Write up for crAPI

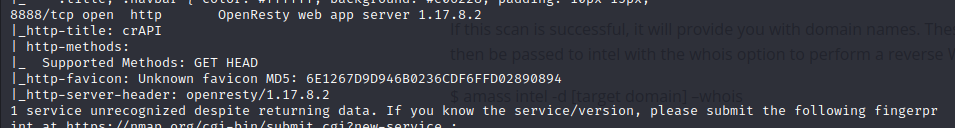
Recon

Đầu tiên chúng ta có thể thực hiện passive recon bằng google,shodan hay một số công cụ khác

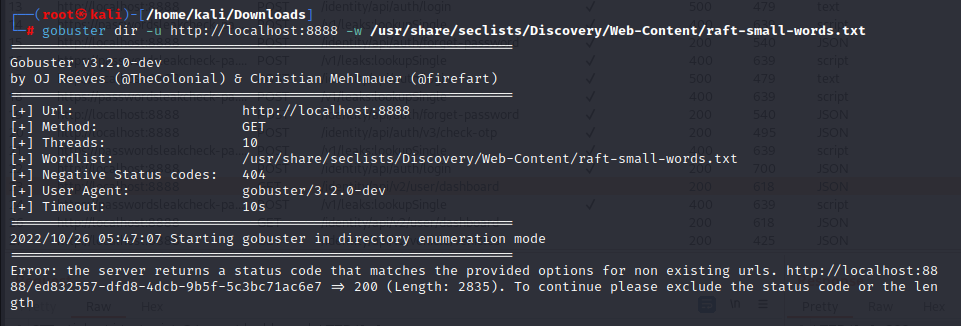
Sau đó là Active recon

Nmap

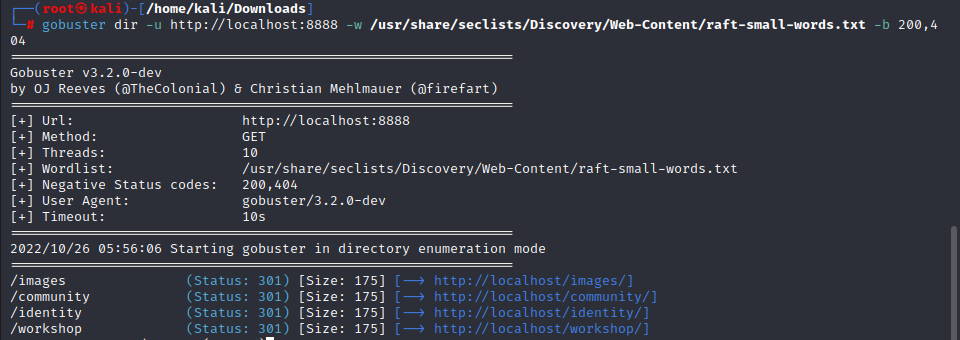
Ta biết thông tin về server: openresty/1.17.8.2 => có thế tra google tìm CVE của version này



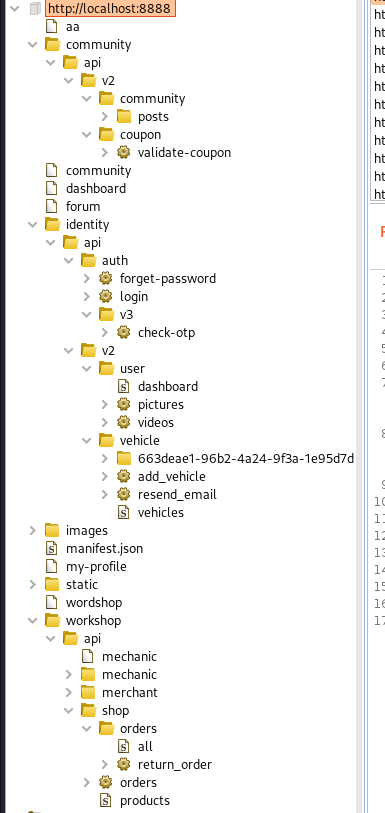
Gobuster

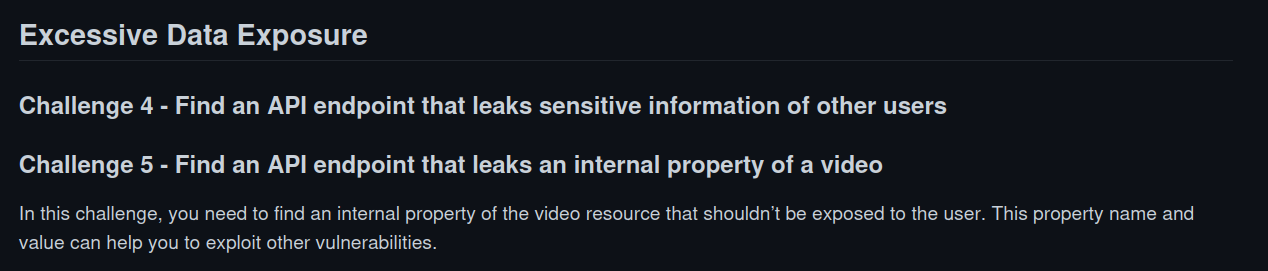


Server tự động redirect nên cả những url invalid cũng được trả về 200 và redirect đến dashboard nên chúng ta filter 200 và 404 đi = -b 200,404

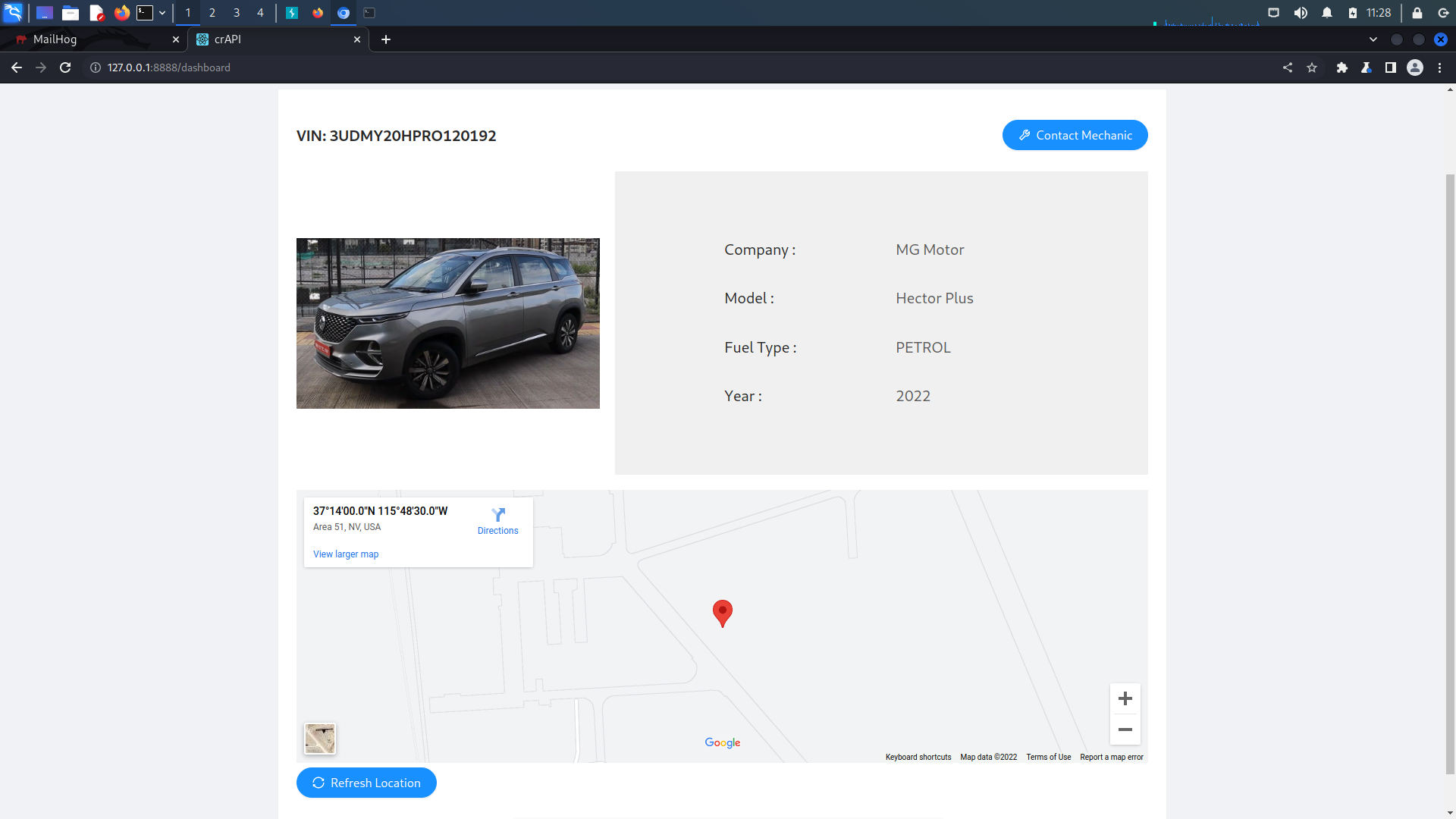


Burp Site map => dạo một vòng và thử hết chức năng trên web site ta được một list api

