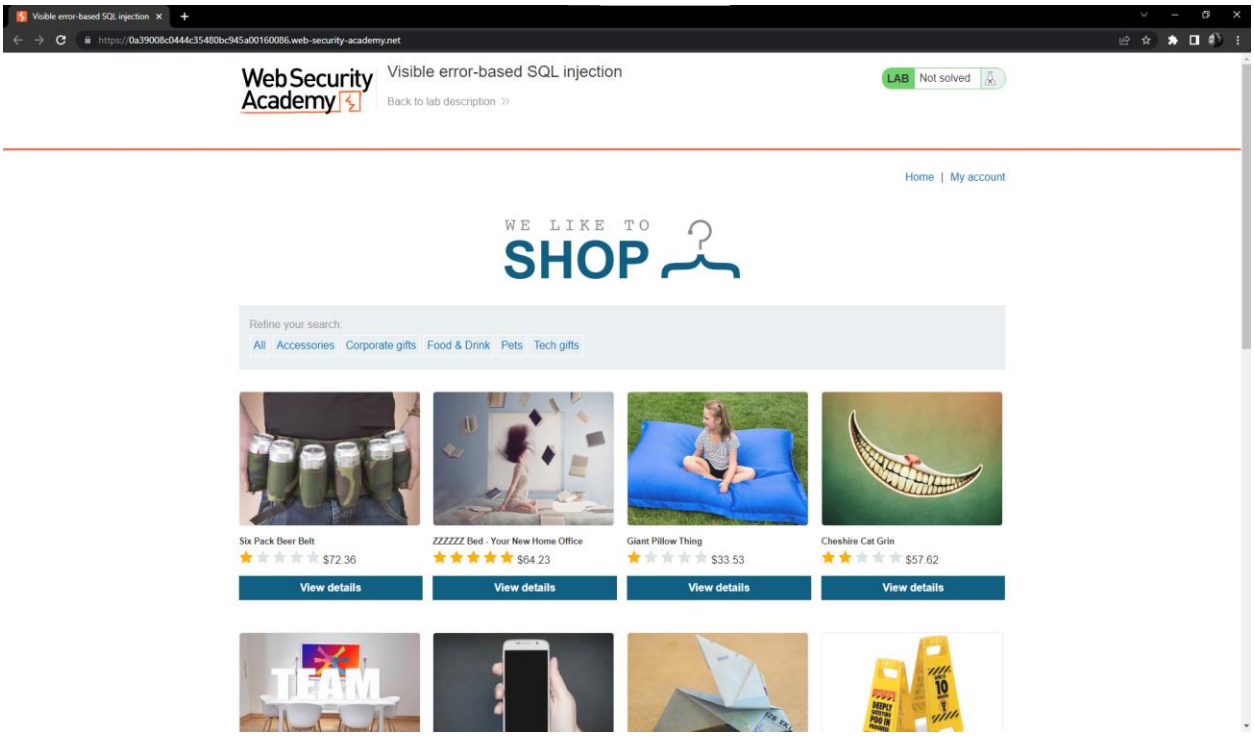
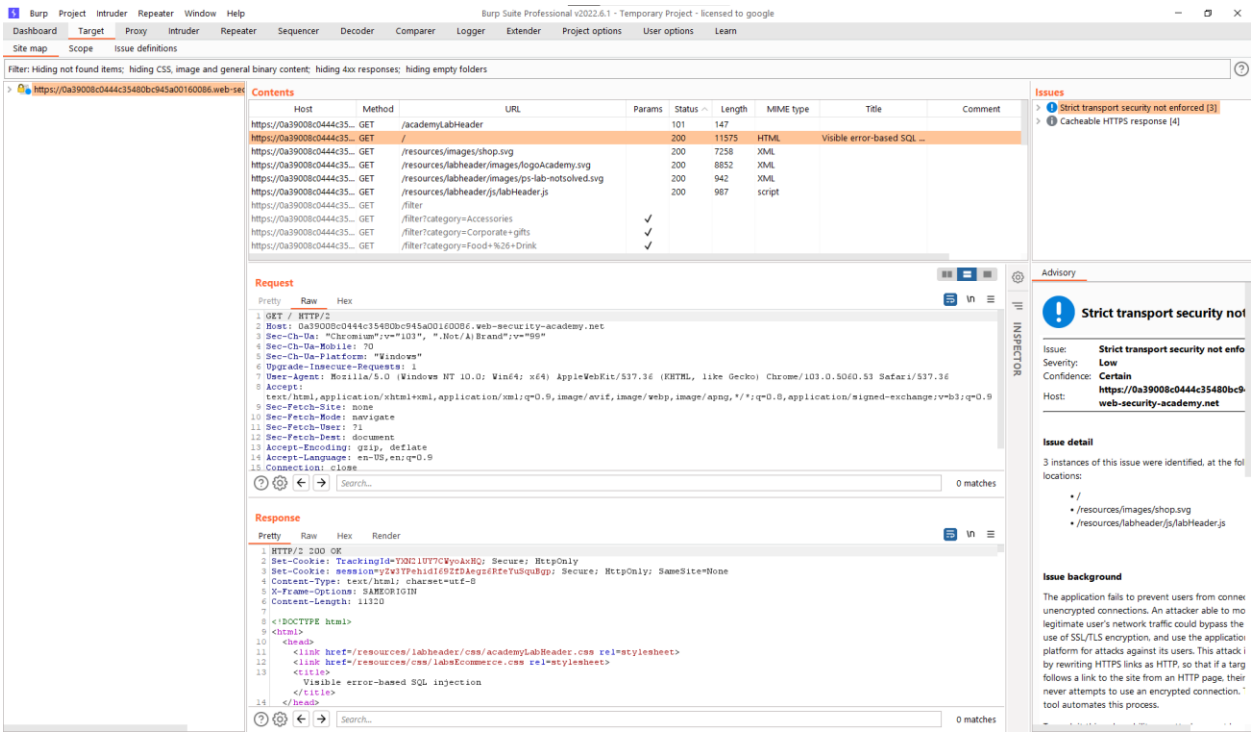
Ta sẽ khai thác lỗ hổng error-based SQL injection sử dụng cookie theo dõi để phân tích và thực hiện những câu lệnh truy vấn SQL có chứa giá trị của cookie để nó trả lại những thông báo lỗi

