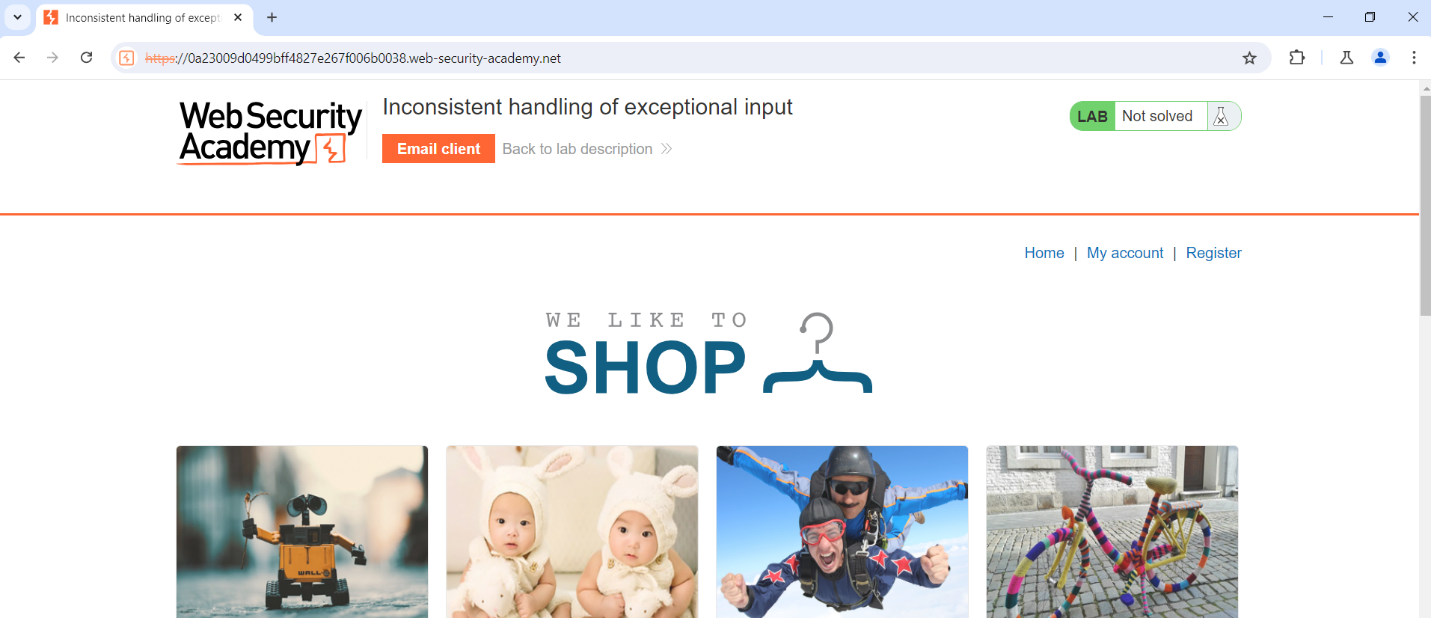
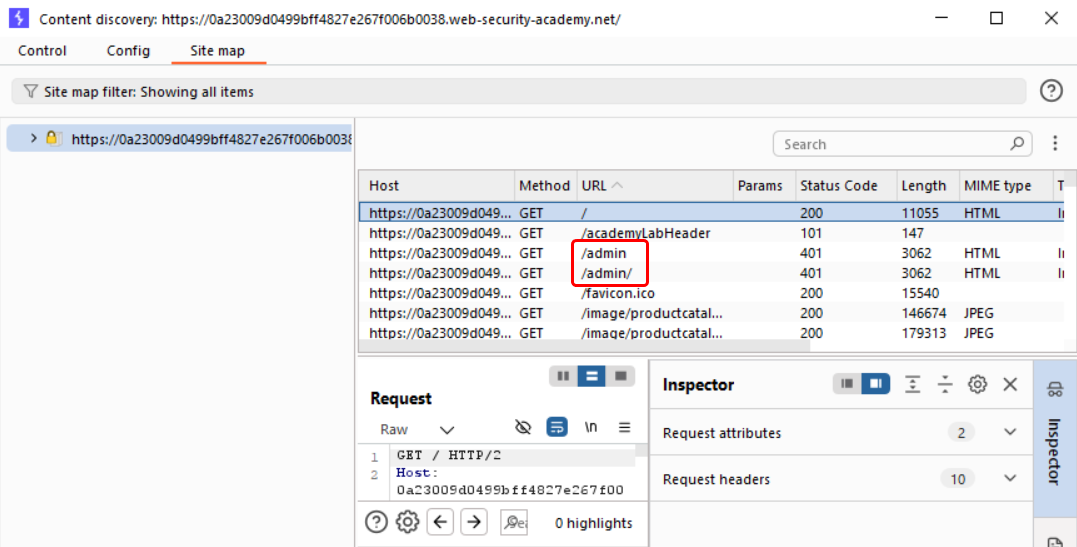