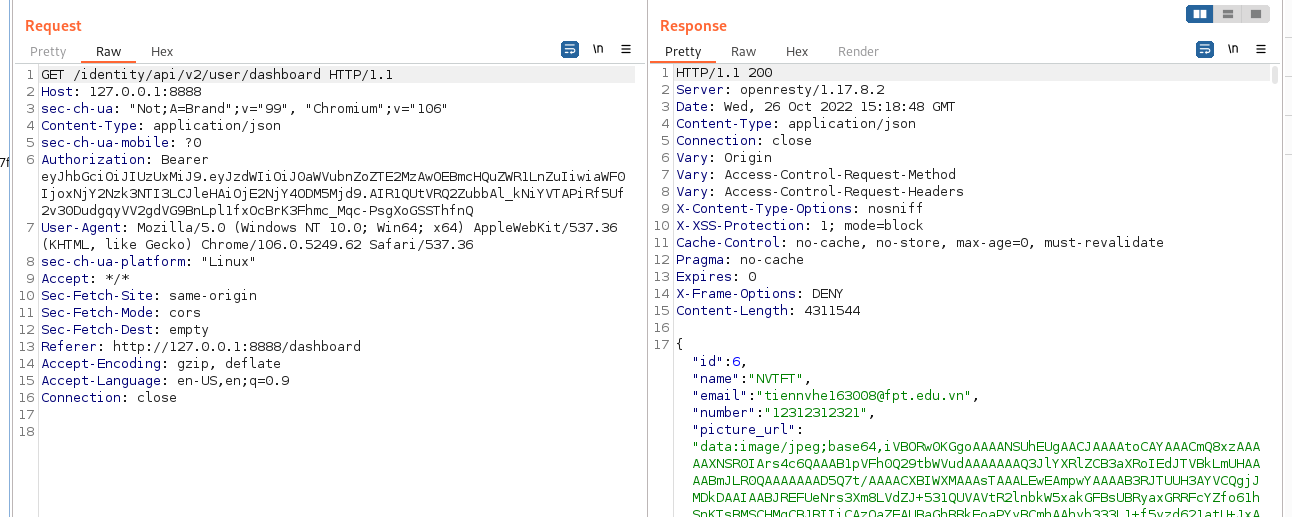




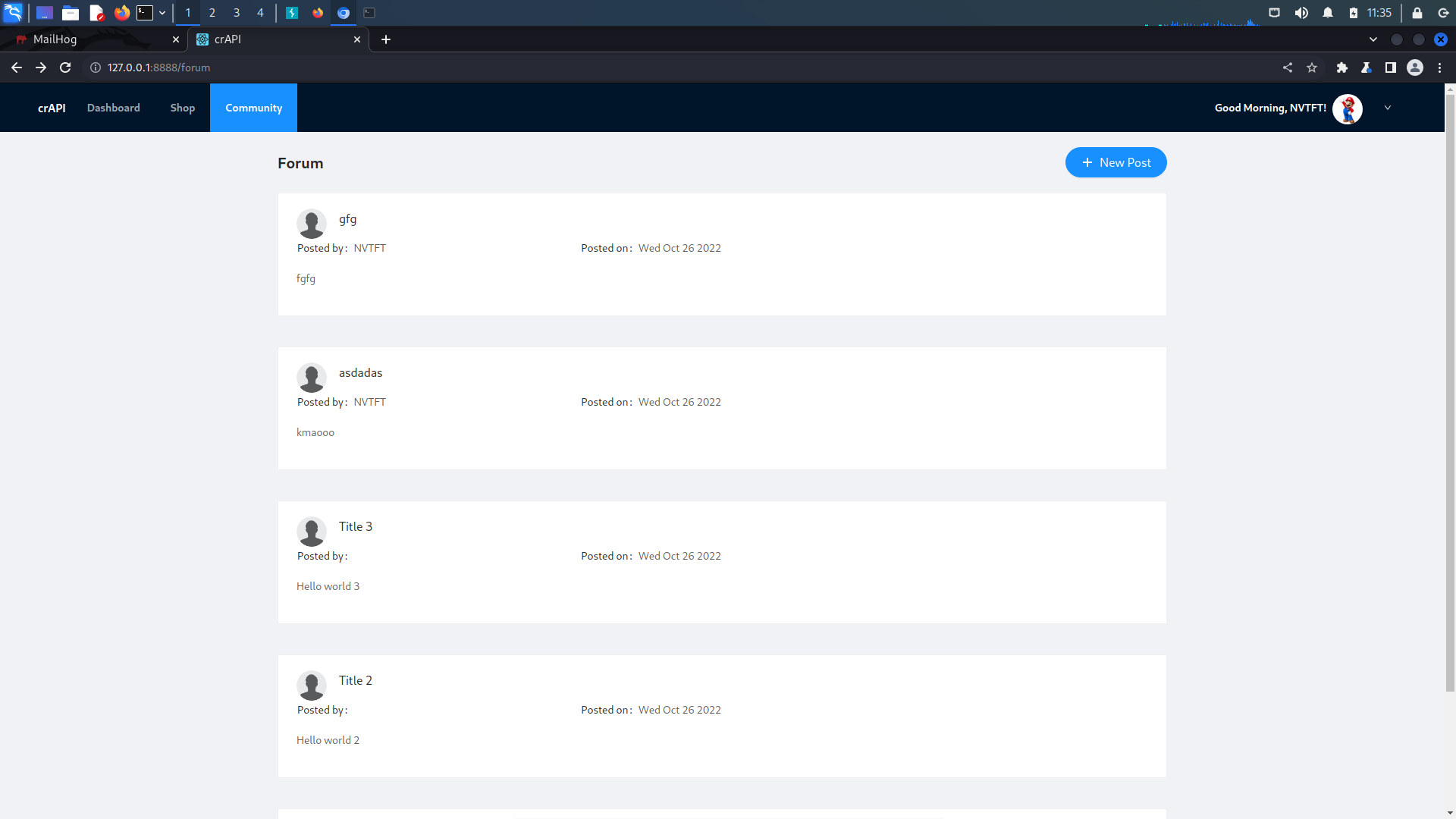
Trang dashboard chứa thông tin của bản thân



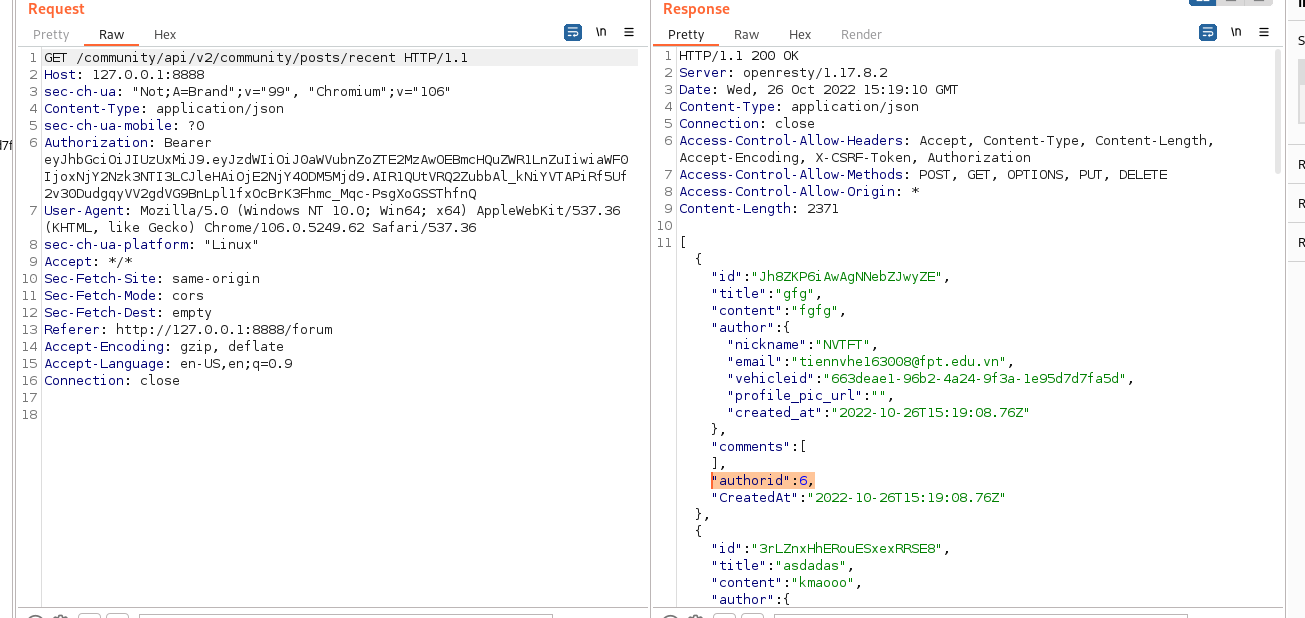
Ta có thể thấy tên của những trường id,name,email => id=6 chứng tỏ còn các user khác id 1→ 5