Mục đích của bài làm này là tìm được tên user và password trong bảng users của trang web

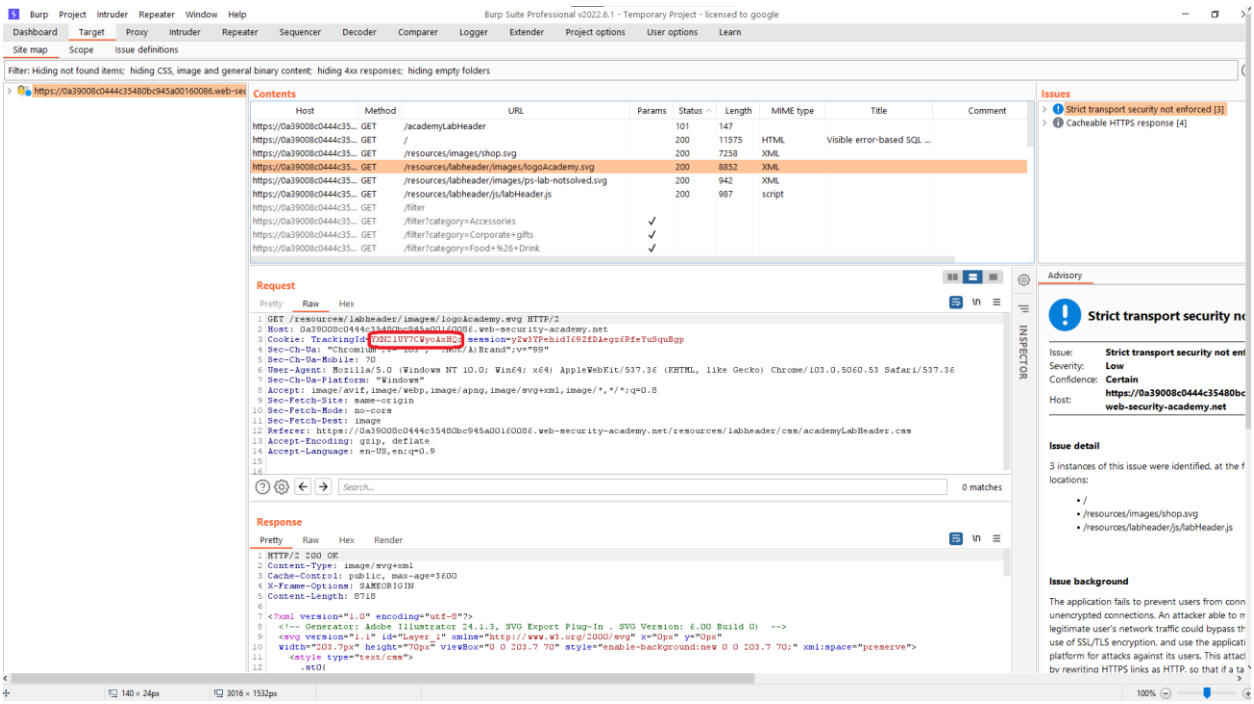
Ta có một trang web như vậy



Bước 1: Đầu tiên chúng ta sẽ mở Brup Suite



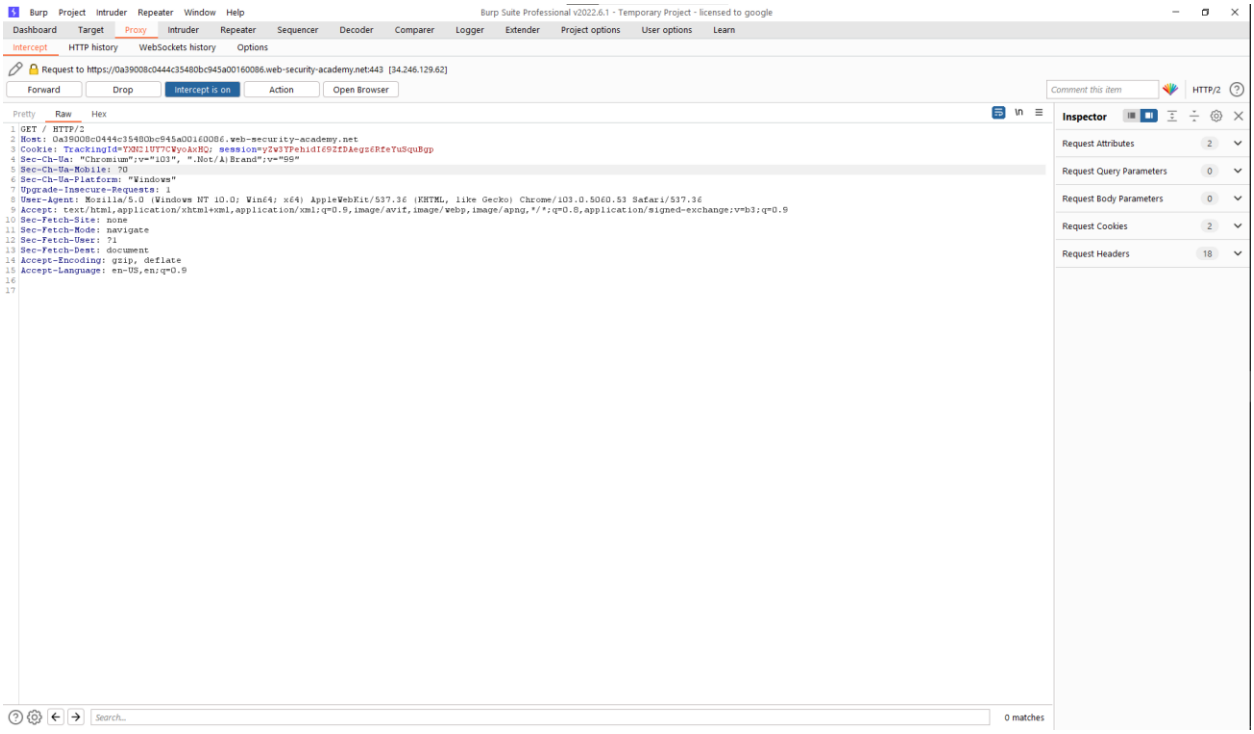
Ta sẽ kiểm tra và thấy được một đoạn cookie để truy vấn của trang web



