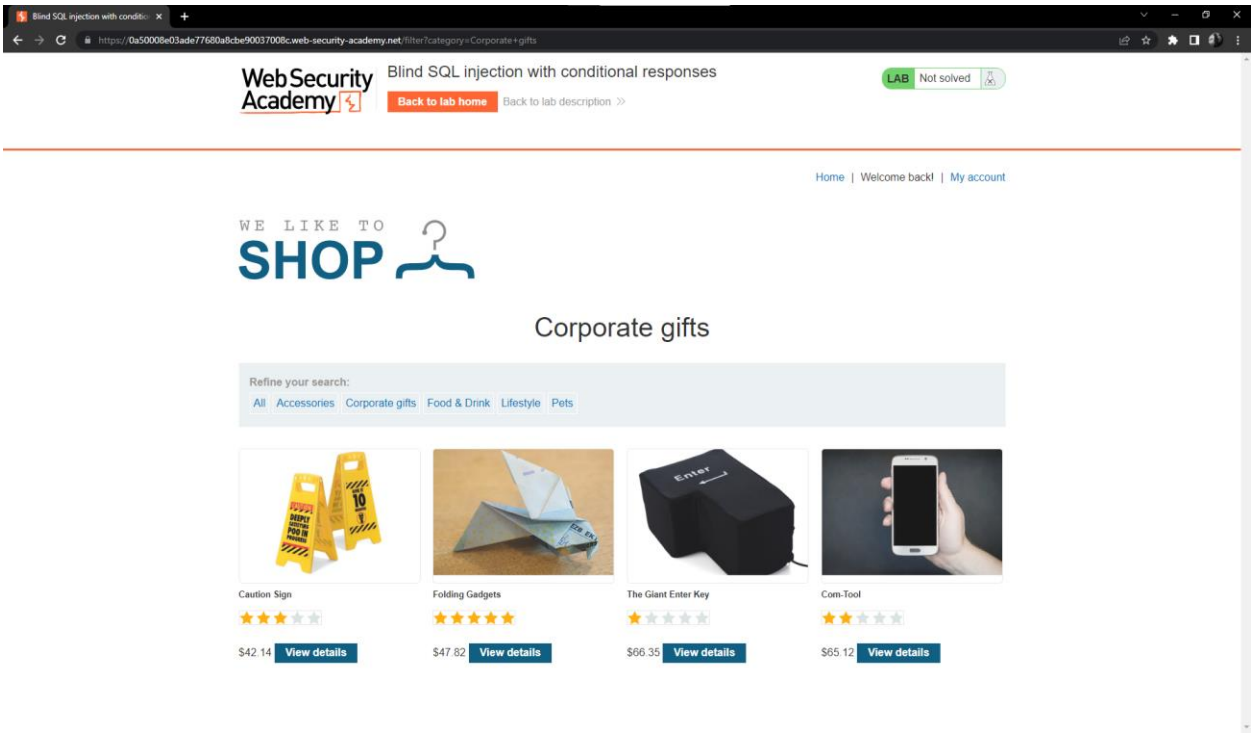
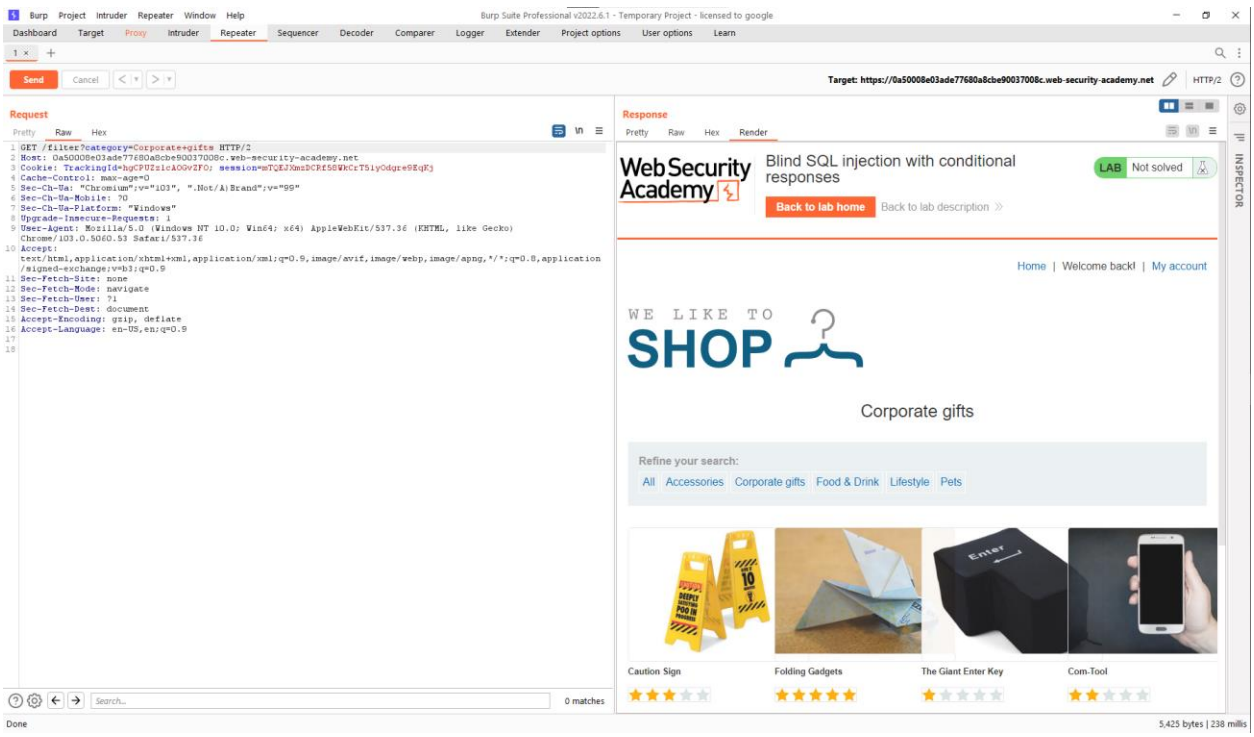
Ở bài Lab này chúng ta sẽ khai thác lỗ hổng Blind SQL injection