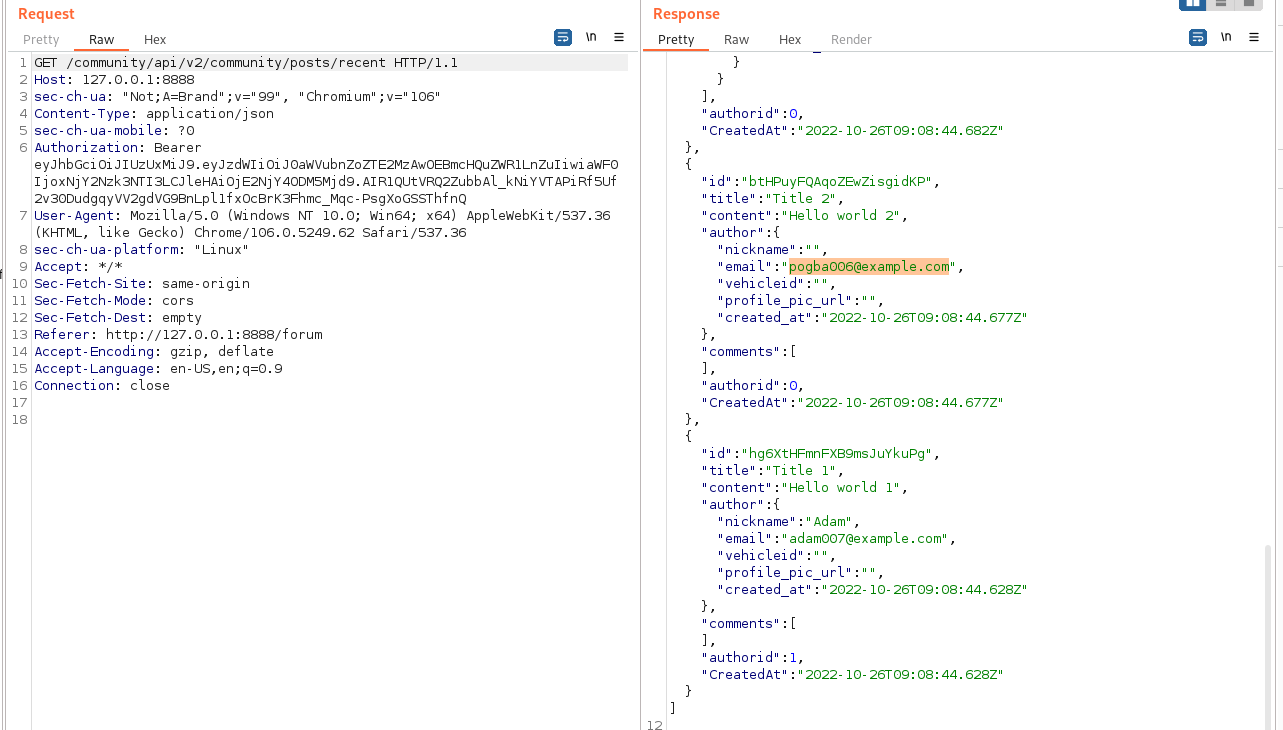


Trang community chứa post và comment của các user

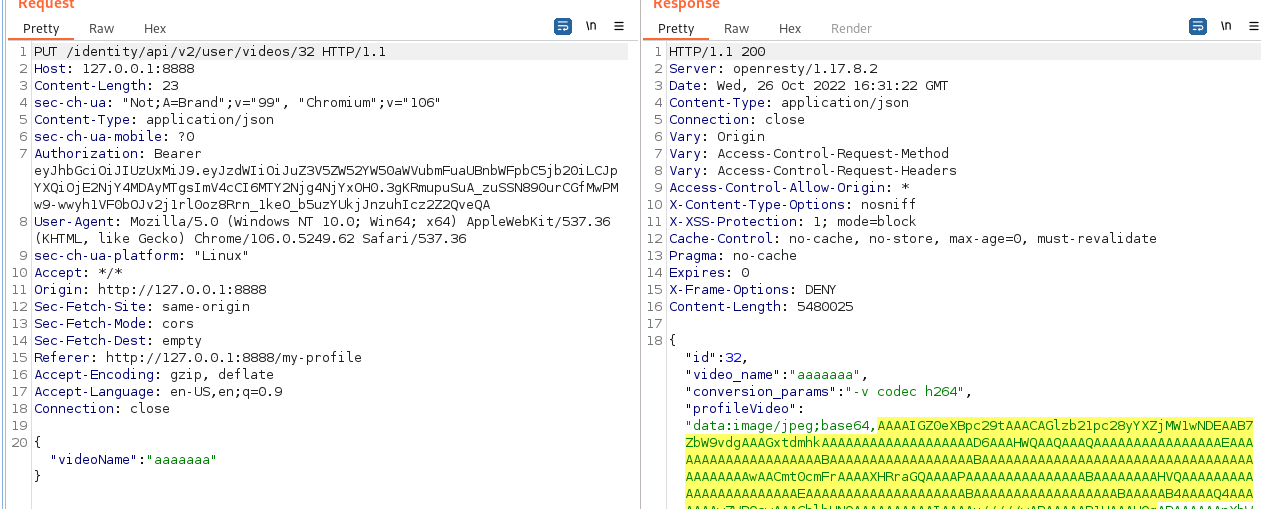


Ta thấy ở bài viết do chính mình đăng có authorid=6 trùng với id=6 bên trên => có thể suy ra id,tên,email,.. của user khác





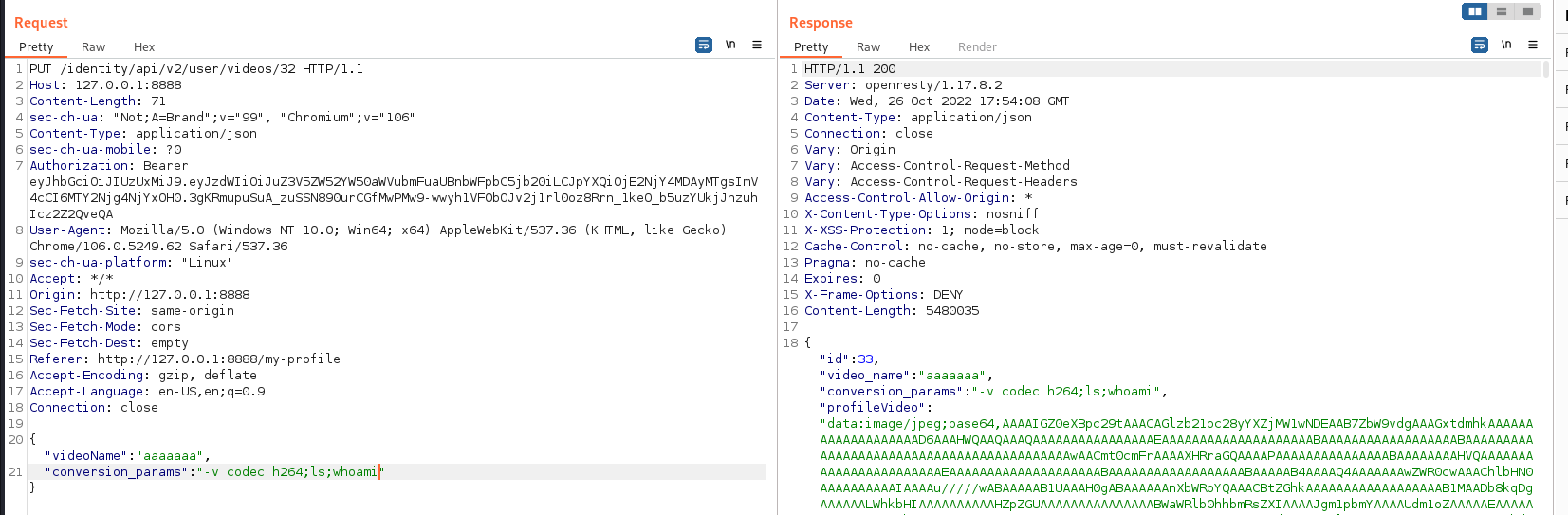
Challenge 5: Ta thấy có conversion\_params leak thông tin về kiểu chuyển đổi của video



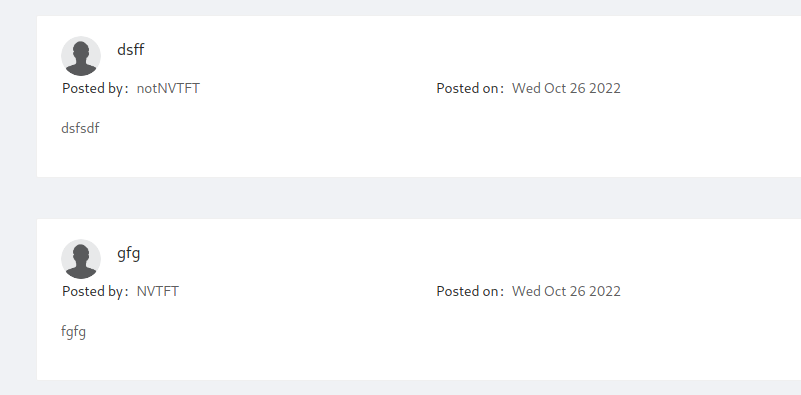


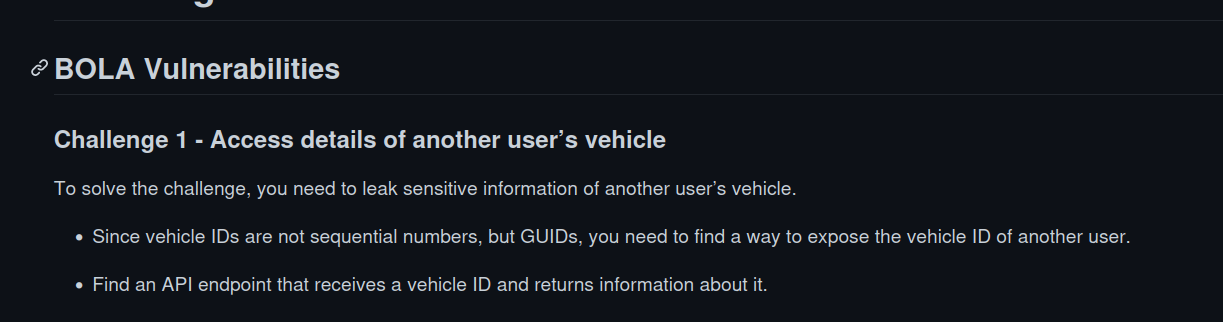
Đây là api khi user upload video lên hoặc update video, Khi ta thay đổi videoName thì tương tự video\_name trên server trả về cũng thay đổi , nhưng id trả về 33 khác với 32 ta request nên đây là request upload video mới chứ không phải update video => thử truyền thêm tham số conversion\_params thì ta thêm được video mới

Có thể tưởng tượng server sẽ chạy lệnh bash “convert … -v codec … “ ta có thể inject bash script hoặc ngôn ngữ nào đó vào và trở thành “convert ….. ; ls ; whoami “



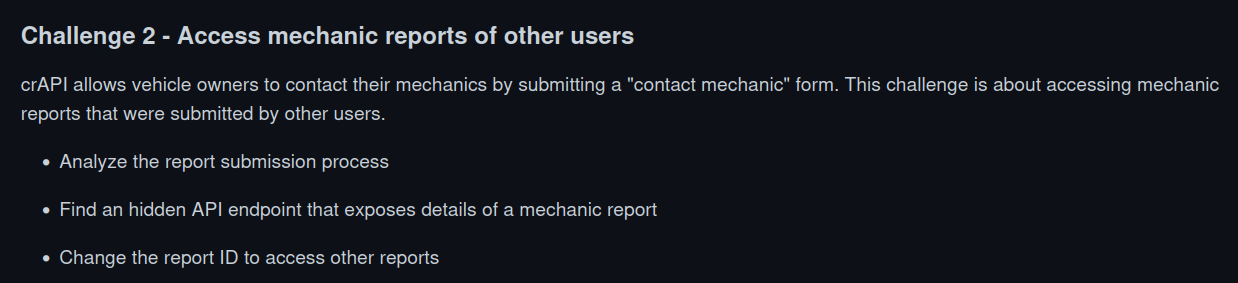
Tiếp theo chúng ta sẽ kiểm tra BOLA vuln, ta tạo 2 user khác nhau và kiểm thử A-B