Câu lệnh SQL để truy vấn web sẽ có dạng

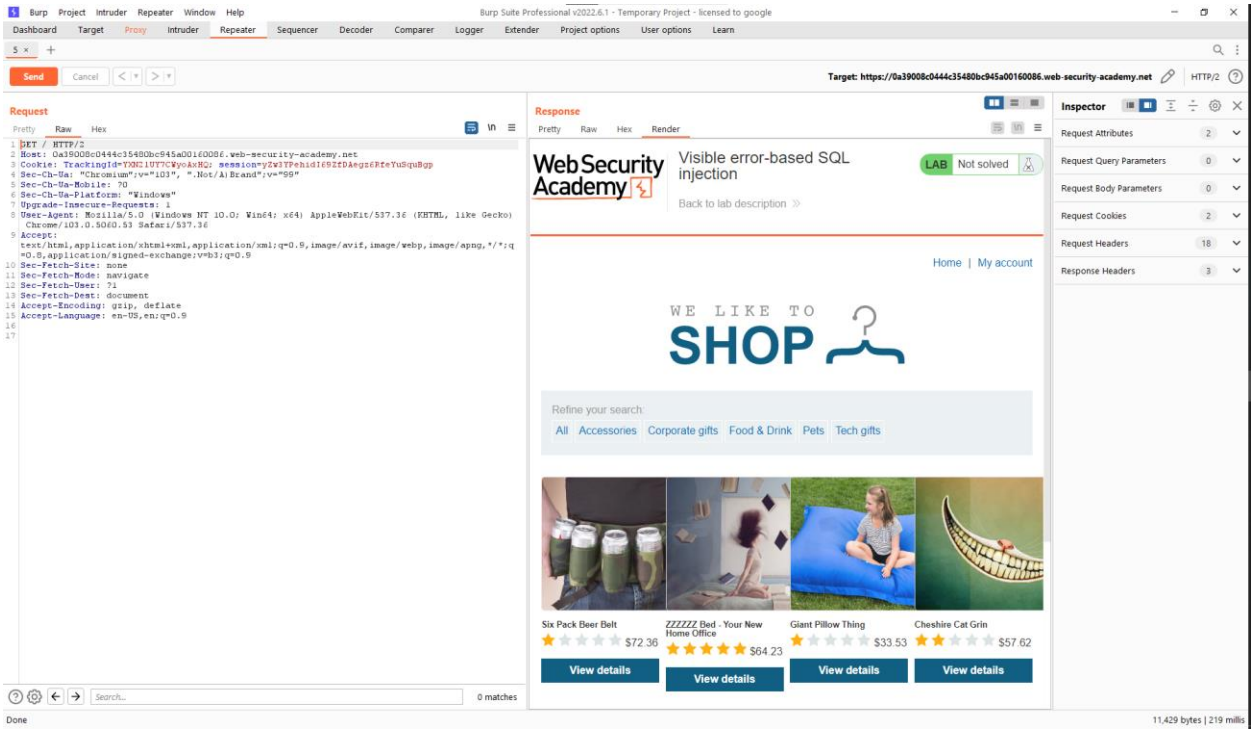
select TrackingID from TeackedUsers where TrackingID ‘YXN2lUY7CWyoAxHQ’

Sauk hi biết được như vậy ta sẽ chuyển sang phần Proxy để lấy ra yêu cầu có chưa TrackeingID



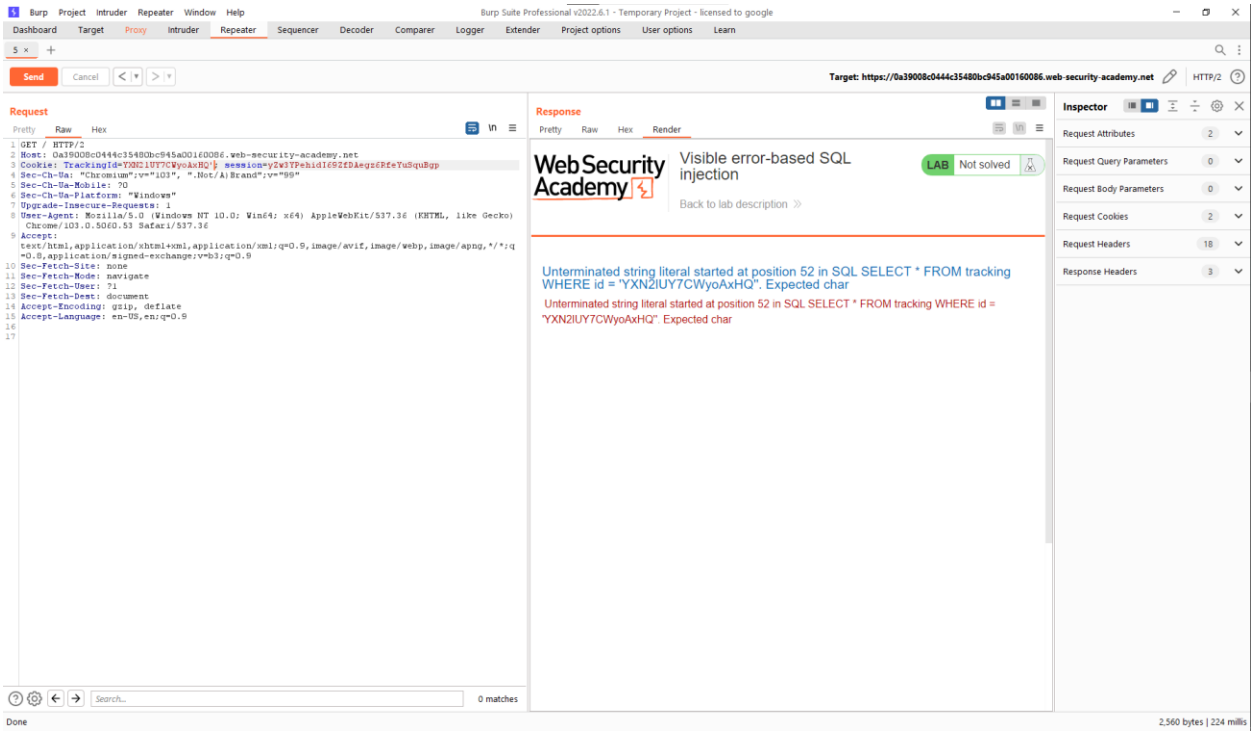
Rồi chuyển toàn bộ đoạn code sang repeater