Ta có một trang web như



Giờ ta sẽ kiểm tra trang web này trên Brup Suit



Ở đây ta thấy dòng Cookie của trang web

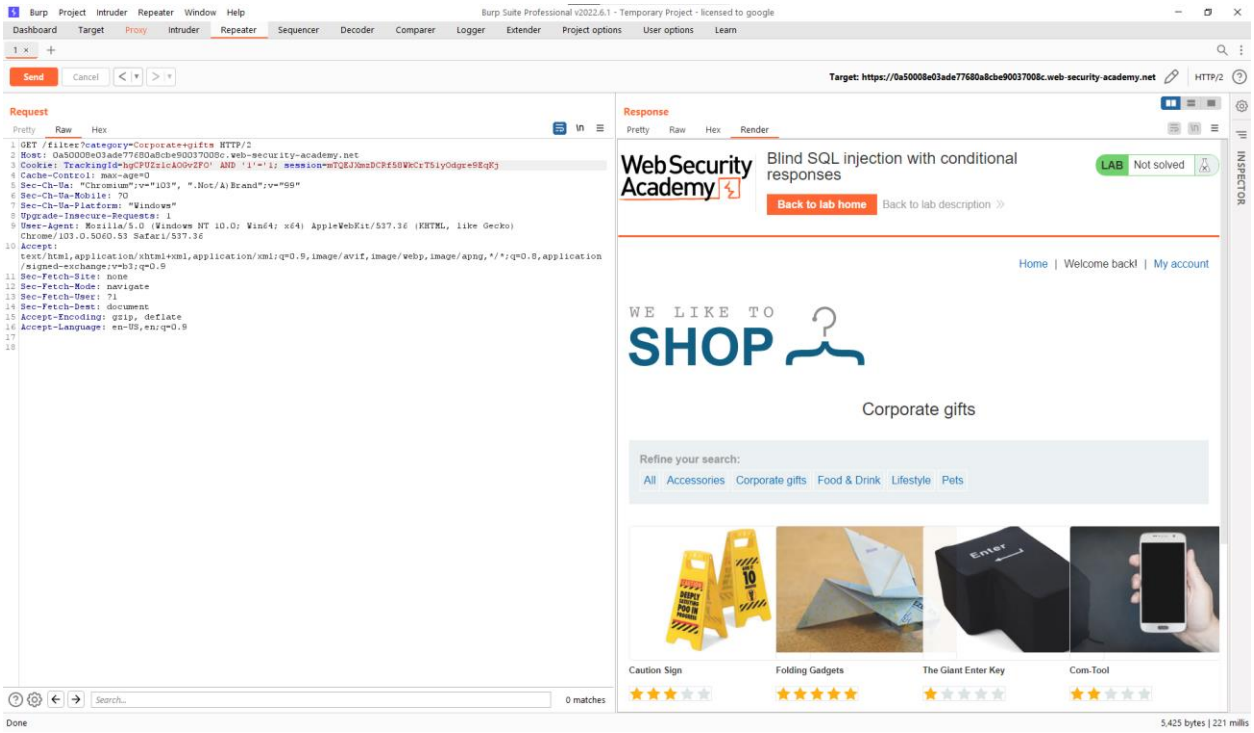
TrackingId=hgCPUZzlcAOGvZFO

Câu lệnh SQL để truy vấn web sẽ có dạng

select TrackingID from TeackedUsers where TrackingID ‘hgCPUZzlcAOGvZFO’

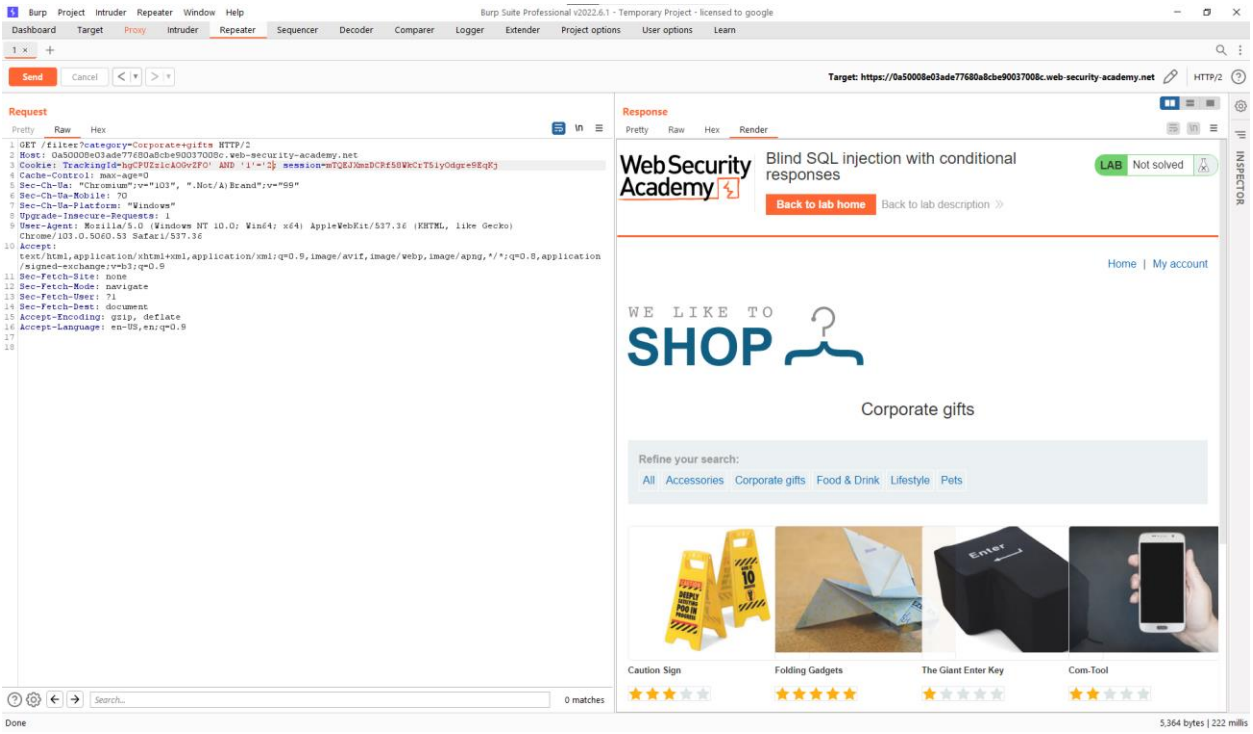
Giờ ta sẽ đi thay đổi câu lệnh này thành

