**CVE-2023-23488**

Plugin : Paid Memberships Pro

Phiên bản lỗi: <2.9.8

Lỗi : Unauthenticated Blind time-based SQLi

a)mô tả

Paid Memberships Pro (PMPro) là một plugin WordPress được sử dụng để tạo và quản lý các khách hàng trả phí trên trang web của bạn. Plugin này cung cấp một loạt các tính năng và chức năng để tạo và quản lý chương trình thành viên trả phí trên trang web của bạn.

b)hàm xử lý bị lỗi

Sử dụng REST API của Wordpress được đăng ký theo router

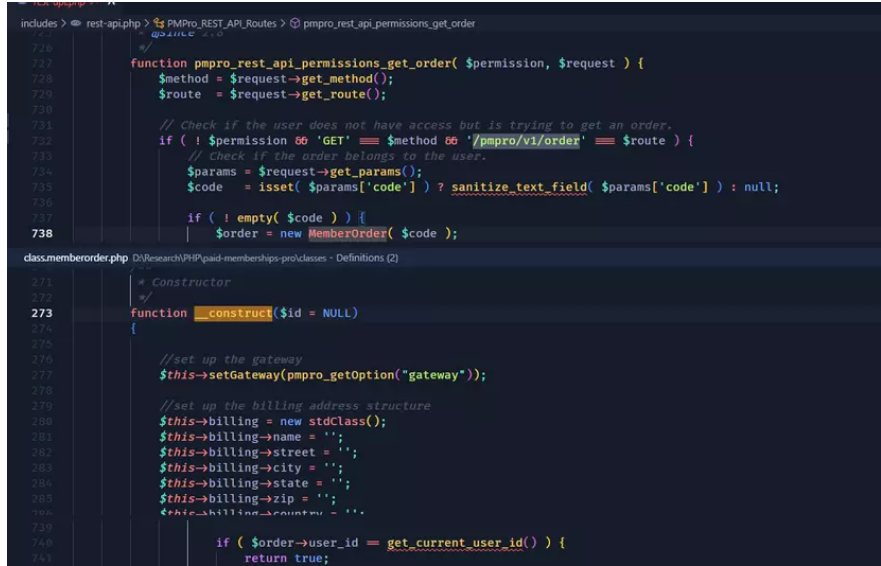


nhảy vào function pmpro\_rest\_api\_permissions\_get\_order() với

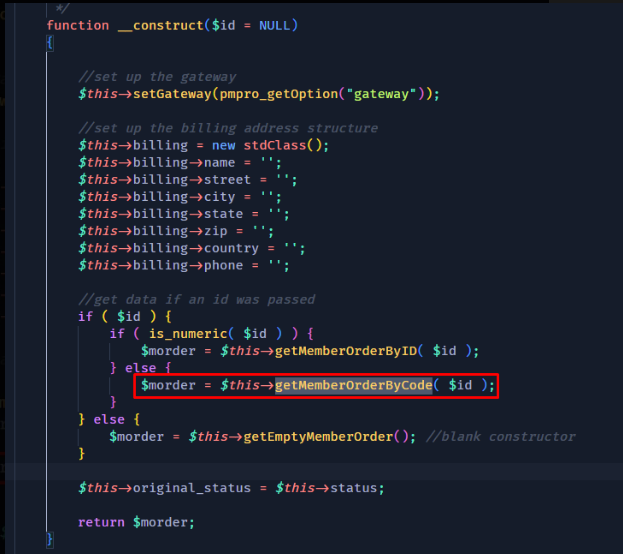
nhảy vào function pmpro\_rest\_api\_permissions\_get\_order() với

GET /?rest\_route=/pmpro/v1/order HTTP/1.1

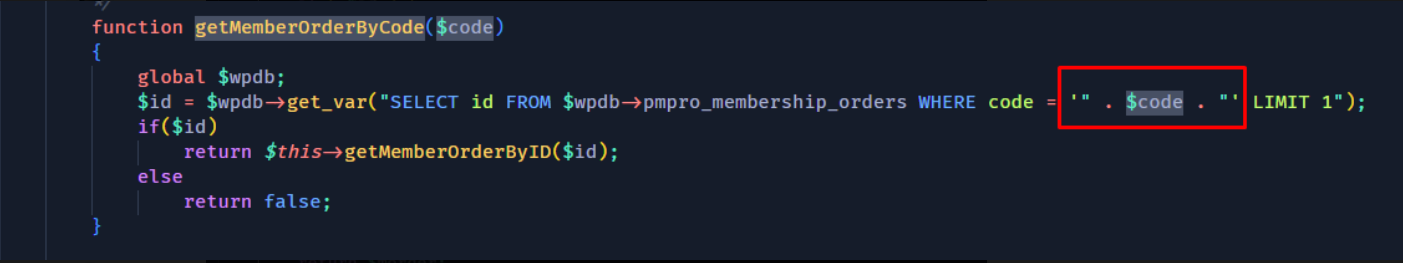
Sau đó truyền thêm tham số code vào khởi tạo MemberOrder, nhảy trực tiếp đến \_\_construct