Sauk hi chúng ta ấn vào nút Send thì chúng ta sẽ có phần response như hình



Giờ chúng ta sẽ thử thêm một kí tự ‘ vào phần TrackingID

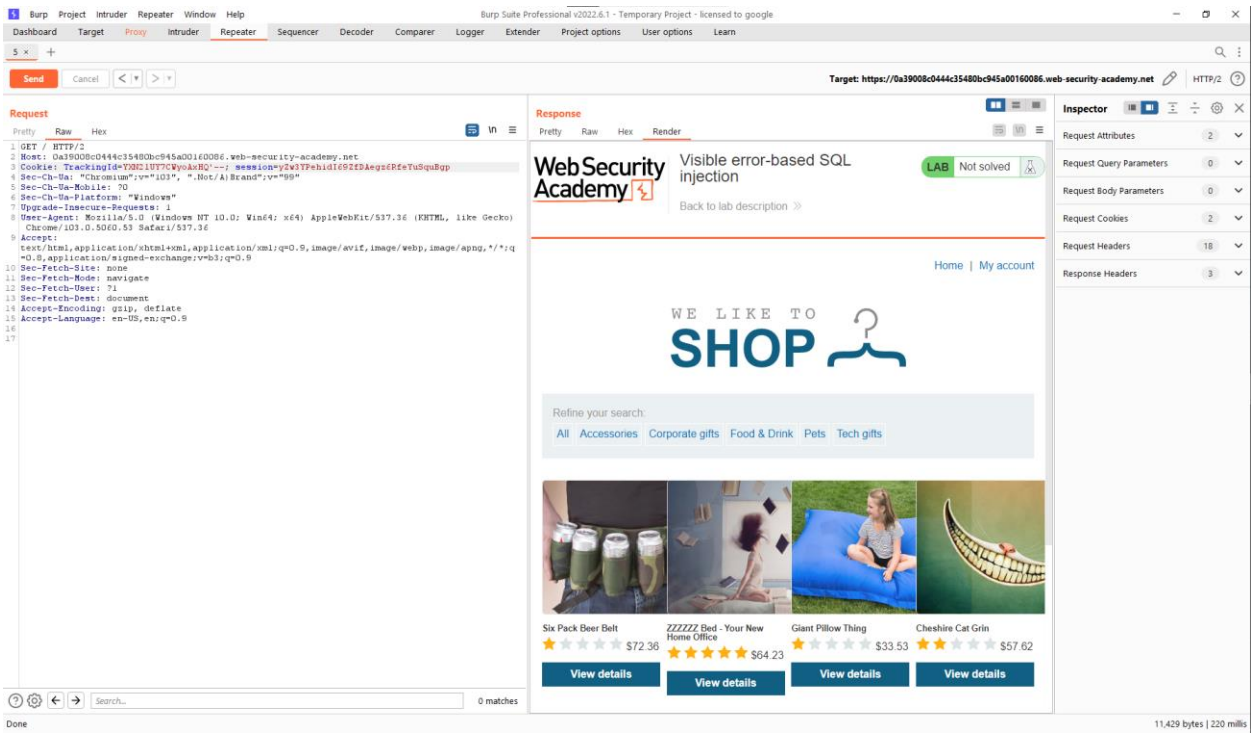
TrackingId= YXN2lUY7CWyoAxHQ'



Sau đó ta sẽ nhận được thông báo lỗi và ta sẽ biết được câu lệnh SQL được truy vấn đã đầy đủ, và điều này cũng chứng minh rằng có một đoạn kí tự string chưa được tiết lộ. Ta cũng thấy được TrackingID của ta có trả lại trong thông báo lỗi.