TrackingId= hgCPUZzlcAOGvZFO ' AND '1'='1



Tiếp theo ta sẽ tiếp tục thay đổi nó thành

TrackingId= hgCPUZzlcAOGvZFO ' AND '1'='2

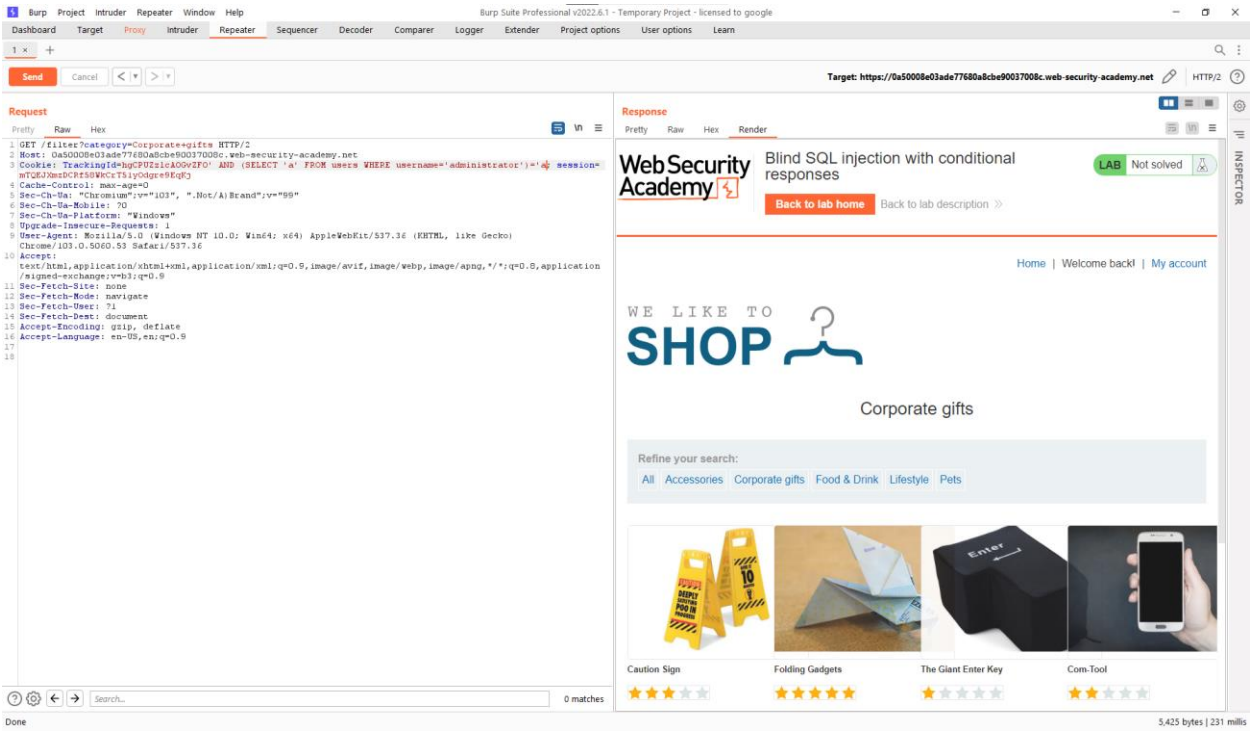


Sau khi ta thay đổi ta đã không còn thấy dòng chữ Welcome back! Xuất hiện nữa

Điều này chứng tỏ chúng ta có thể kiểm tra điều kiên Boolean và suy ra được kết quả

Tiếp theo chúng ta sẽ kiểm tra xem có user nào tên là administrator trong dữ liệu của username hay không

TrackingId=hgCPUZzlcAOGvZFO' AND (SELECT 'a' FROM users WHERE username='administrator')='a

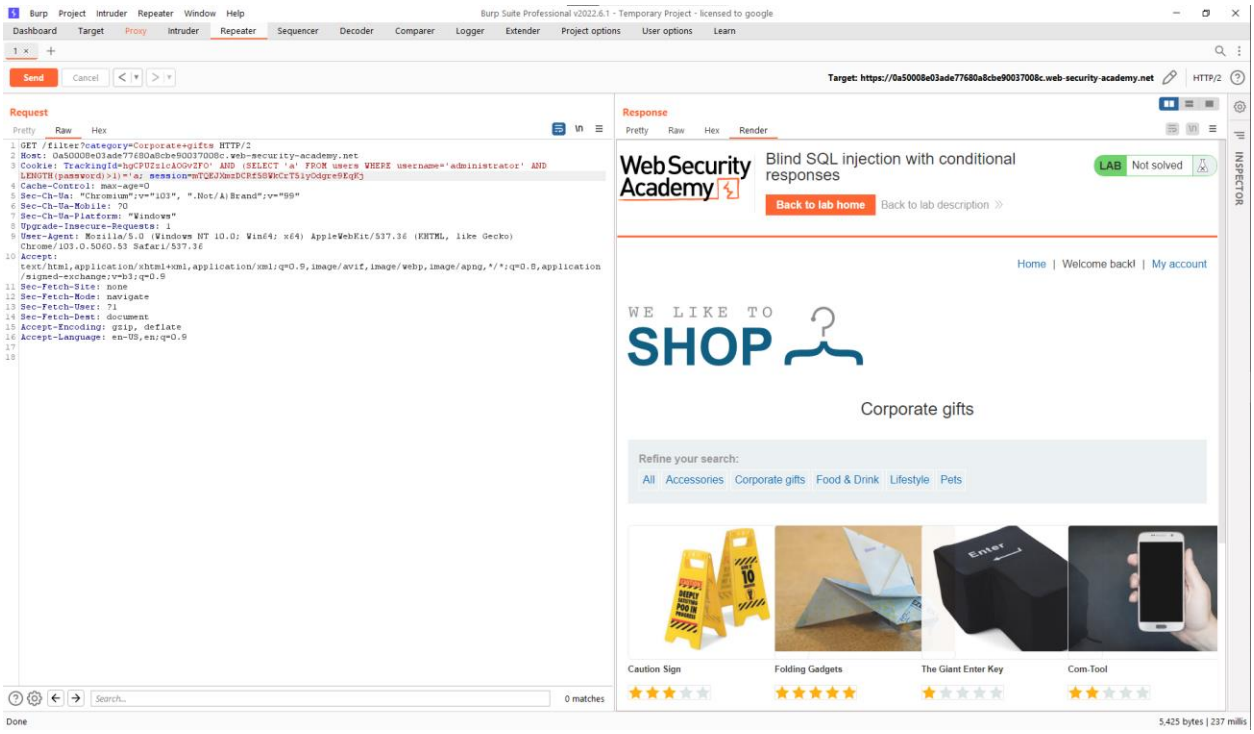


Ta thấy nó hiện lên chữ Welcome back! Chứng tỏ có một user với tên là administrator

Sau khi biết được tên user thì chúng ta sẽ phải đi kiểm tra password của nó

Trước hết chúng ta sẽ kiểm tra xem password của user administrator có bao nhiêu kí tự

TrackingId=hgCPUZzlcAOGvZFO' AND (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)>1)='a