Ở đây ta truyền giá trị code không phải là số sẽ nhảy sang function getMemberOrderByCode($id)

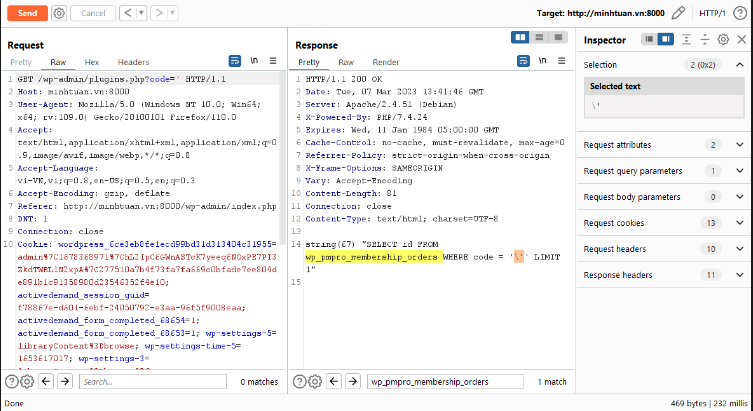


Tại đây giá trị code được truyền vào hoàn toàn không được filter hay escape gì, tại đây chúng ta có thể inject SQL vào đây theo kiểu TimeBased



c)khai thác

bắt yêu cầu từ burp

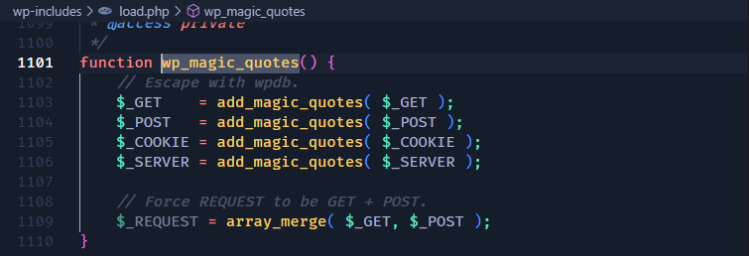


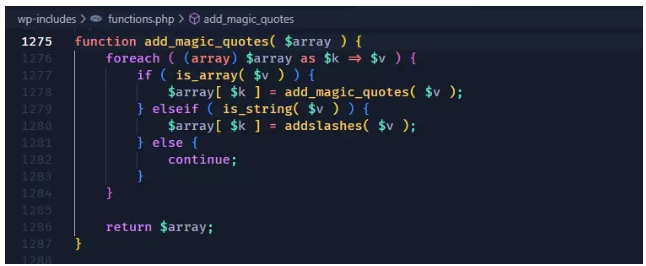
Như đã thấy rằng giá trị $\_GET['code'] đã tự động thêm dấu \ từ đây ta không thể nào break ra khỏi dấu nháy đơn để thoát khỏi string

NOTE: WordPress sẽ tự động xử lý và áp dụng addslashes() cho các giá trị này để đảm bảo rằng chúng an toàn khi được sử dụng trong các câu lệnh SQL hoặc các tình huống khác. Hàm được gọi lên ngay từ wp-setting.php



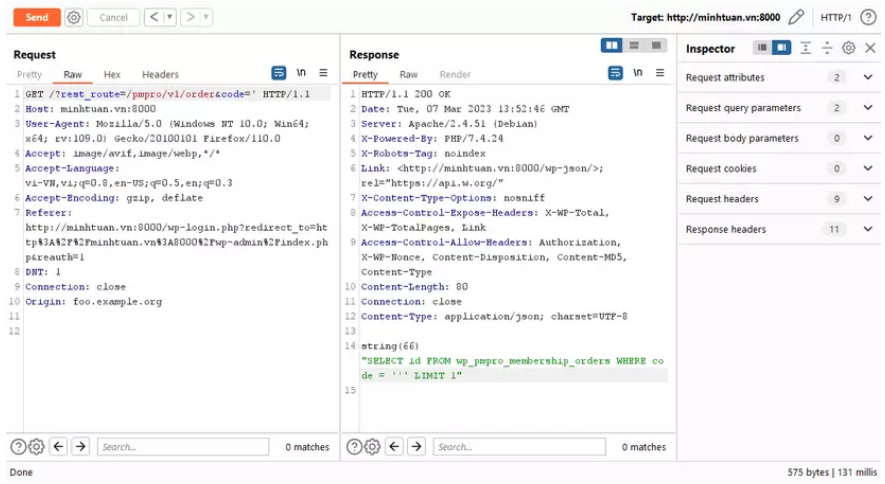
Với ghi chú rõ ràng rằng sử dụng để escape cho wpdb