Sau đó ta sẽ thêm kí tự -- vào đằng sau ta sẽ thấy được

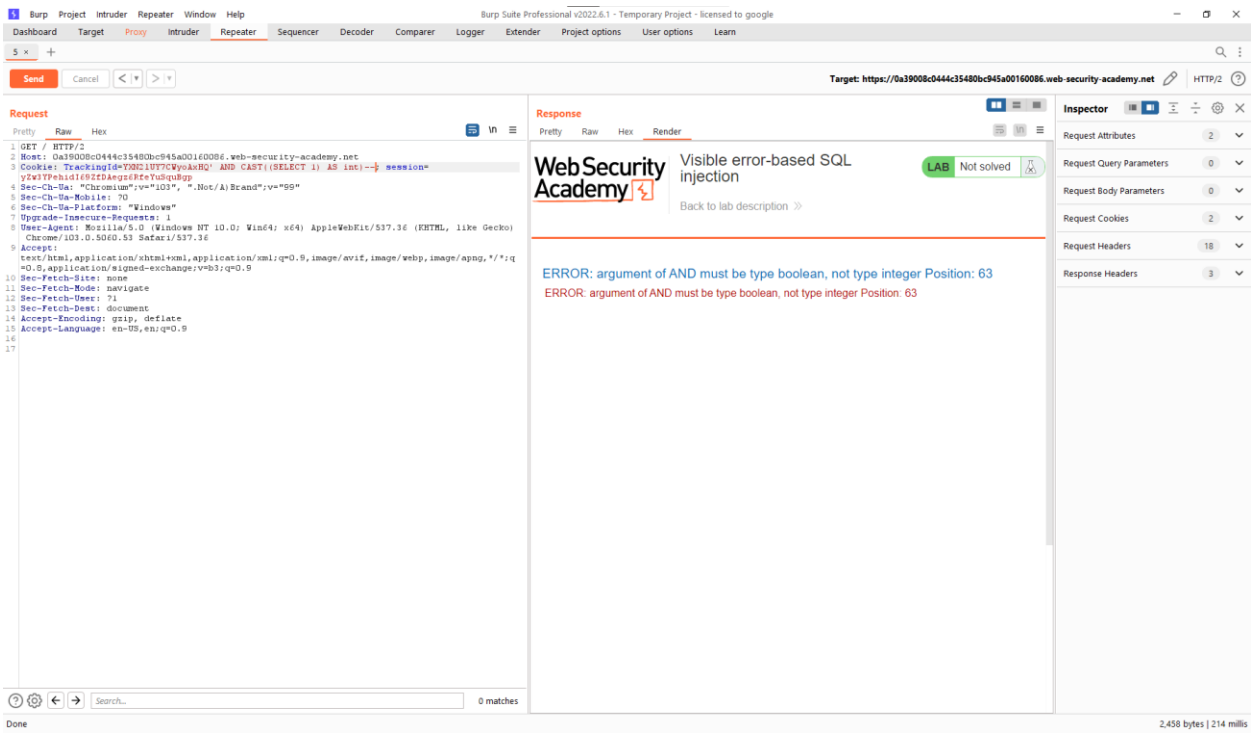
TrackingId= YXN2lUY7CWyoAxHQ'--



Web đã trả về đứng và không còn gặp lỗi nữa cũng thể hiện truy vấn hiện đã trả về giá trị về mặt cú pháp

Giờ ta sẽ thêm vào câu lệnh truy vấn Select và chuyển giá trị về int

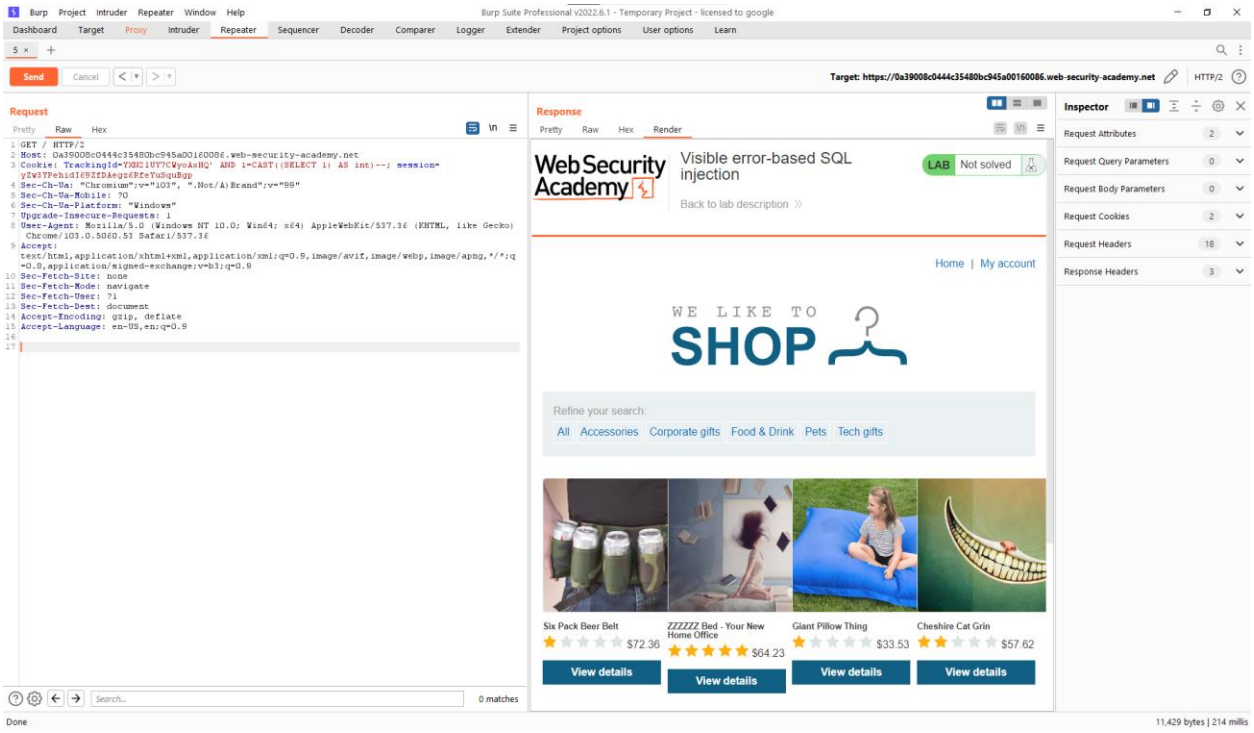
TrackingId= YXN2lUY7CWyoAxHQ' AND CAST((SELECT 1) AS int)--