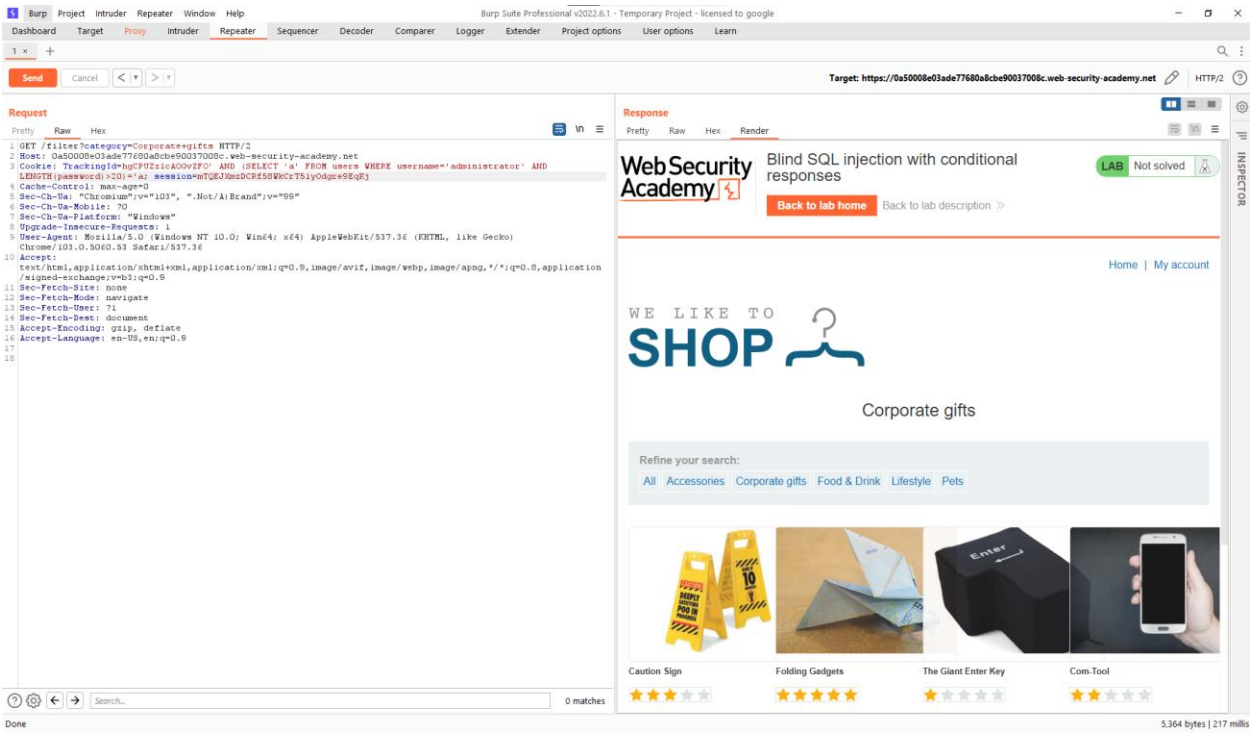


Ở câu lệnh này chúng ta biết được là password này có nhiều hơn 1 kí tự

Việc bây giờ của chúng ta sẽ là phải tăng Length của password lên và kiểm tra cho đến khi nó không hiện Welcome back! Nữa

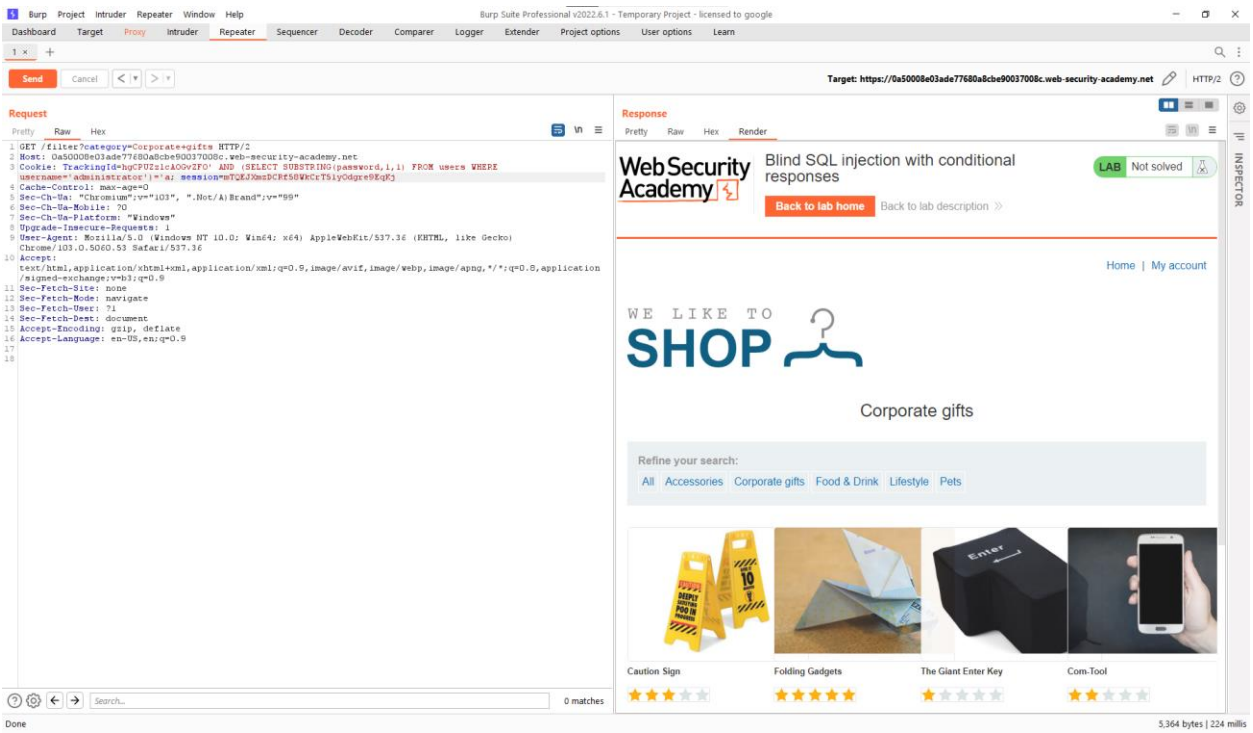
Và sau khi thử rất nhiều lần và dừng lại ở con số là 20 thì chữ Welcome back! Không còn xuất hiện nữa

Vậy ta xác định được password của user administrator có 20 kí tự tất cả



Câu lệnh để kiểm tra xem kí tự của password ở vị trí đó đúng không nó sẽ là

TrackingId=hgCPUZzlcAOGvZFO' AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')='a