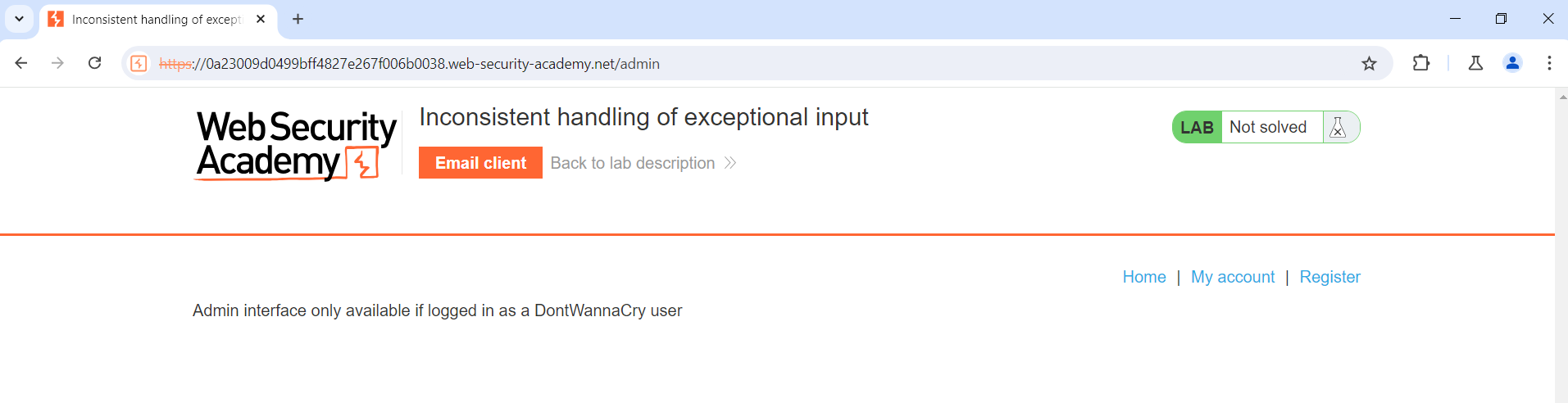
* Mục tiêu: Truy cập vào giao diện admin và xóa tài khoản carlos