Ta sẽ nhận được một thông báo lỗi là And thì phải đi với một biểu thức Boolean

Ta sẽ thêm so sanh vào biểu thức truy vấn 1=CAST câu lệnh truy vấn sẽ trở thành

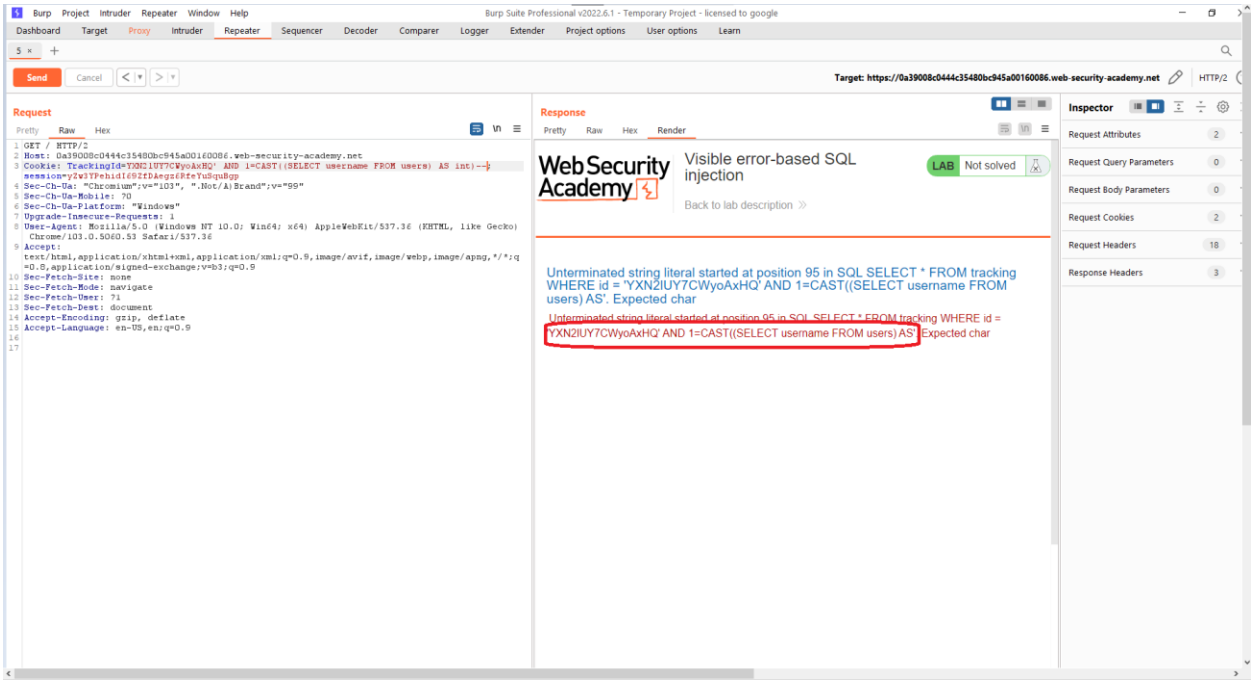
TrackingId= YXN2lUY7CWyoAxHQ' AND 1=CAST((SELECT 1) AS int)-- ta sẽ được



Ta thấy nó đã trả về web điều này cho thấy câu lệnh truy vấn của ta đã hợp lệ

Giờ ta sẽ điều chỉnh câu lệnh truy vấn để nó truy xuất tên người dùng

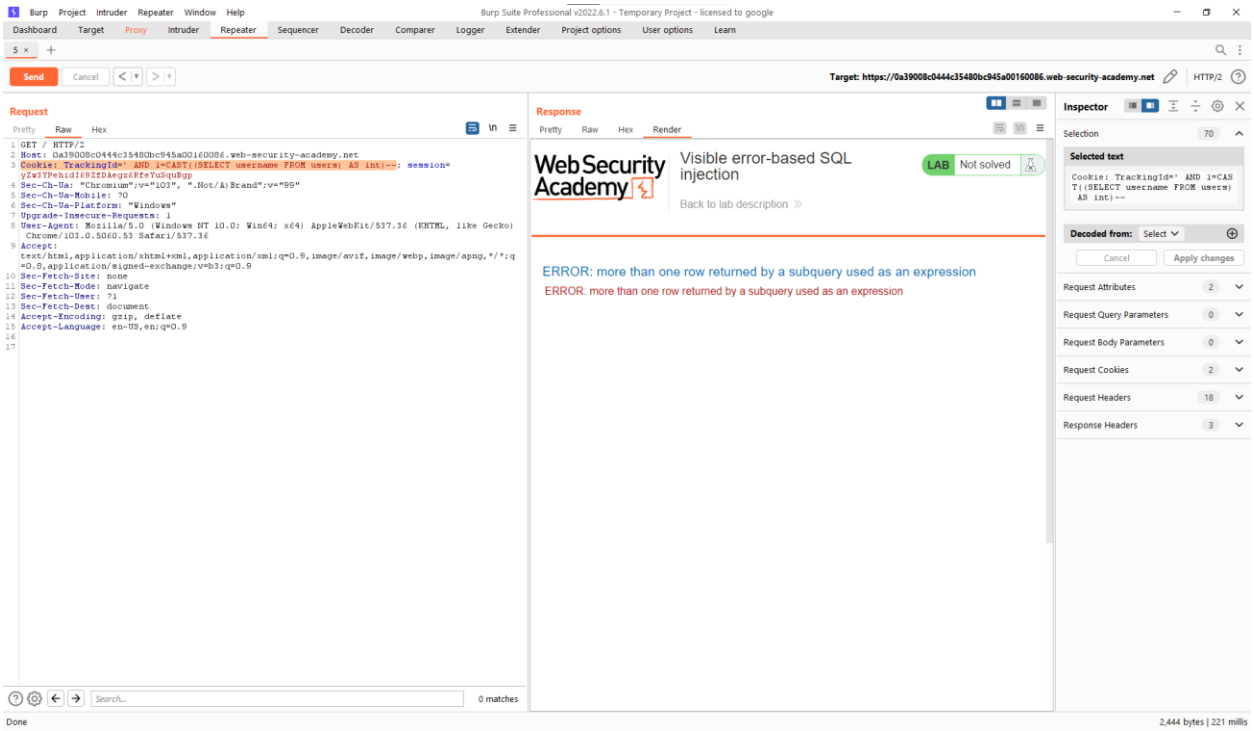
TrackingId=YXN2lUY7CWyoAxHQ' AND 1=CAST((SELECT username FROM users) AS int)--



ở đây ta thấy nó hiển thị lại lỗi như ban đầu và thấy được câu lệnh truy vấn của ta đã bị rút ngắn đi giờ ta sẽ xóa đi phần TrackingID ban đầu