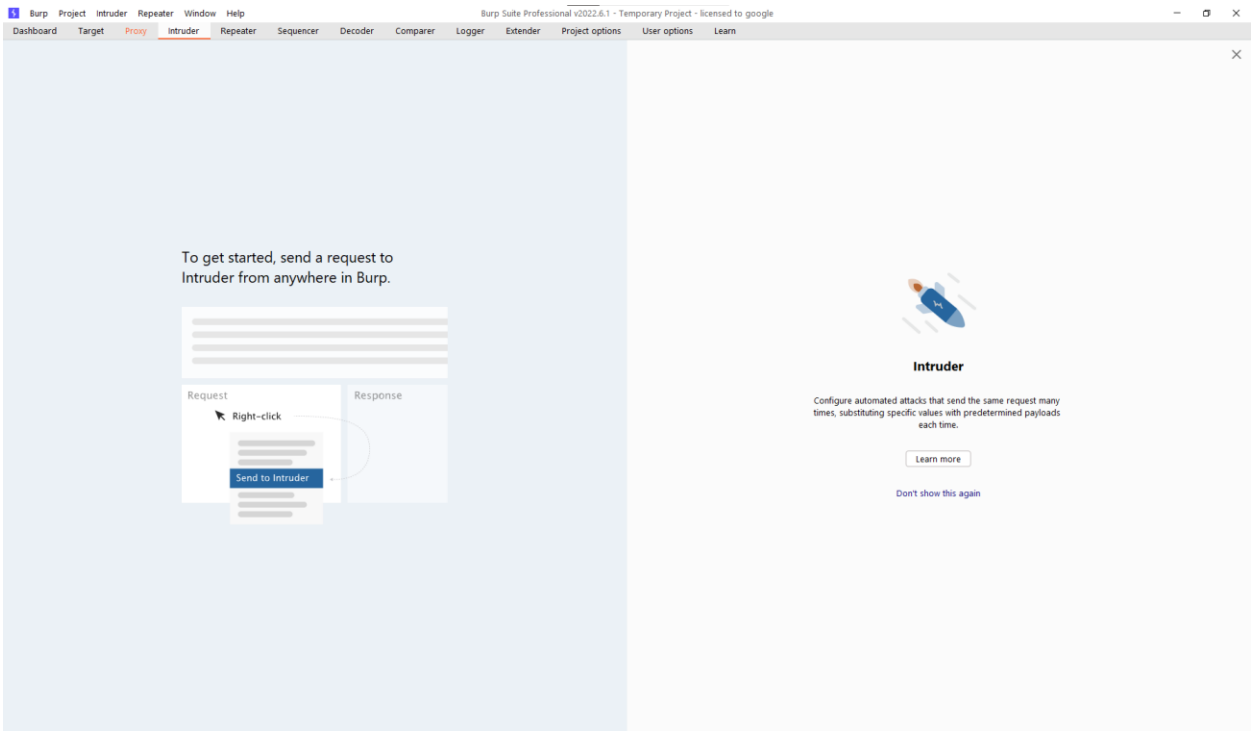


Ở đây với kí tự a không trùng khớp với kí tự ở vị trí thứ nhất của password việc của chúng ta là thử từng kí tự một cho đến khi nó hiện ra chữ Welcome back! Thì dừng và kiểm tra ở vị trí thứ 2

Với câu lệnh

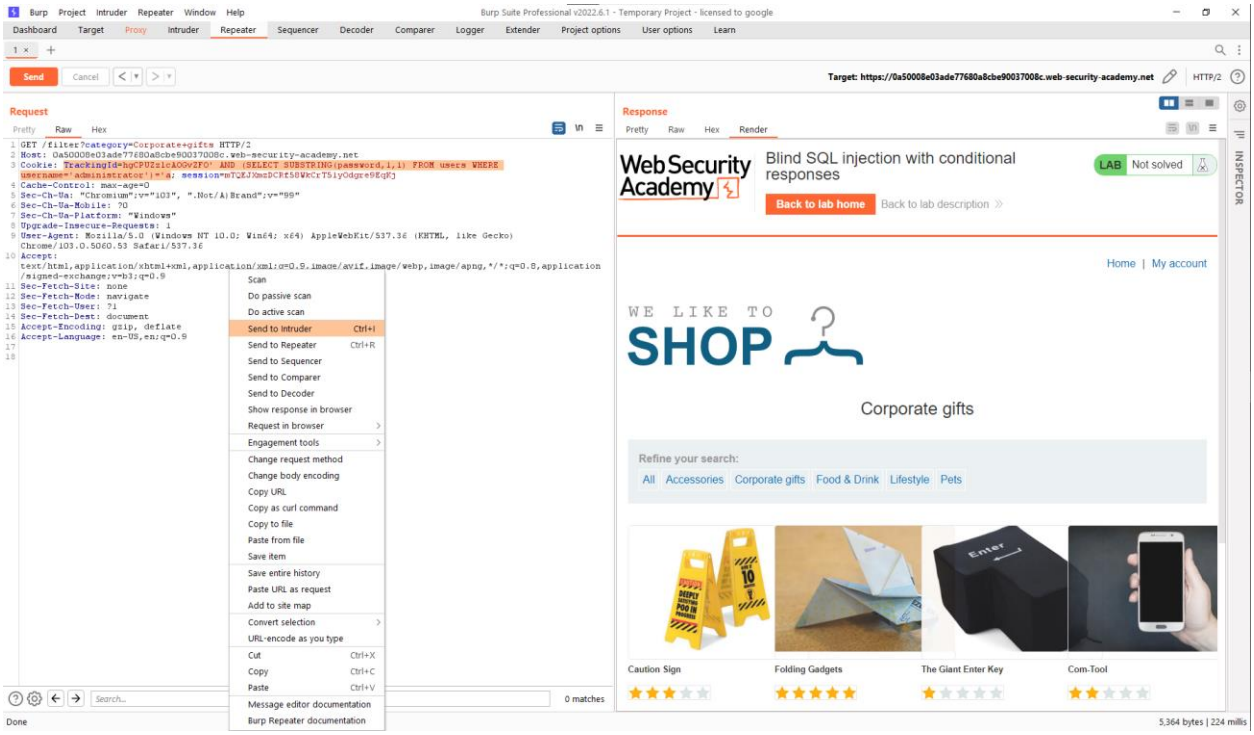
TrackingId=hgCPUZzlcAOGvZFO' AND (SELECT SUBSTRING(password,2,1) FROM users WHERE username='administrator')='a

Những mà việc này mà làm tay thì sẽ rất là cực nên chúng ta cần tìm một tool gì đó để làm cho nhanh