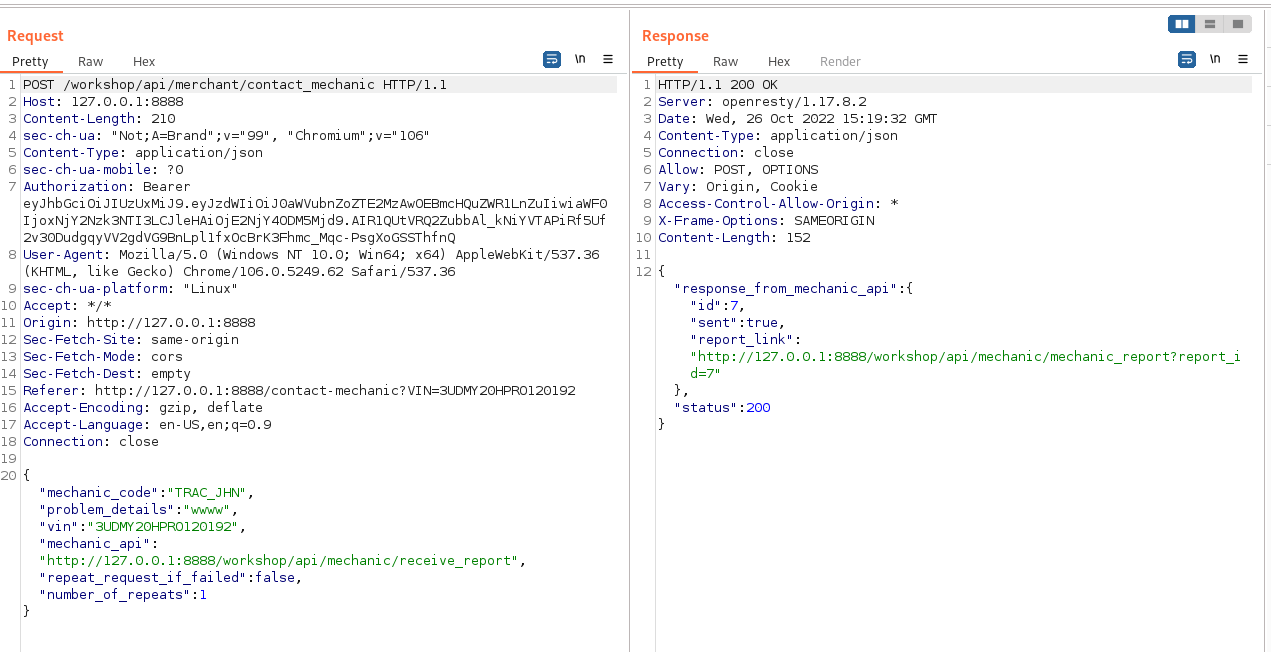


Đăng nhập vào user 1 và tạo vehicle ta có vehicle id và jwt token của user đó. Thử lấy token của user 2 thay vào nhưng vẫn đọc được thông tin về vehicle. Api này chỉ cần truyền vào vehicle id nhưng nó đã bị lộ từ bên trên nên chúng ta có thể được thông tin vehicle của tất cả user

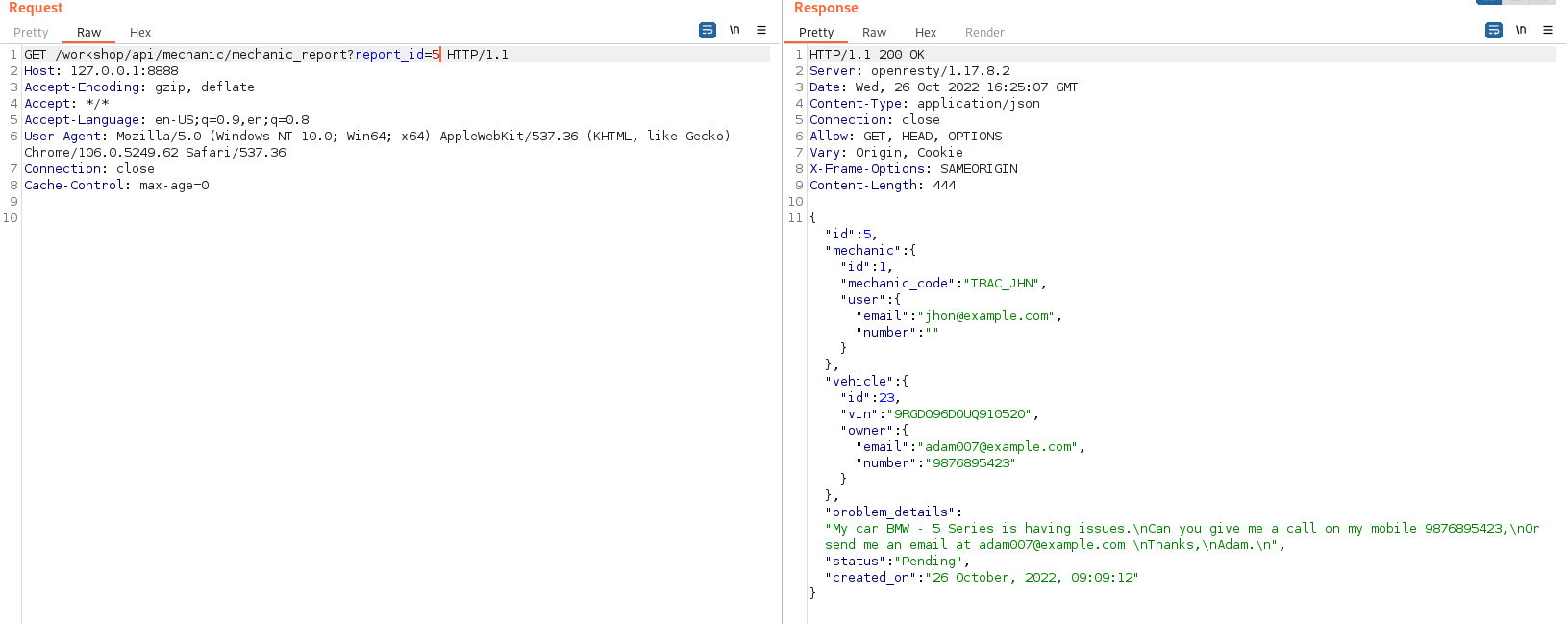


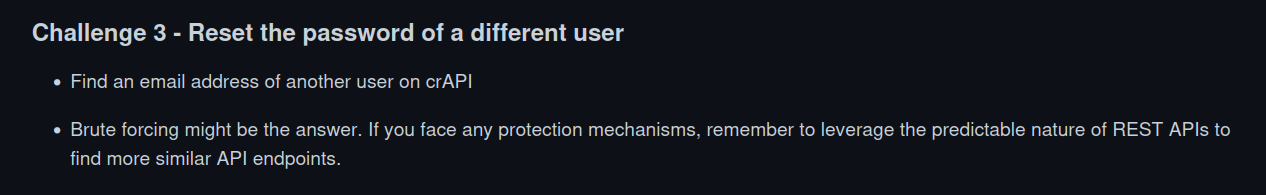


Khi report đến mechanic ta thấy co mechanic api và server trả về status 200 và report link. Có vẻ server đã thực hiện 1 request đên mechanic\_api của chúng ta truyền vào. Chúng ta có thể thay đổi => SSRF

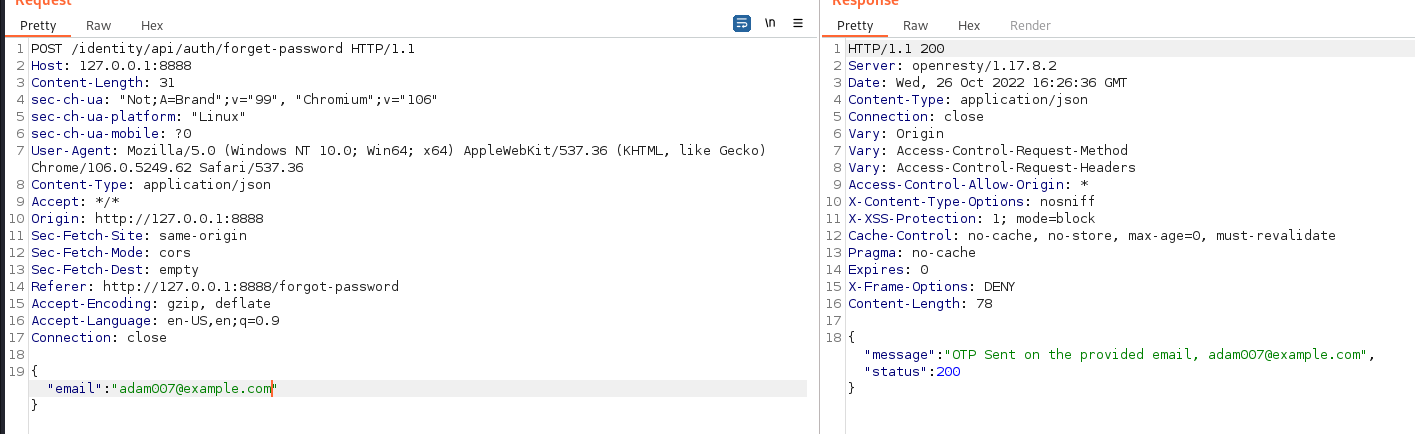


Đồng thời chúng ta cũng có thể truy cập vào report\_id của các user khác mà không cần jwt token