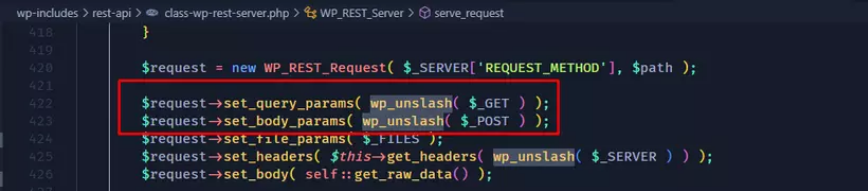


với **mọi** $\_GET, $\_POST, $\_COOKIE, $\_SERVER khi truyền từ input người dùng thì đều sẽ bị thêm slash vào.

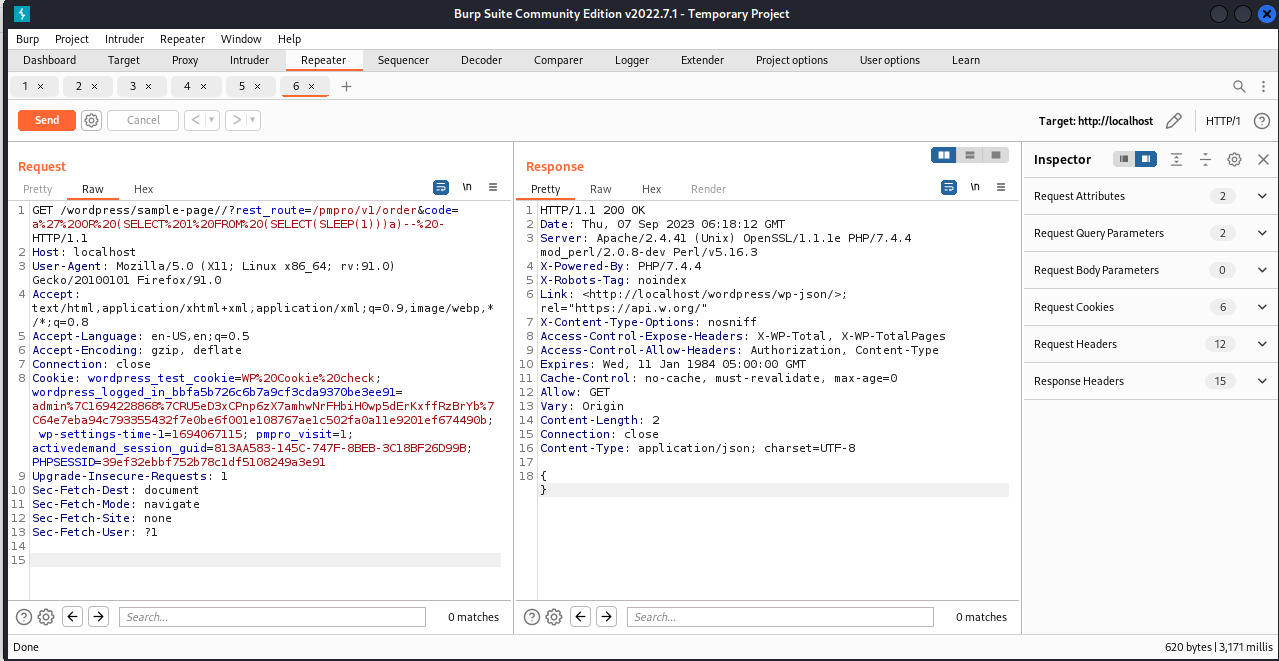
Tuy nhiên, tại sao khi sử dụng REST API thì Wordpress lại xoá mất dấu slash đi. Chúng ta có thể break ra khỏi dấu nháy đơn, inject câu lệnh SQL tuỳ ý.



Đoạn xử lý xóa dấu \



Từ đó ta chèn payload timebased vào thấy thời gian phản hồi lớn hơn 1s



d)Khai thác bằng script