* Ta sẽ Bruteforce xem trang web này có những path nào

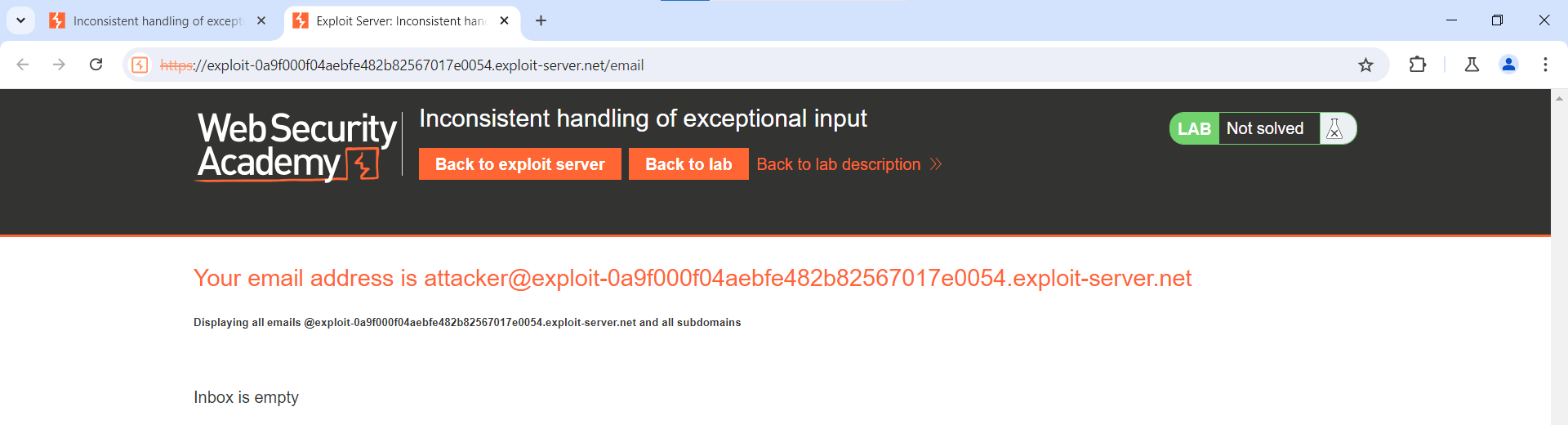


* Phát hiện đường dẫn đến trang admin

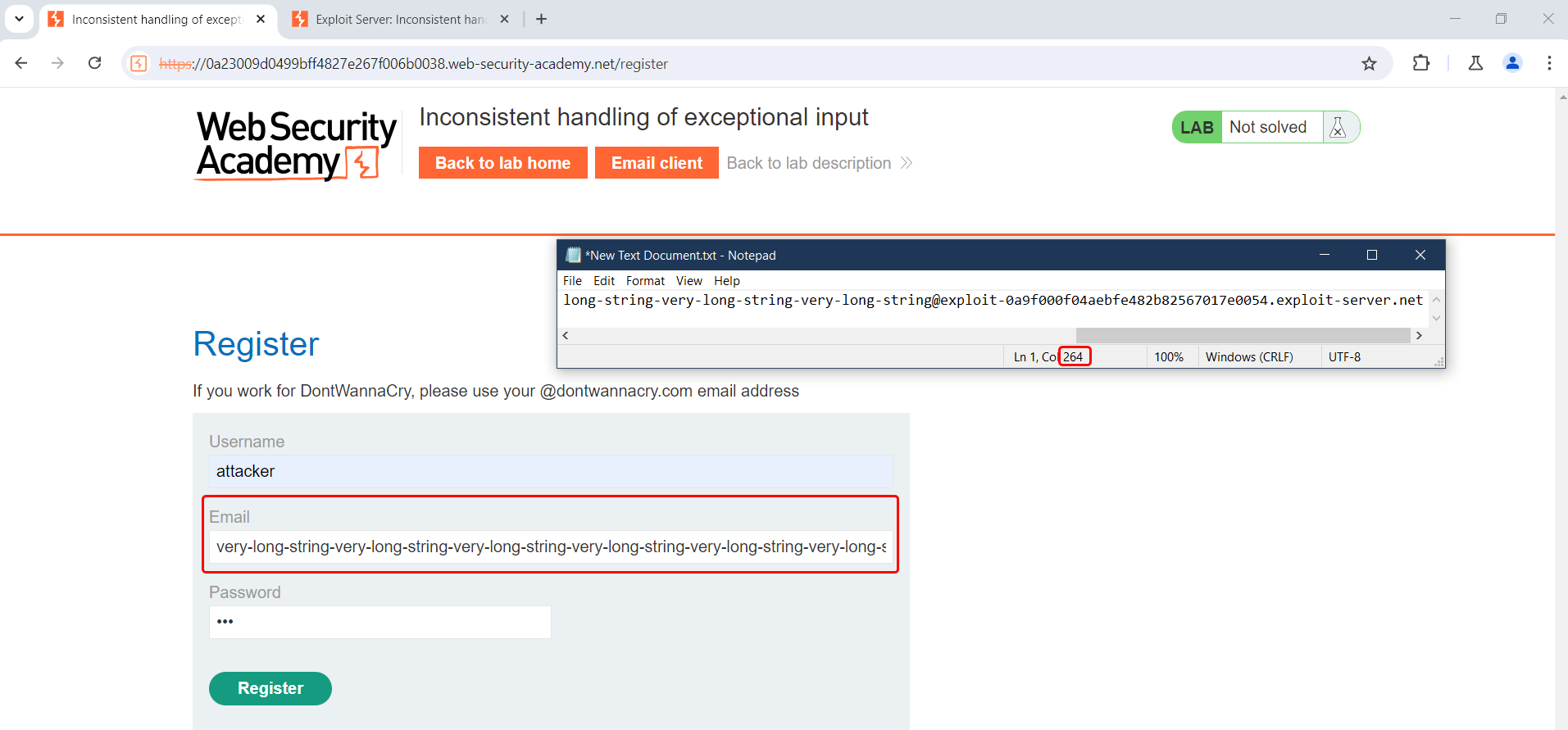


* Không vào được vì không phải user của DontWannaCry
* Vào email client, ta phát hiện ra trang