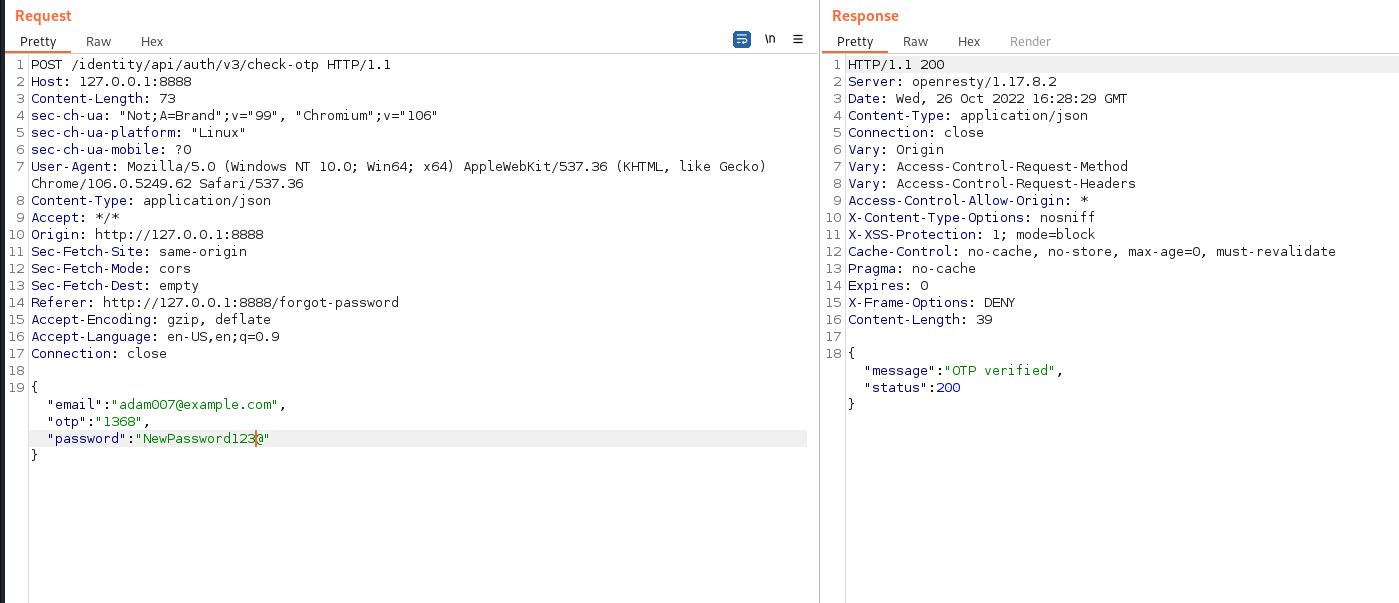




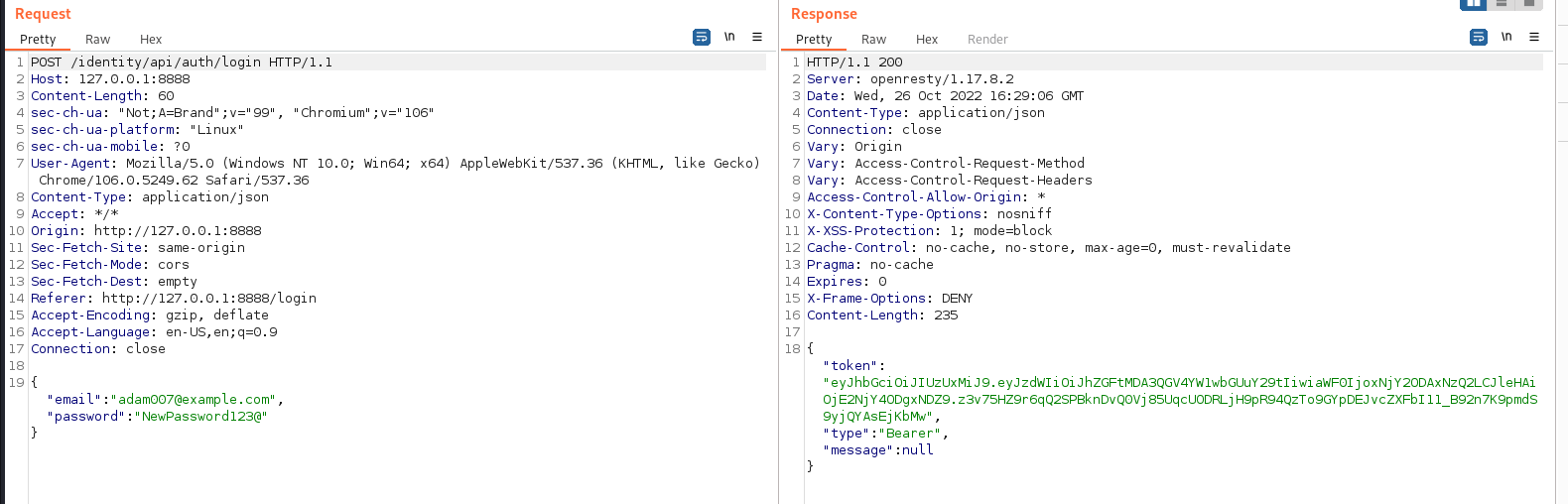
Biết được email lộ từ bên trên ta có thể thay đổi password của user với email