Câu lệnh truy vấn sẽ trở lại như sau

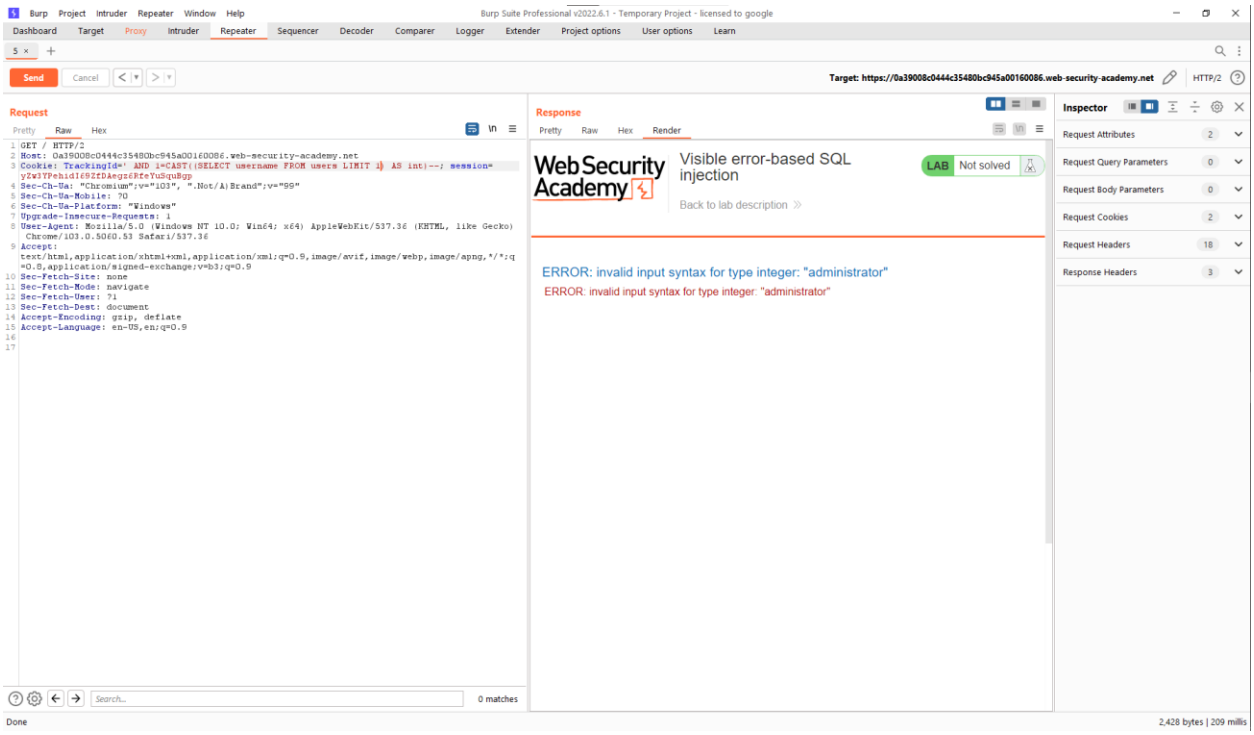
TrackingId=' AND 1=CAST((SELECT username FROM users) AS int)--



Ta tiếp tục nhận được thêm lỗi và lỗi này do nó trả về quá nhiều hàng, nên ta sẽ sửa lại câu lệnh truy vấn để nó chỉ trả lại một hàng

Câu lệnh truy vấn như sau:

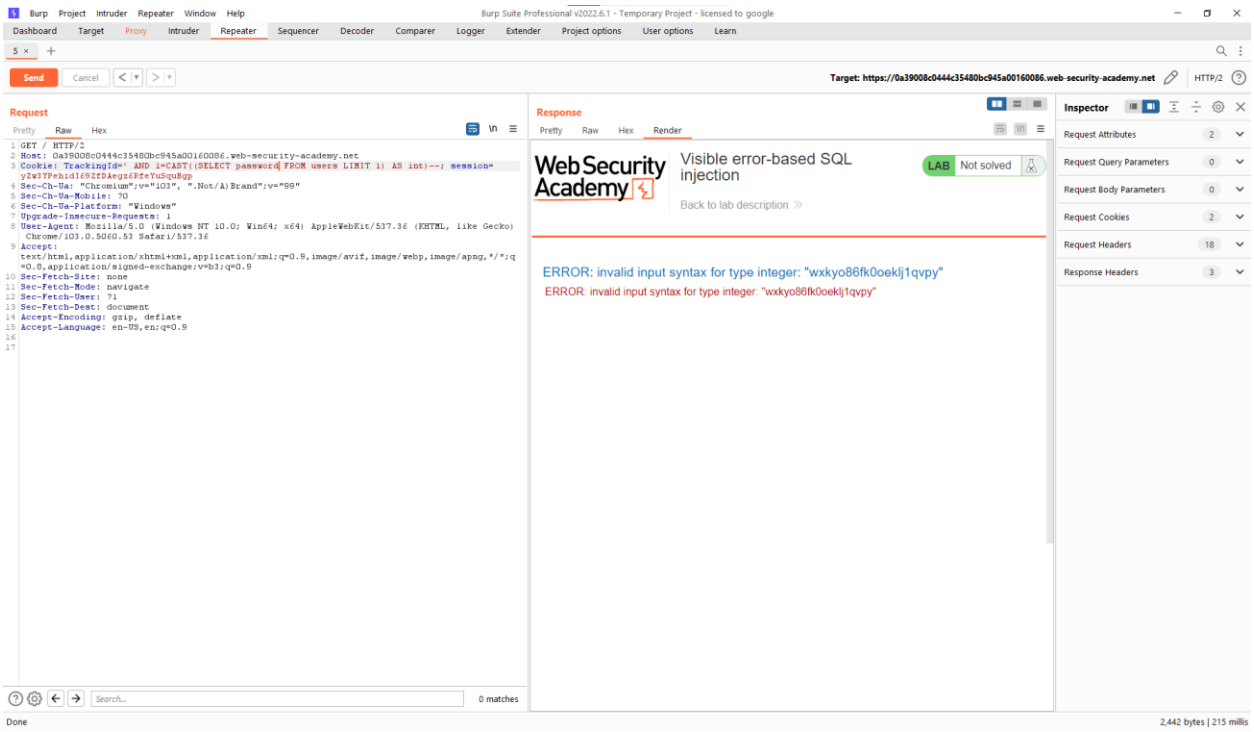
TrackingId=' AND 1=CAST((SELECT username FROM users LIMIT 1) AS int)--