Exploit này sẽ nhận toàn bộ email từ @exploit-0a9f000f04aebfe482b82567017e0054.exploit-server.net và tên miền phụ của nó. Tức là nó vẫn có thể nhận được:

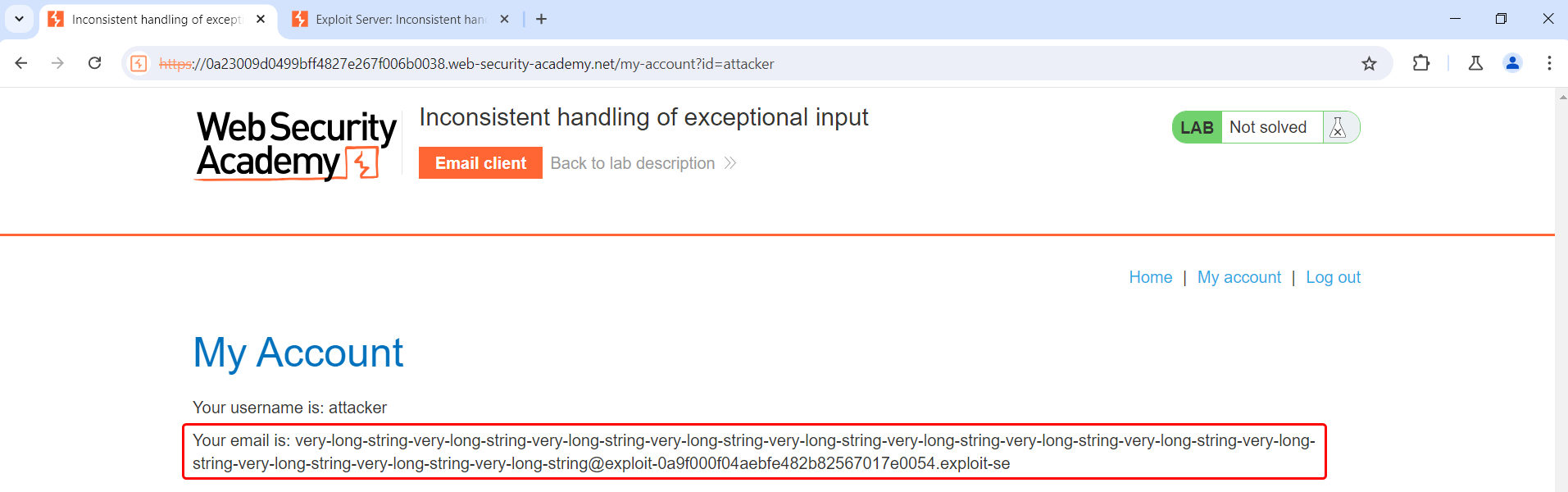
@dontwannacry.com.exploit-0a9f000f04aebfe482b82567017e0054.exploit-server.net