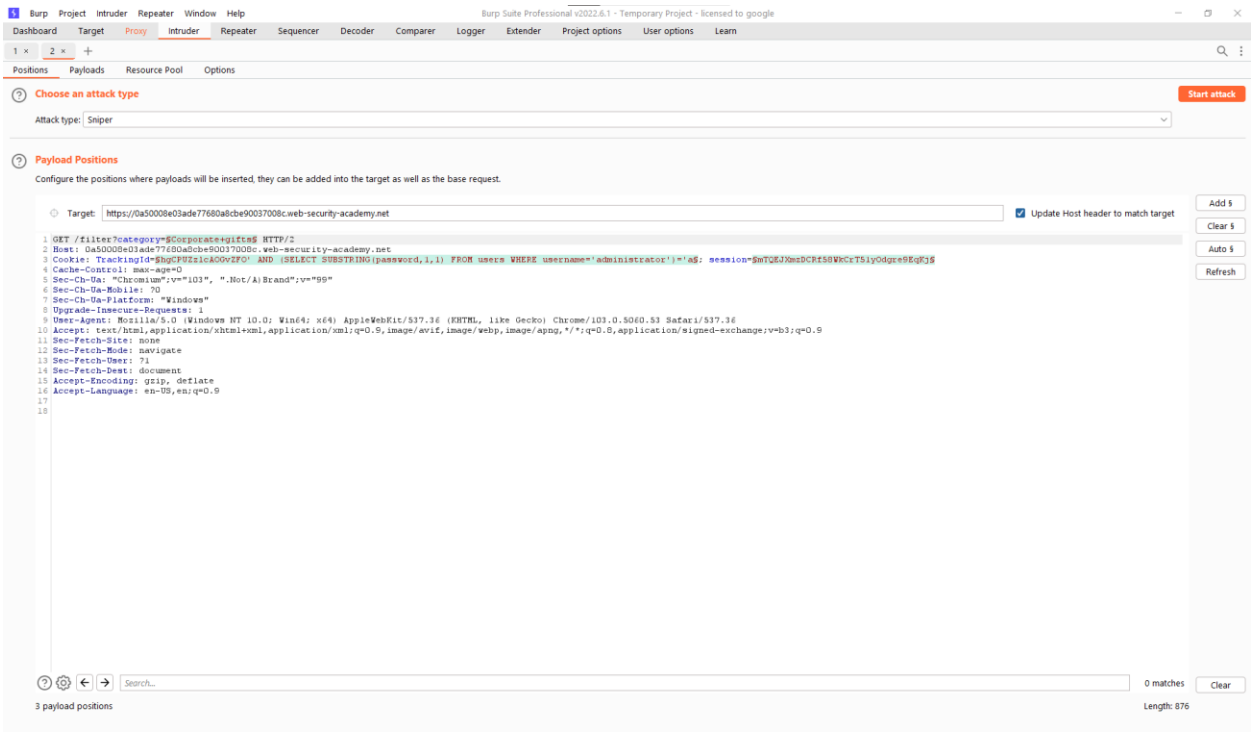


ta sẽ vào Intruder trong Brup Suit để kiểm tra nó nhanh hơn

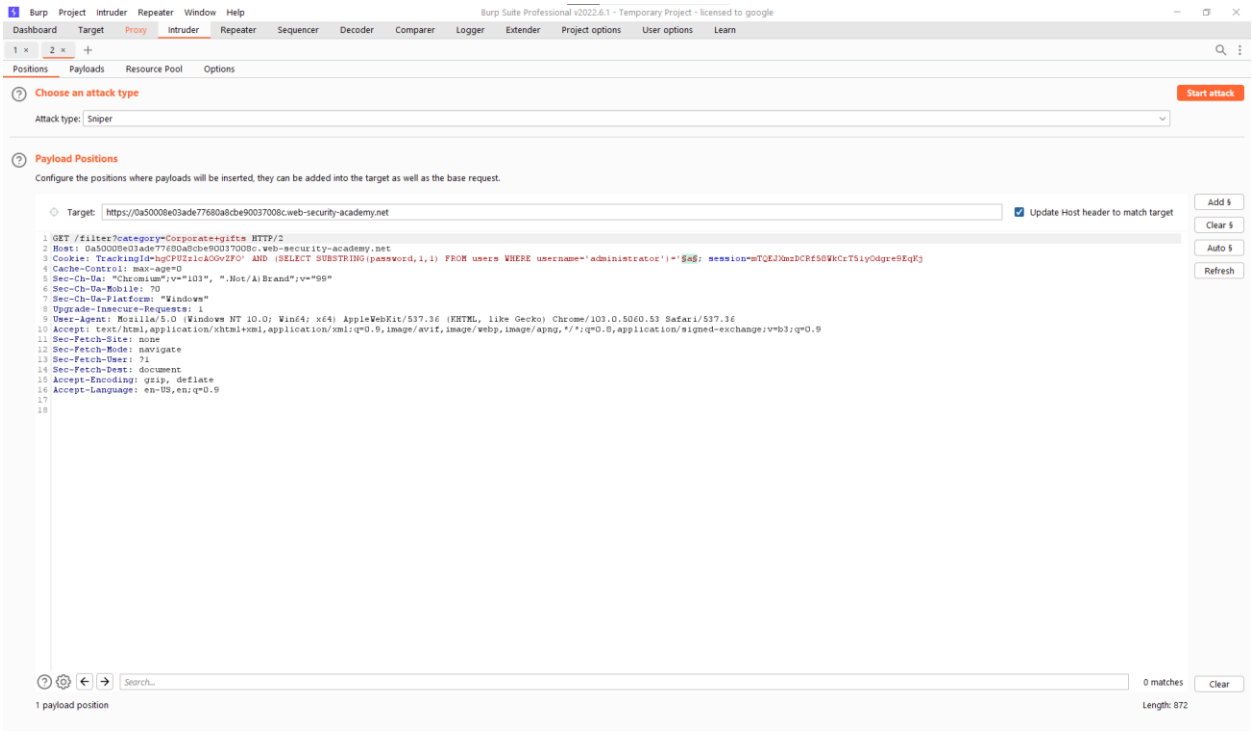
Ta sẽ send code từ Repeter sang Intruder