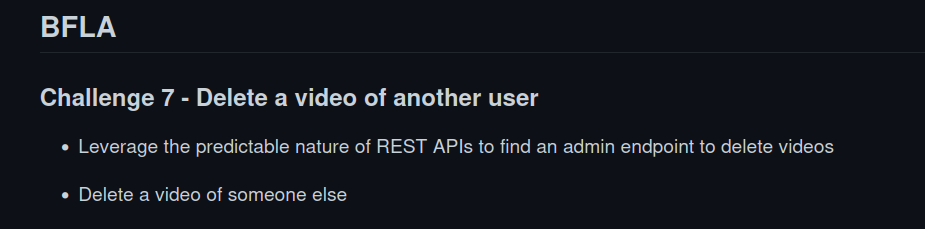


Ta có quyền truy cập vào mail server nên lấy được otp

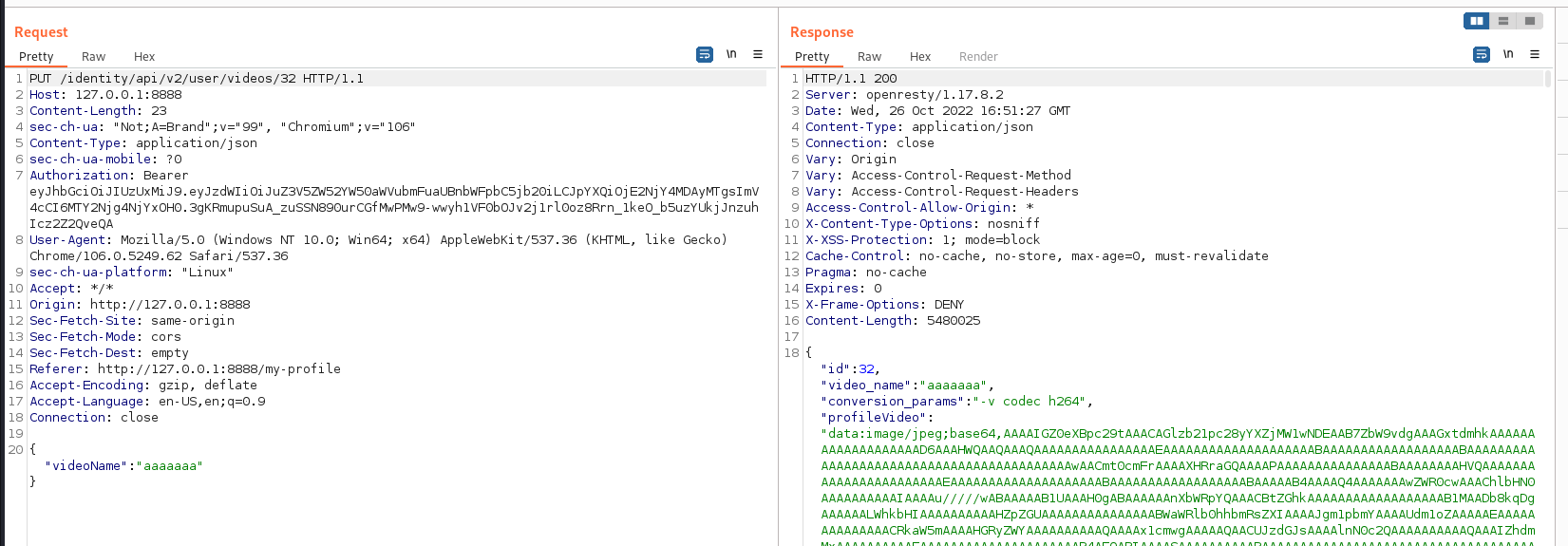


Thử login bằng pasword mới và thành công

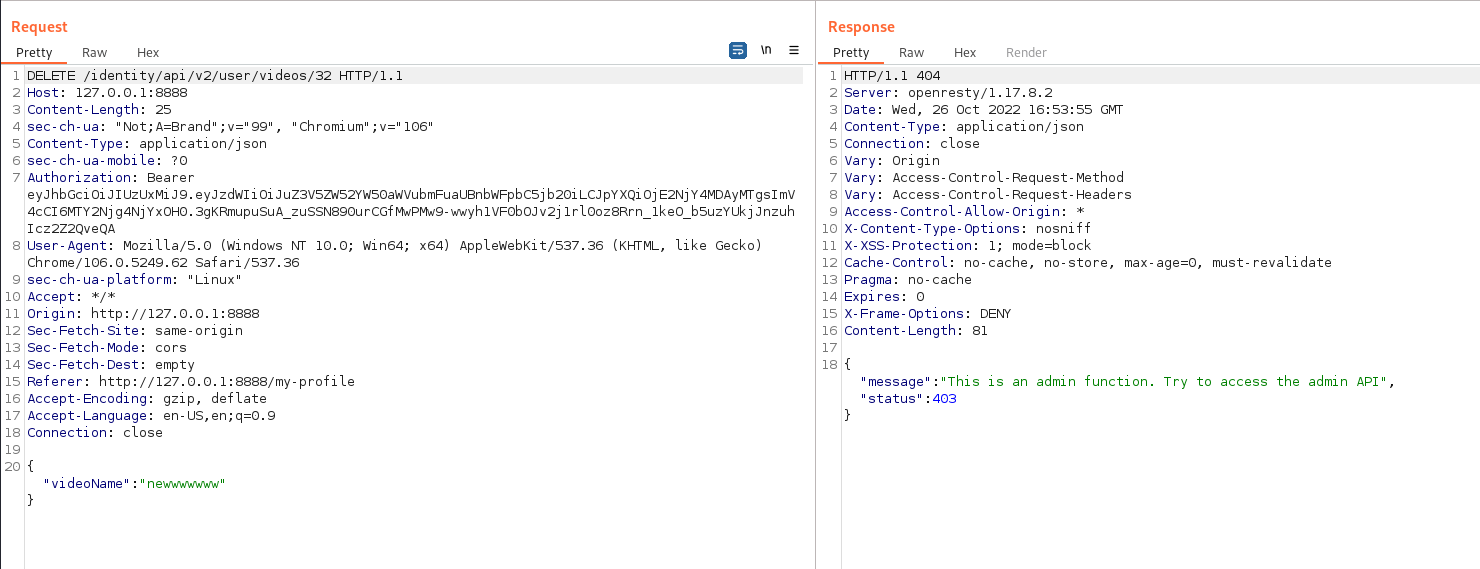




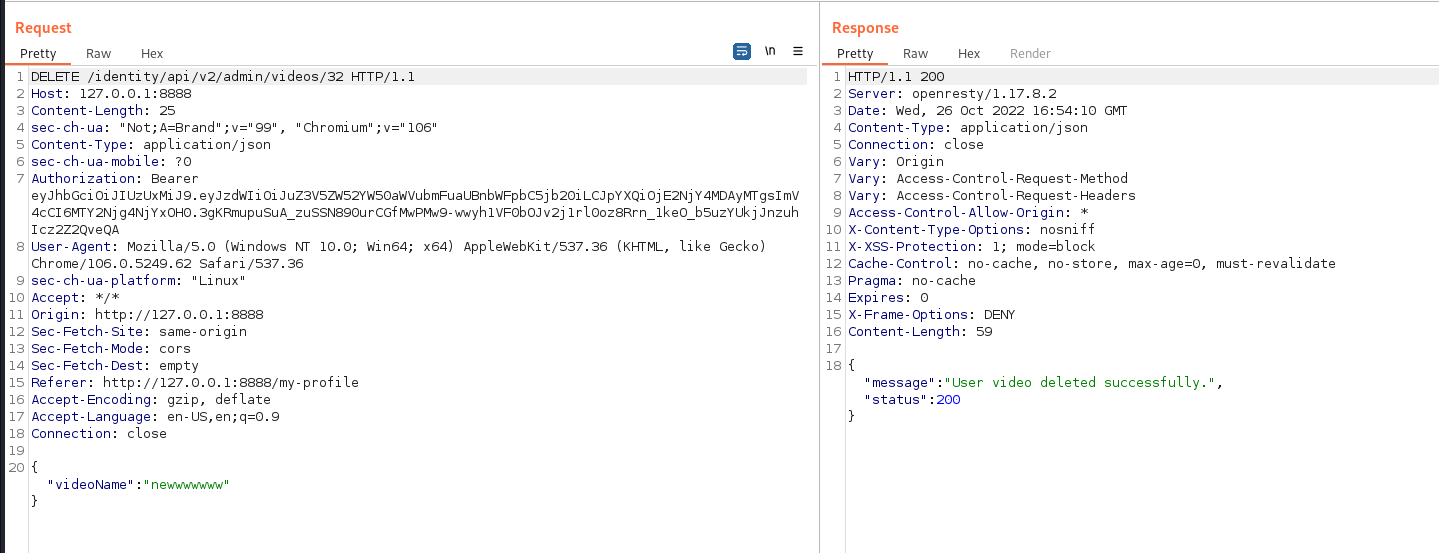
Ta quay lại với api upload hoặc update user video



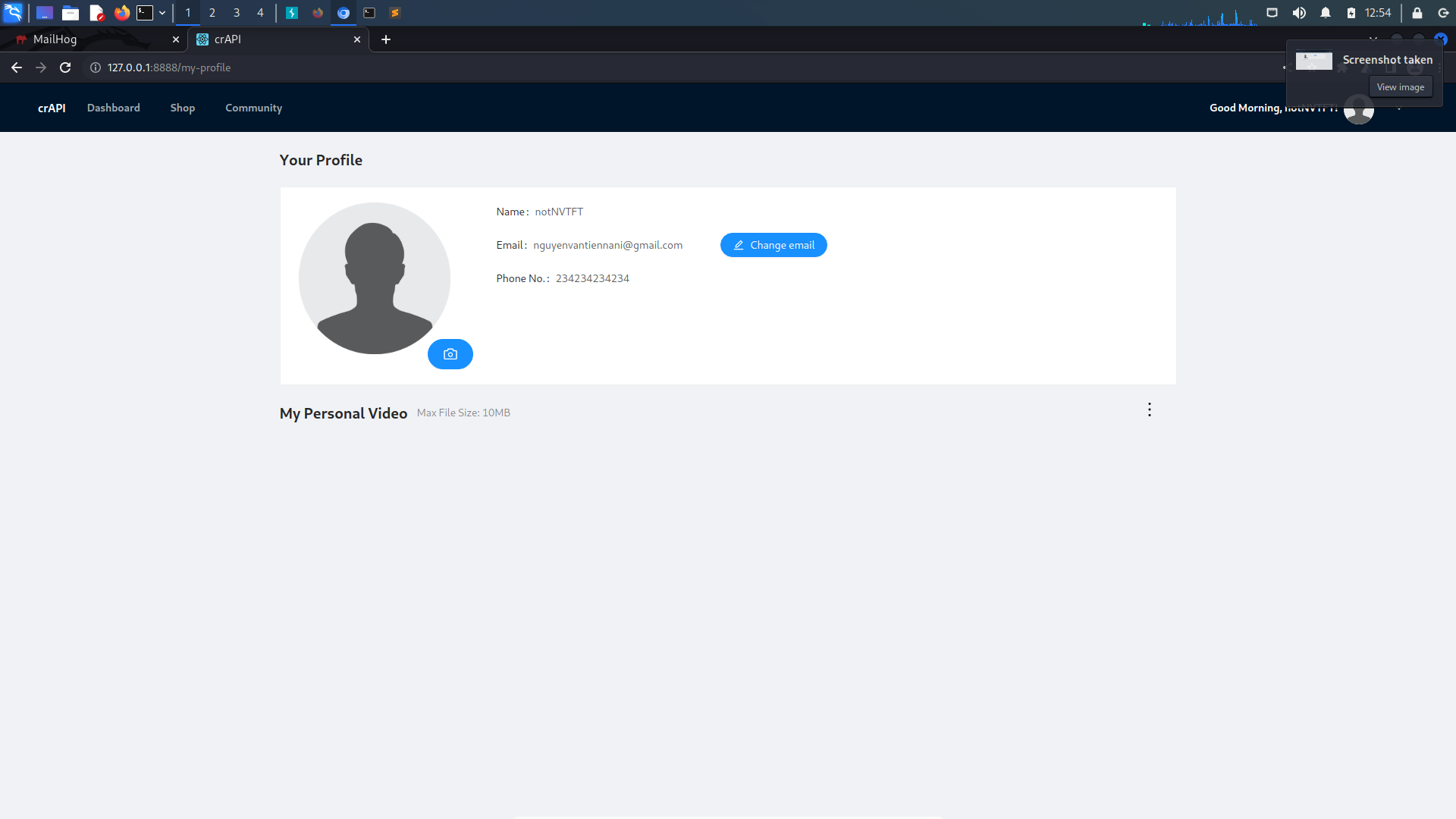
Đổi PUT thành OPTIONS ta thấy rất nhiều lựa chọn: GET, POST ,DELETE thử đổi thành DELETE thì response server trả về thay đổi, ta phải là admin để có thể xóa