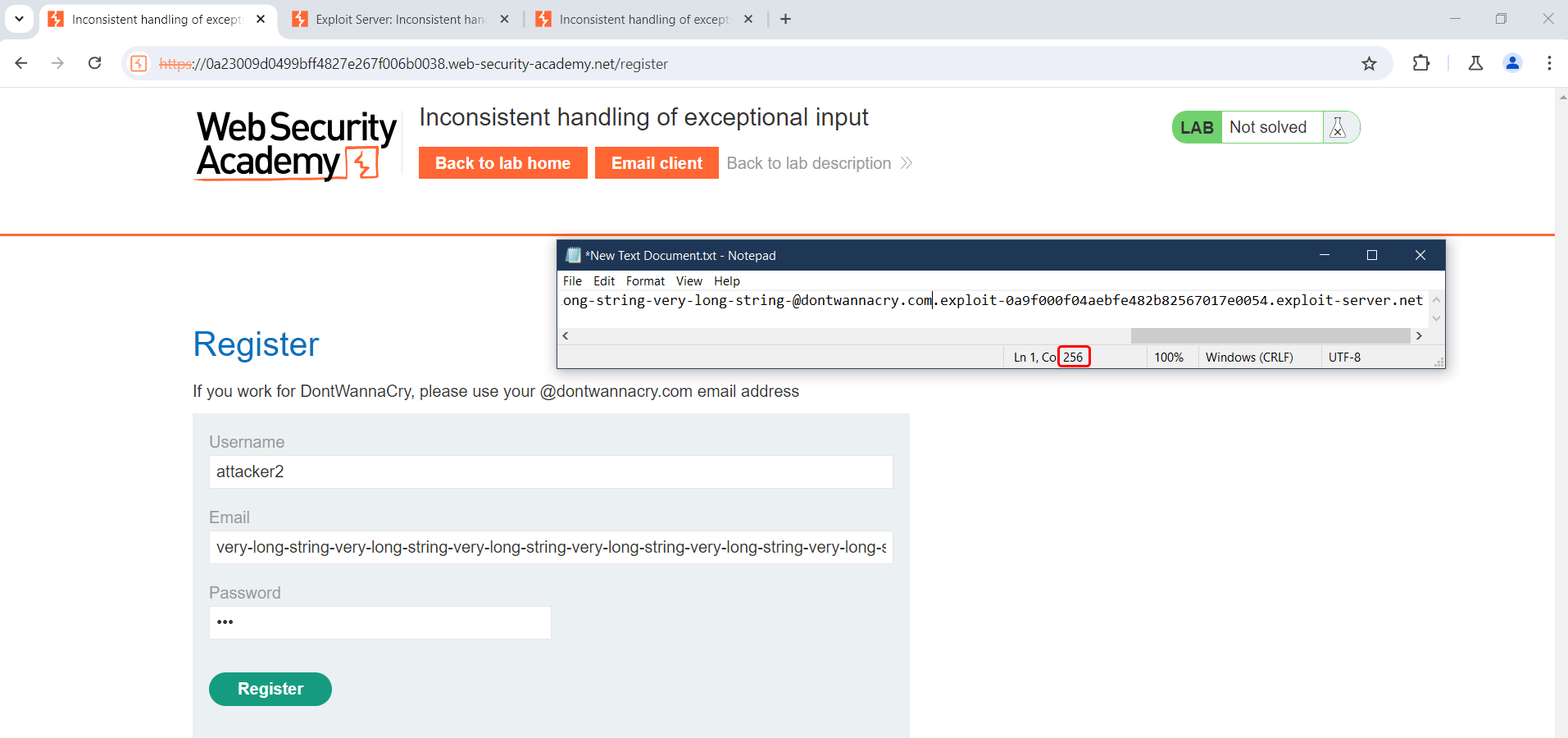
* Tuy nhiên, Server vẫn có thể check xem sau @ có phải của dontwannacry.com thật không nên ta cần phải tìm cách để Server chỉ kiểm tra đến được chữ “m” của @dontwannacry.com.exploit-0a9f000f04aebfe482b82567017e0054.exploit-server.net
* Đăng ký tài khoản mới với tài khoản email cực dài