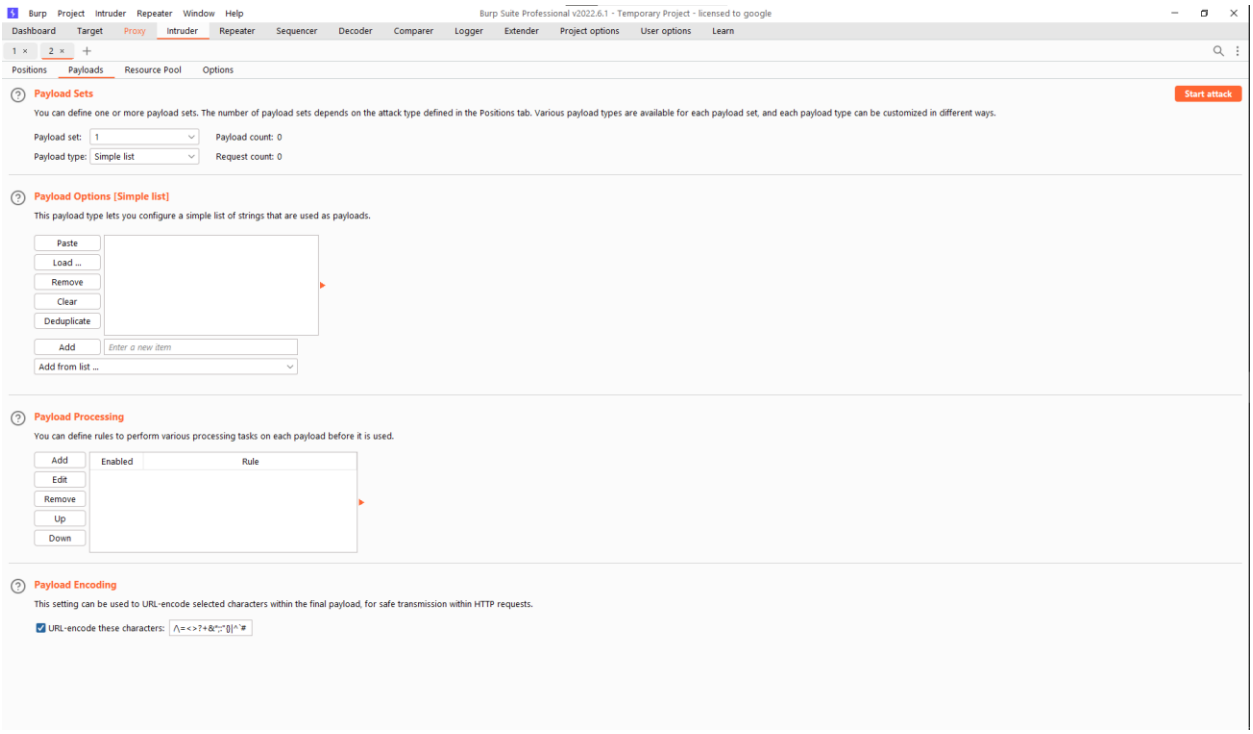
Chúng ta sẽ ra được giao diện như vậy



Sau đó ta sẽ add kí tự ở chữ ADD bên góc phải màn hình vào nơi mà chúng ta cần phải thay đổi kí tự để check

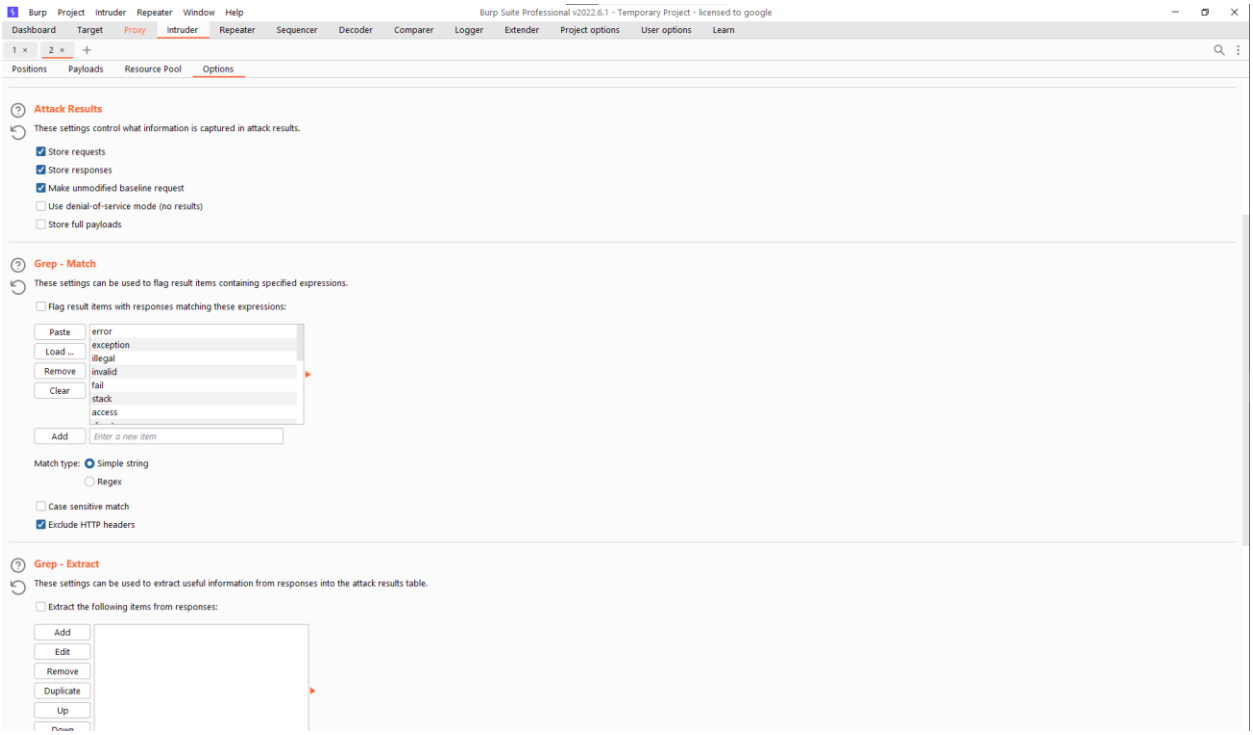


Sau khi add kí tự vào xong chúng ta chuyển sang phần Payload

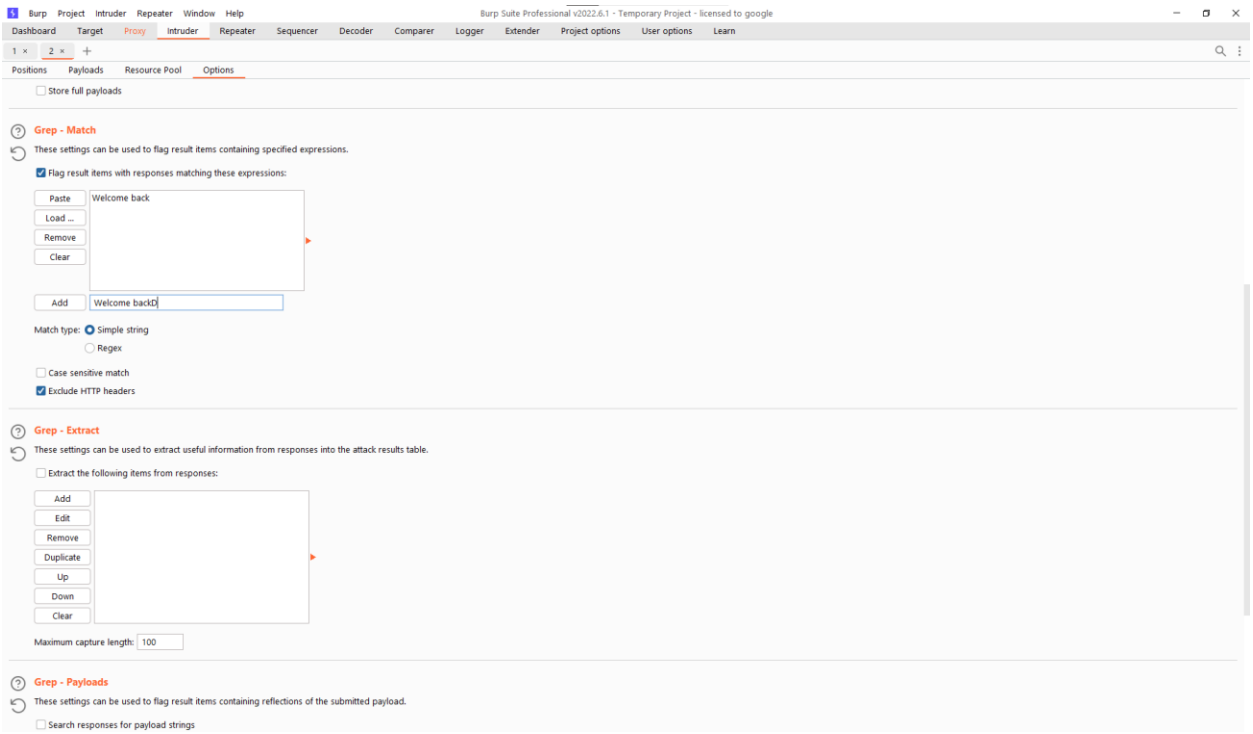


Ở đây ta sẽ add a-z và 0-9 tại password này theo đề bài cho thì chỉ có chữ cái thường và chữ số