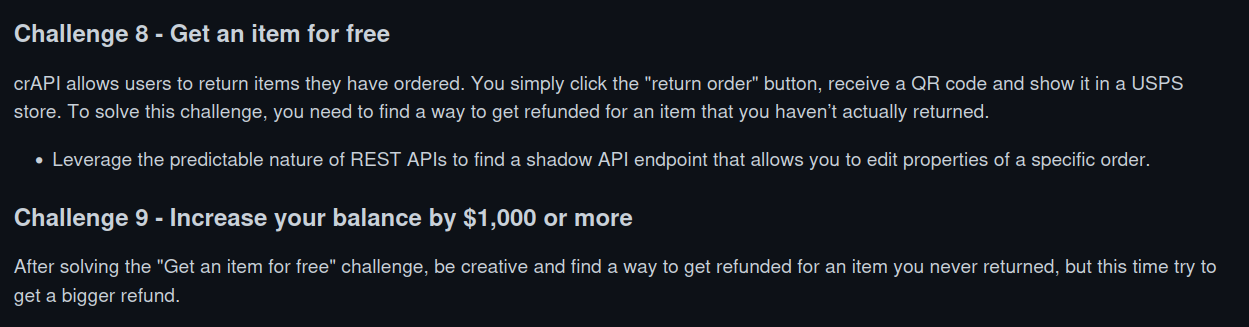


Thử thay đổi api user thành admin và ta đã có thể xóa video của bất kì user nào

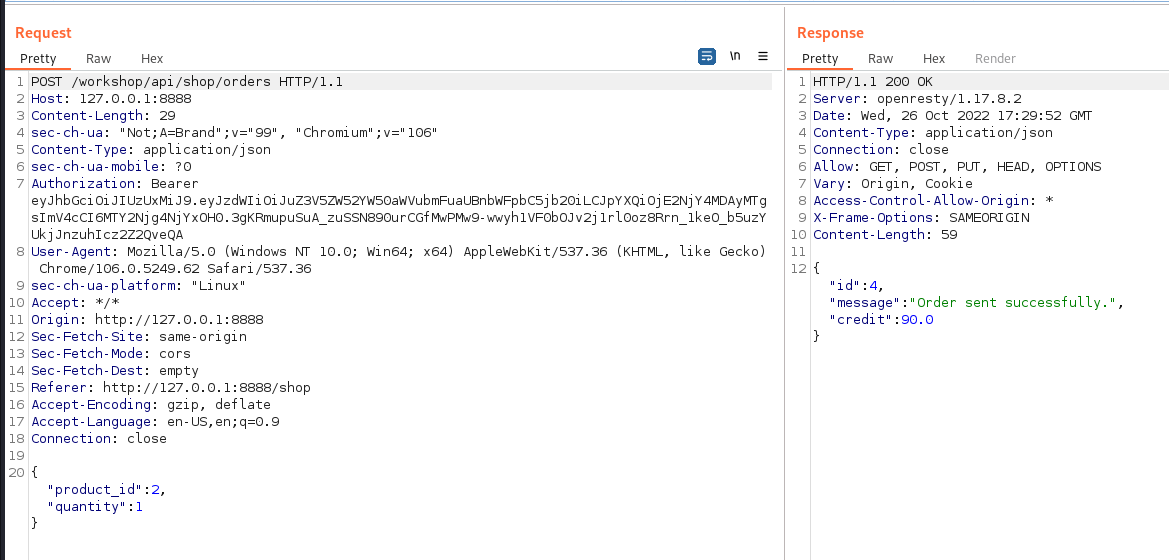


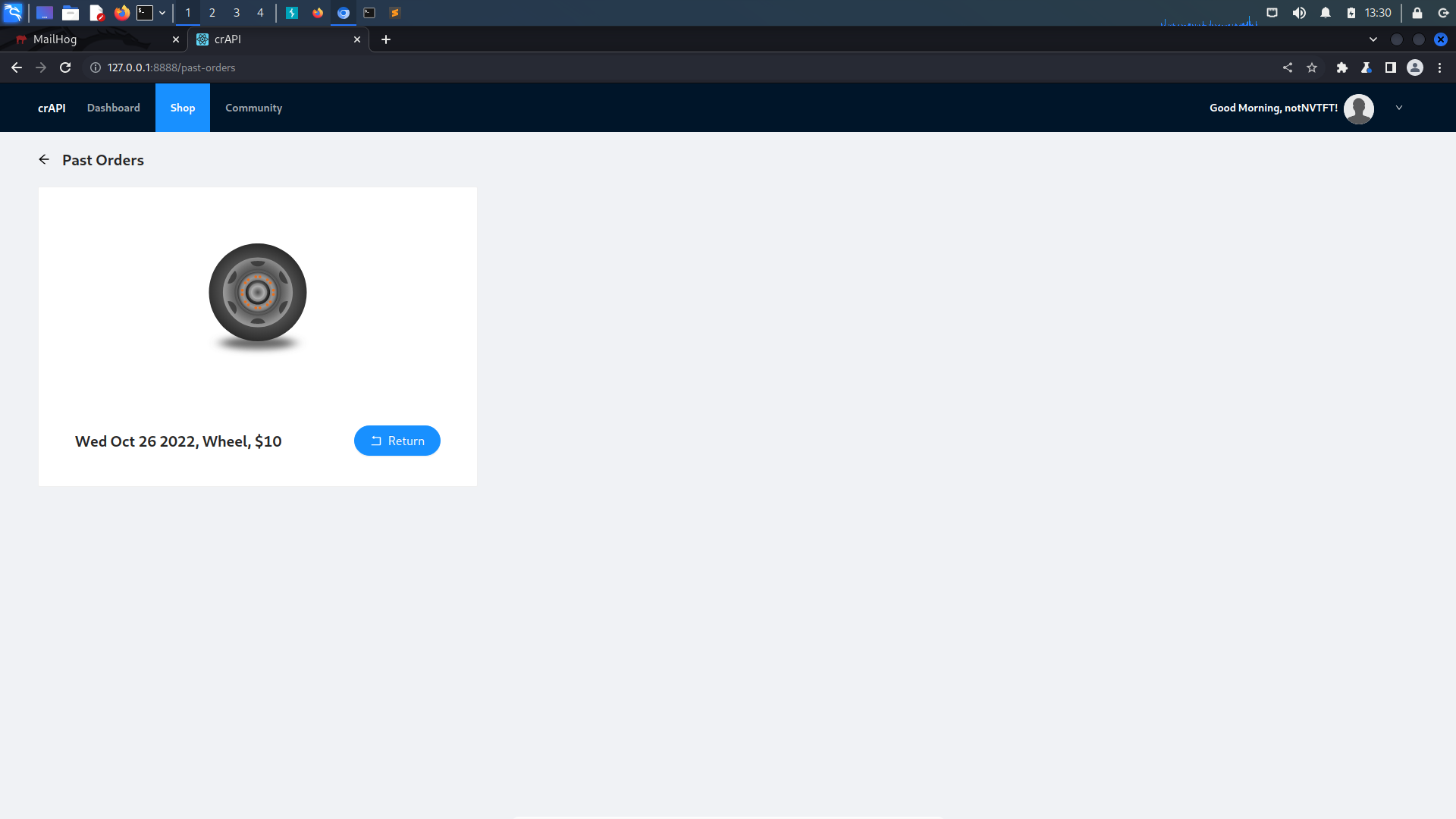
kiểm tra lại video của ta ta thấy không còn nữa



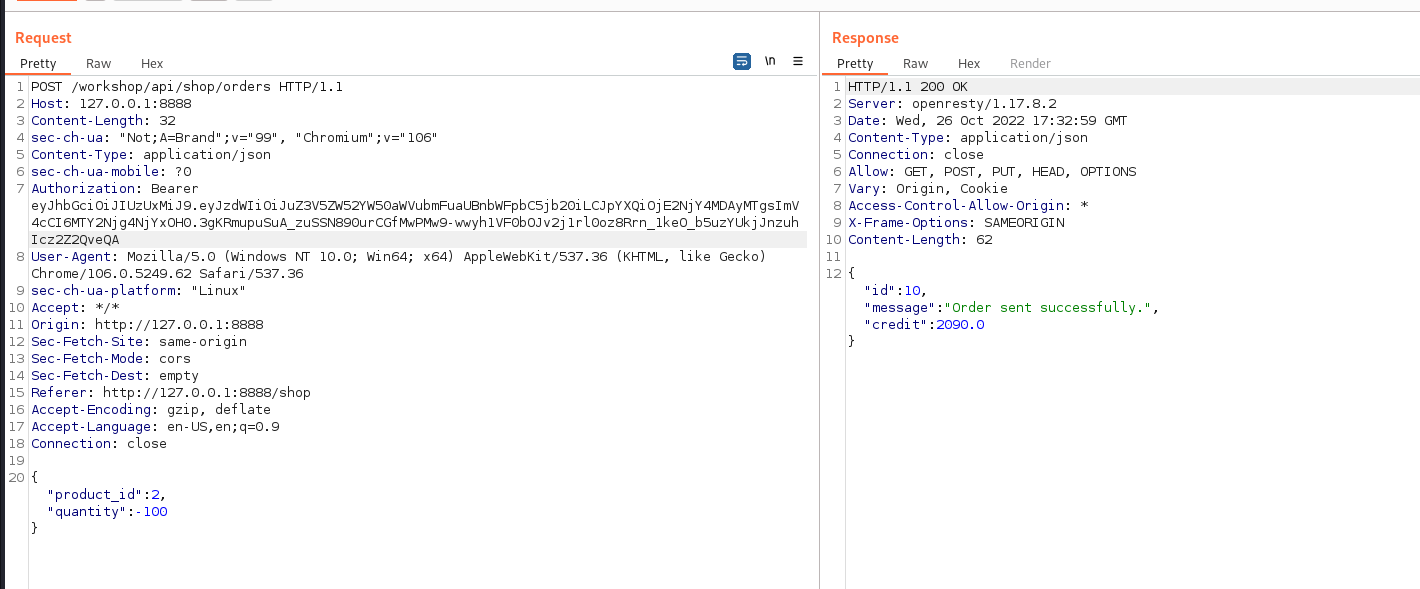


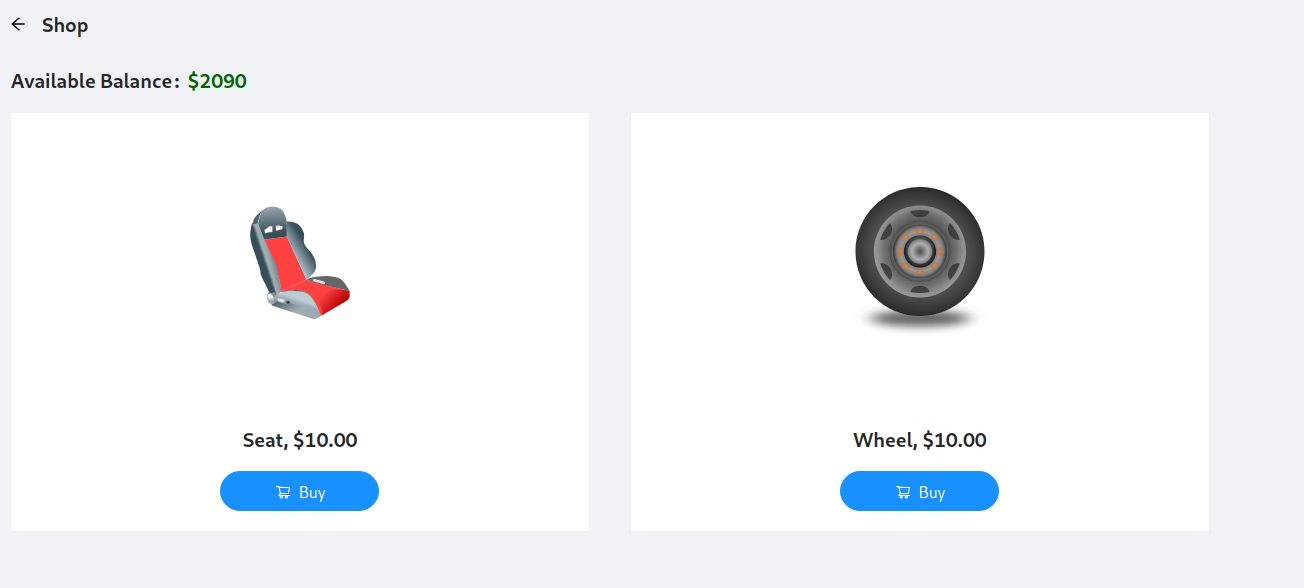
Khi thực hiện request mua hàng ta thấy ta truyền vào product\_id tương ứng với sản phẩm và quantity là số lượng muốn mua, server trả về id của order và credit chúng ta còn lại