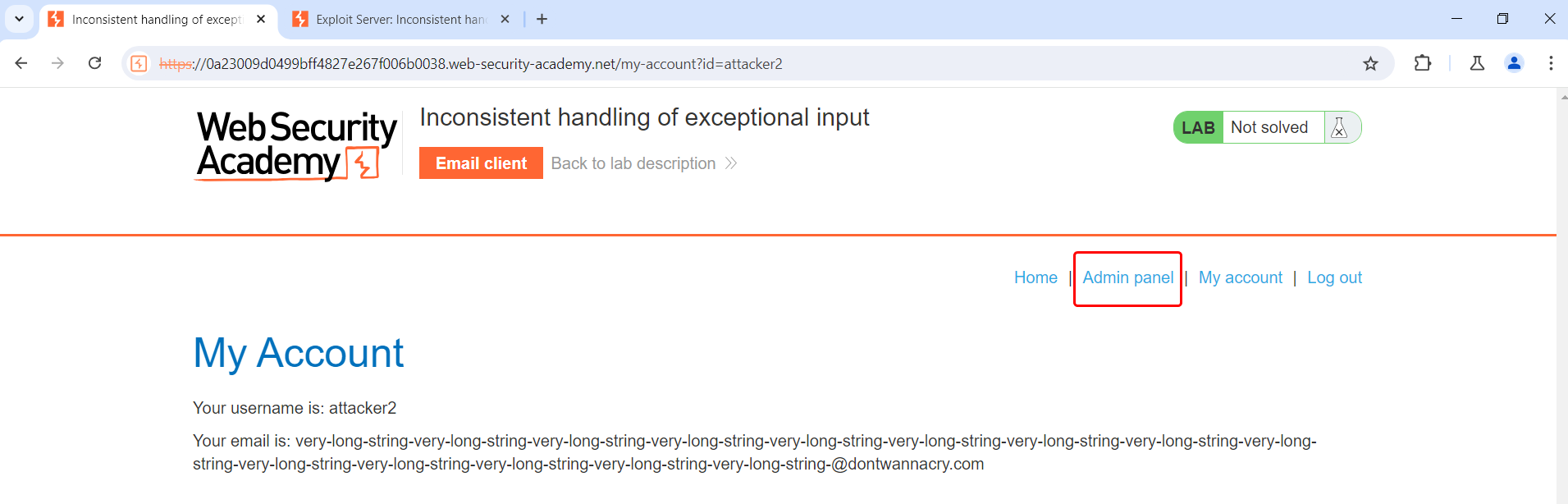
* Sau khi xác nhận thành công và đăng nhập, ta thấy rằng email đã bị rút gọn lại xuống 250 ký tự



* Ta có thể dựa vào điều này để thực hiện khai thác và rút gọn xuống chữ “m” trong email @dontwannacry.com.exploit-0a9f000f04aebfe482b82567017e0054.exploit-server.net
* Đăng ký tài khoản mới.



* Sau khi đăng nhập lại trang thì đã xuất hiện “Admin panel”



* Xóa tài khoản “carlos” và hoàn thành labs

