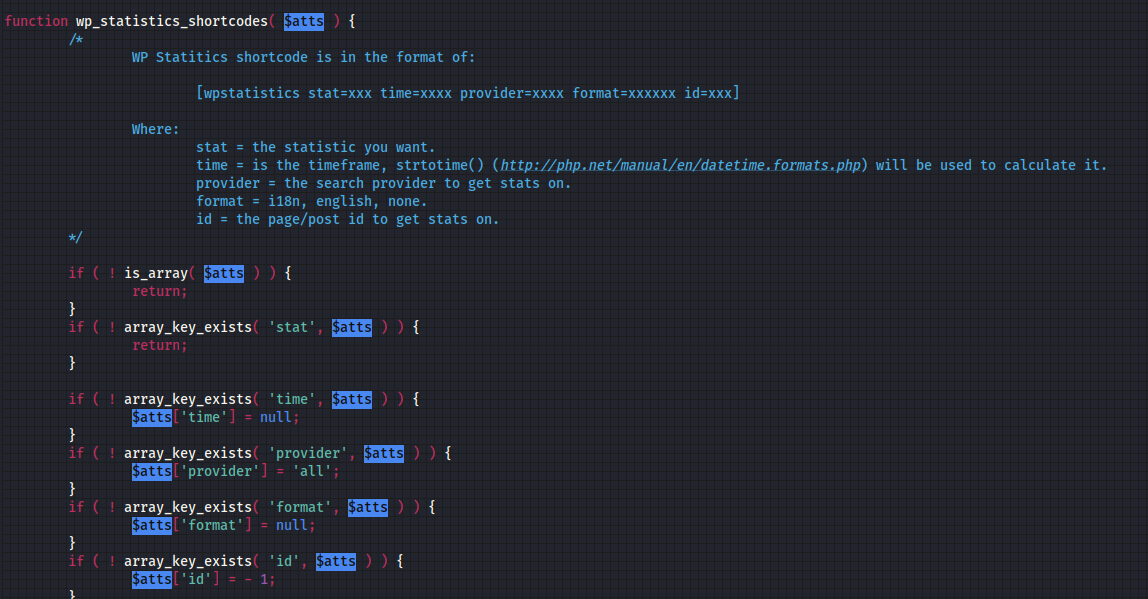
a)Mô tả

- Plugin này cho phép người dùng sử dụng 1 số các shortcode để thông kê 1 số các thông tin(số người online, tổng số người đã ghé qua page,…) .

- Nhưng do 1 không kiểm soát đầu vào chặn chẽ nên khi kẻ tấn công vào được trang quản trị thì hacker có thể từ các tham số trong shortcode để thực hiện các truy vấn độc hại.

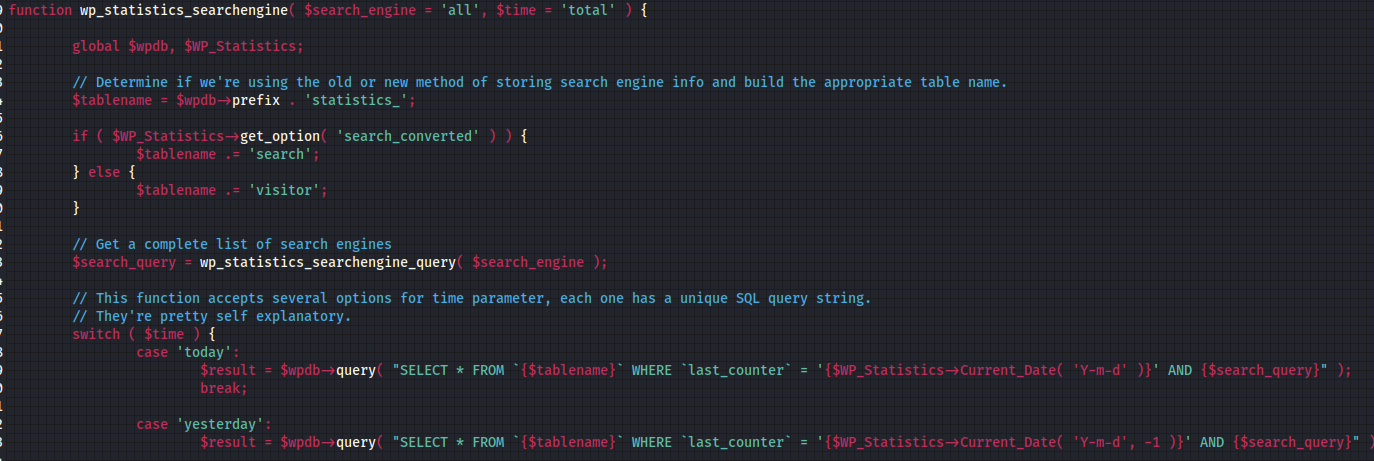
b) Hàm sử lý bị lỗi

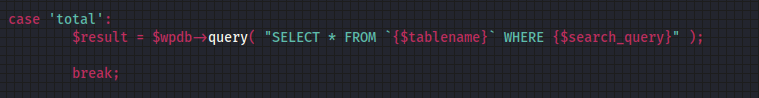
- Trong số các chức năng khác, *Thống kê WP* cho phép người dùng quản trị nhận thông tin chi tiết liên quan đến số lượt truy cập chỉ bằng cách gọi mã ngắn bên dưới:





- Một số thuộc tính của mã ngắn **wpstatistics** đang được truyền dưới dạng tham số cho các chức năng quan trọng nhưng không được làm sạch



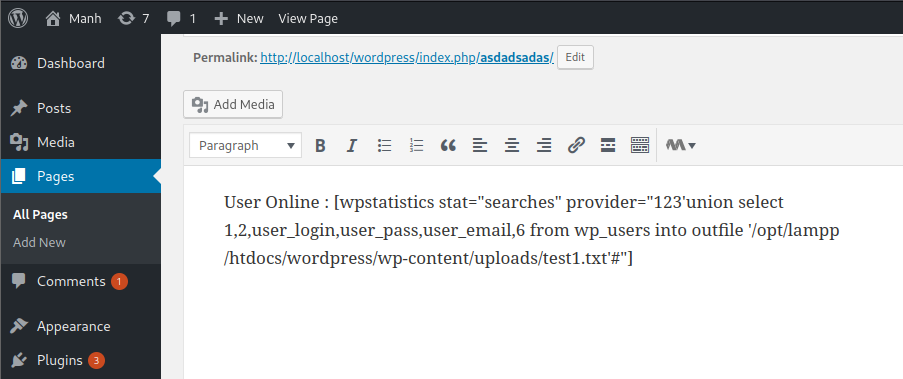


- Một trong những chức năng dễ bị tấn công **wp\_statistics\_searchengine\_query()** trong tệp “include/functions/functions.php”

- Về cơ bản, wp\_statistics\_searchengine\_query **()** trả về giá trị giống như giá trị được chuyển trong **nhà cung cấp** thuộc tính mã ngắn và nội dung của nó được thêm trực tiếp vào truy vấn SQL .

c) Khai thác

- Khi ta vào được trang admin ta vào phần page và gọi lên shortcode



Truy vấn trong thực hiện sẽ là

*SELECT \* FROM wp\_statistics\_useronline WHERE provider="123'union select 1,2,user\_login,user\_pass,user\_email,6 from wp\_users into outfile '/opt/lampp/htdocs/wordpress/wp-content/uploads/test.txt'#"*

Kết quả là kết quả của truy vấn sẽ gửi về file test.txt