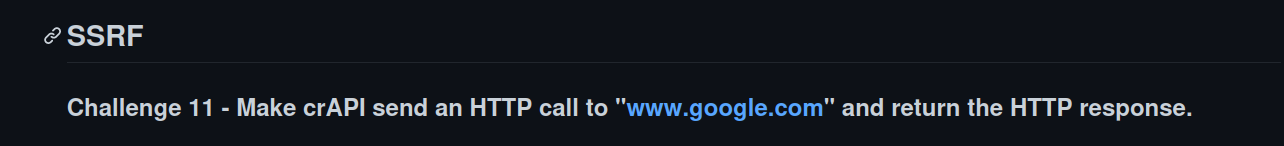




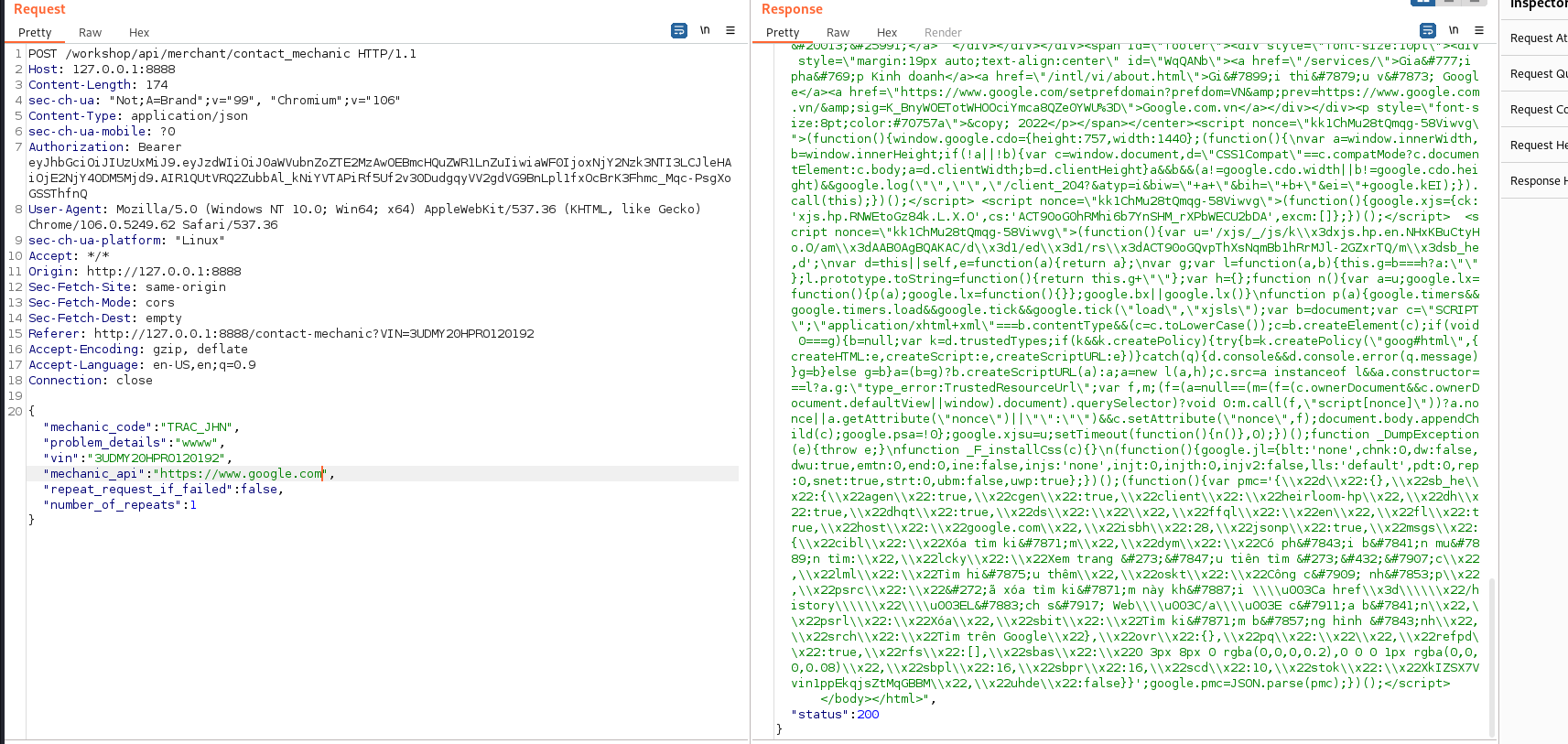
Thử thay đổi số lượng mua thành âm => credit của ta đã tăng lên 2000

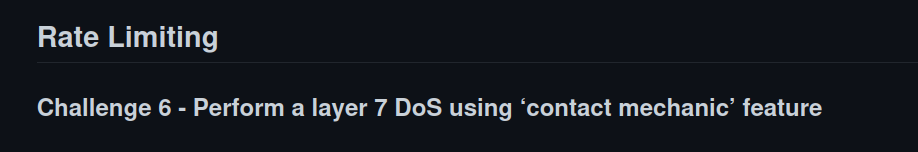




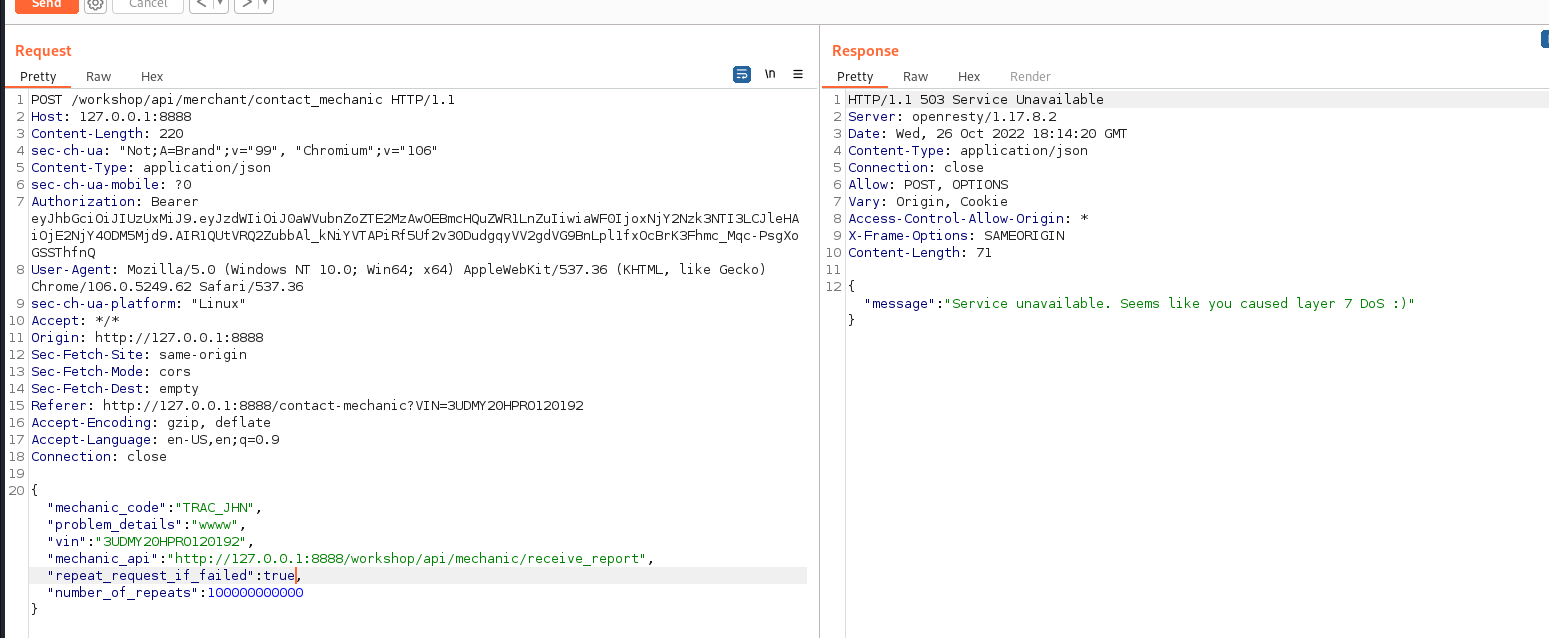


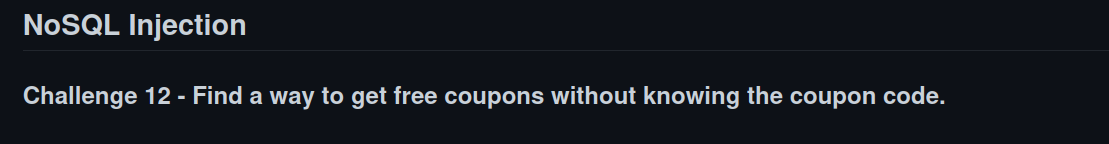
thay đổi mechanic\_api như đã nói bên trên và ta có thể thực hiện truy vấn đến google.com



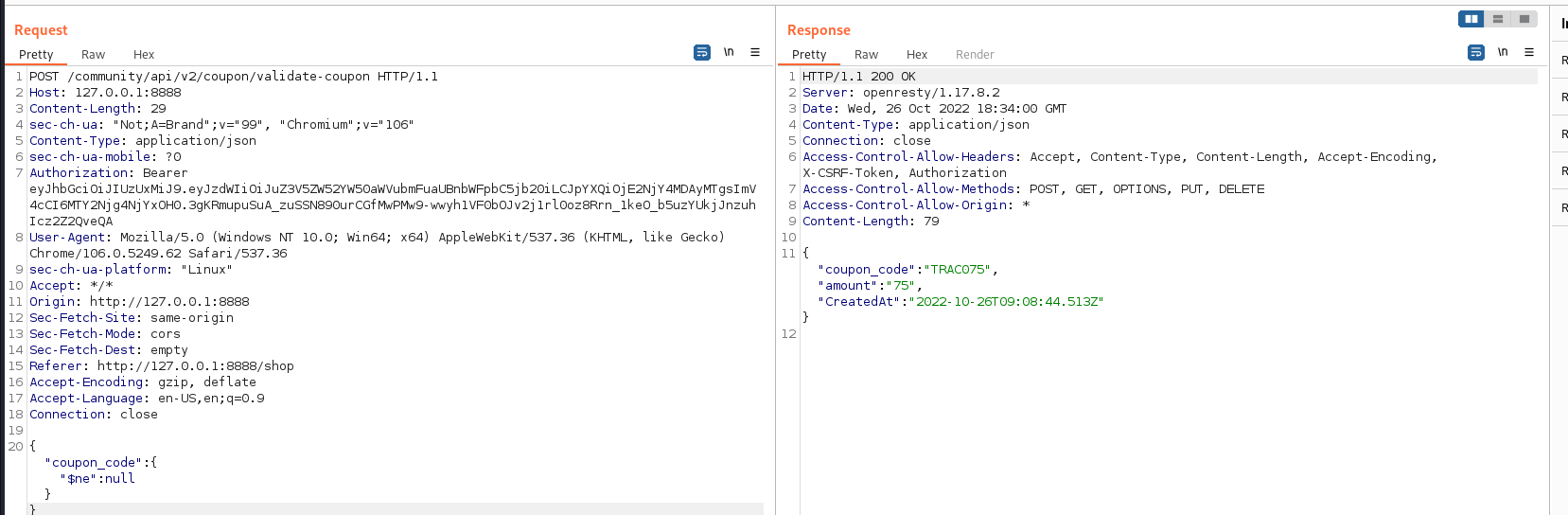


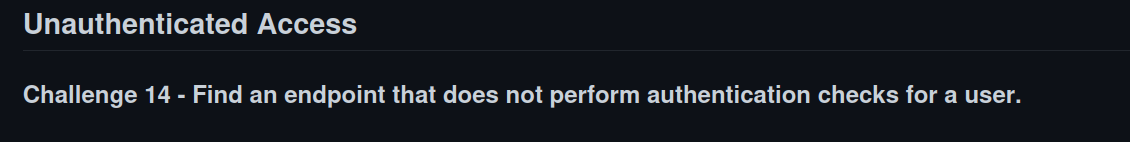
Ở request contact\_mechanic ta thấy params repeat request if fail và number of repeat, ta thử set repeat = true và lặp lại nhiều lần => ta thực hiên được layer 7 Dos





Ở truy vấn kiểm tra coupon ta có thể truyền vào tên của coupon, thử thay bằng payload của nosql ( tìm những coupon mà code khác null) => server trả về valid coupon





Như đã nói bên trên, request này được server tự thực hiện, không liên quan đến user nên coder có thể quên thêm jwt authen ở đây