Ở đây ta đã nhìn thấy được user đầu tiên chính là administrator

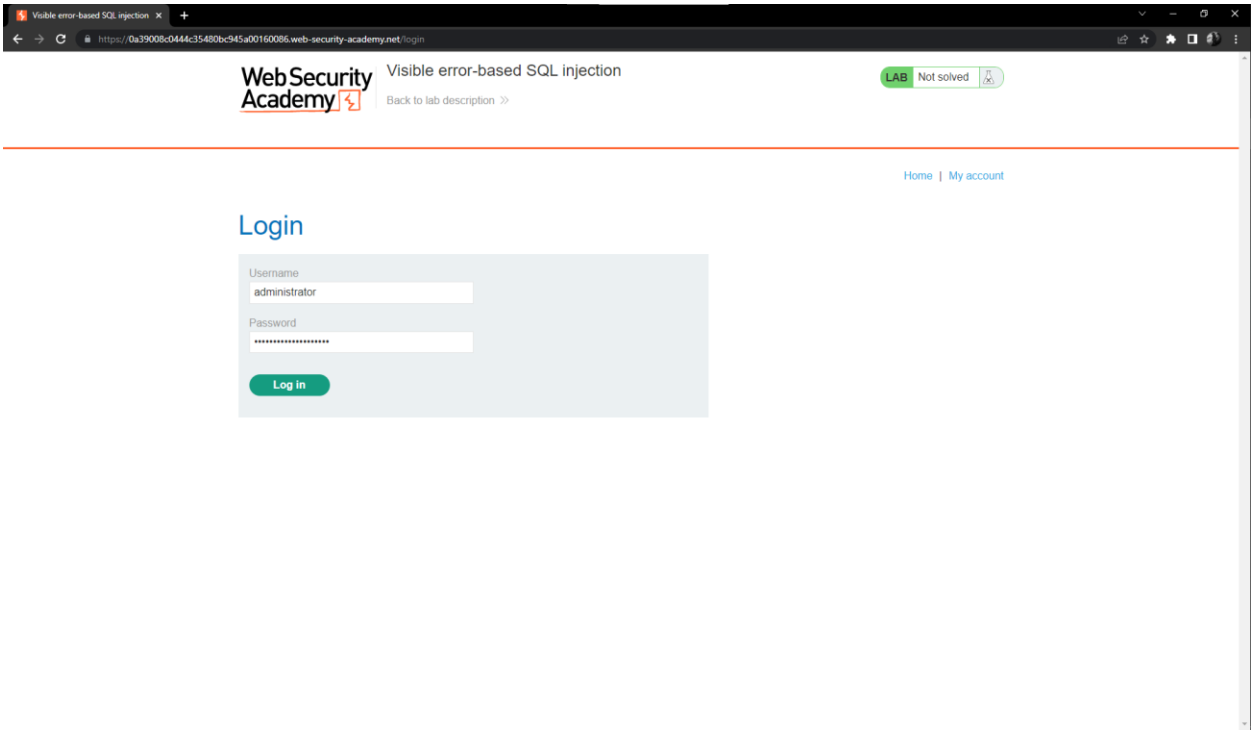
Tiếp đến ta sẽ tìm đến password của administrator với câu lệnh truy vấn là

TrackingId=' AND 1=CAST((SELECT password FROM users LIMIT 1) AS int)--

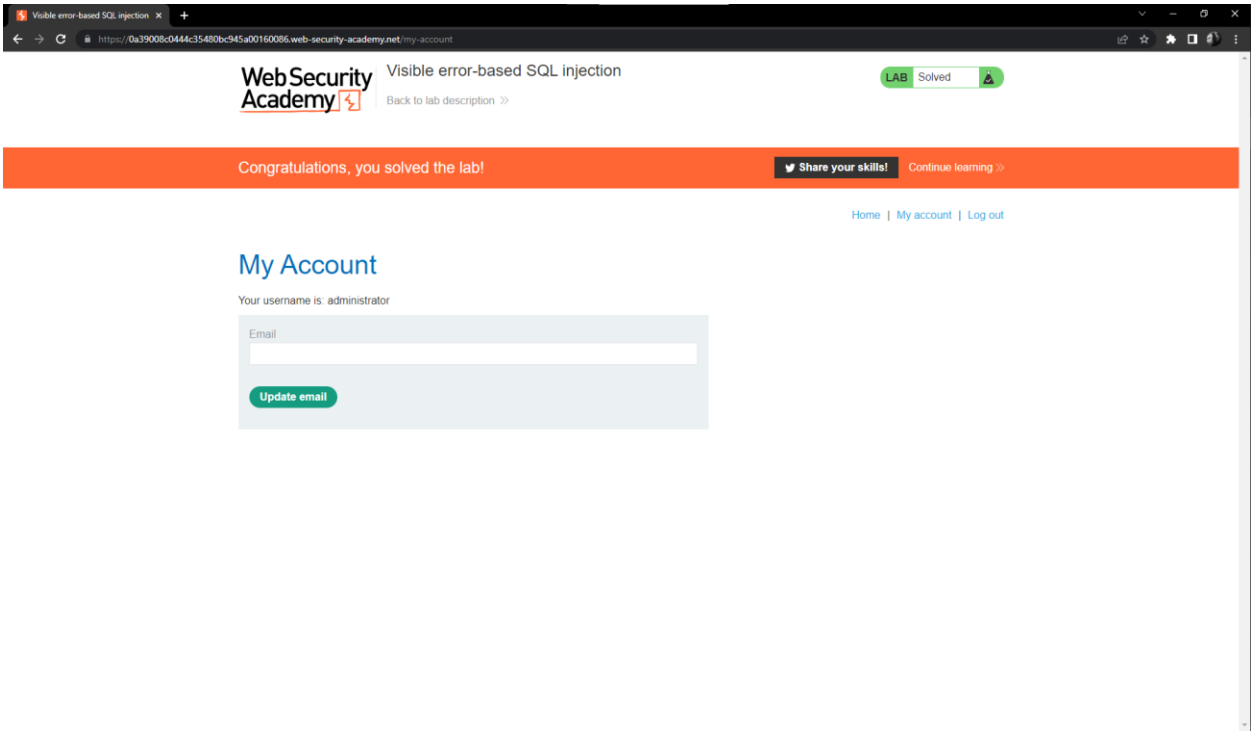


ở đây ta đã thấy được password được trả về là wxkyo86fk0oeklj1qvpy

bây giờ ta sẽ đăng nhập thử bằng những gì ta đã có



Sau khi login ta sẽ thấy được your usename is administrator chứng tỏ chúng ta đã thành công đăng nhập vào user admin của trang web này


Visible error-based SQL injection
https://0a39008c0444c35480bc945a00160086.web-security-academy.net/my-account
Web Security Academy
Visible error-based SQL injection
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account | Log out
My Account
Your username is: administrator
Email
Update email