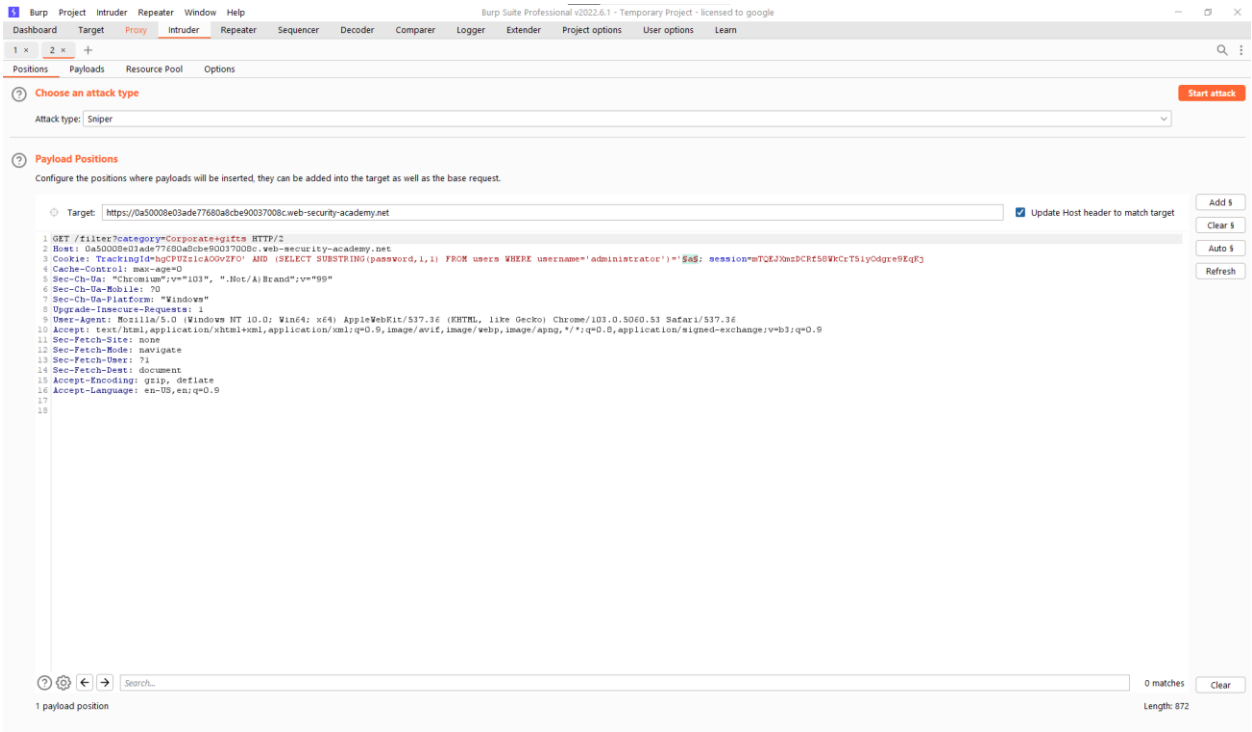
Sau đó ta sẽ chuyển sang phần Options để chỉnh flag chúng ta cần tìm



Ta sẽ add Welcome back vào flag ta cần tìm



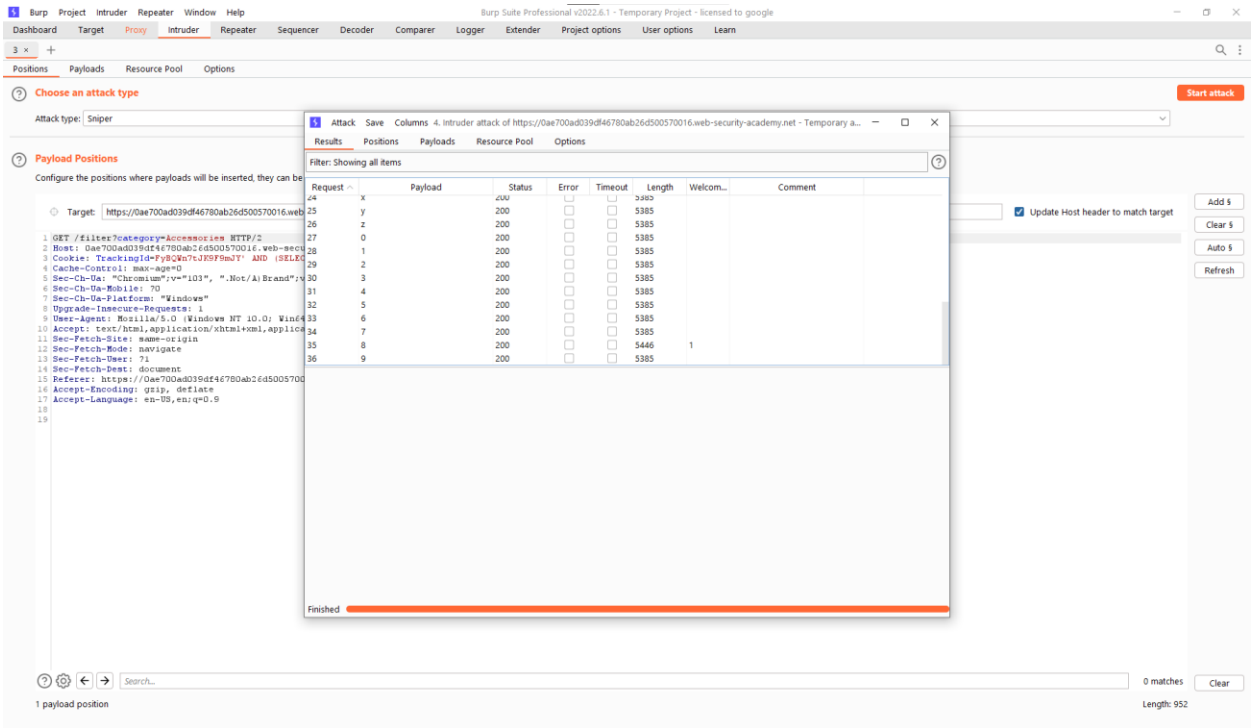
Sau đó ta về lại Position



Sau đó ấn Start attackbox

Ở đây do làm bài lâu quá nên bài lab đã bị reset nên trong ảnh TrackingID sẽ khác

Và sau khi start attackbox ta được kết quả

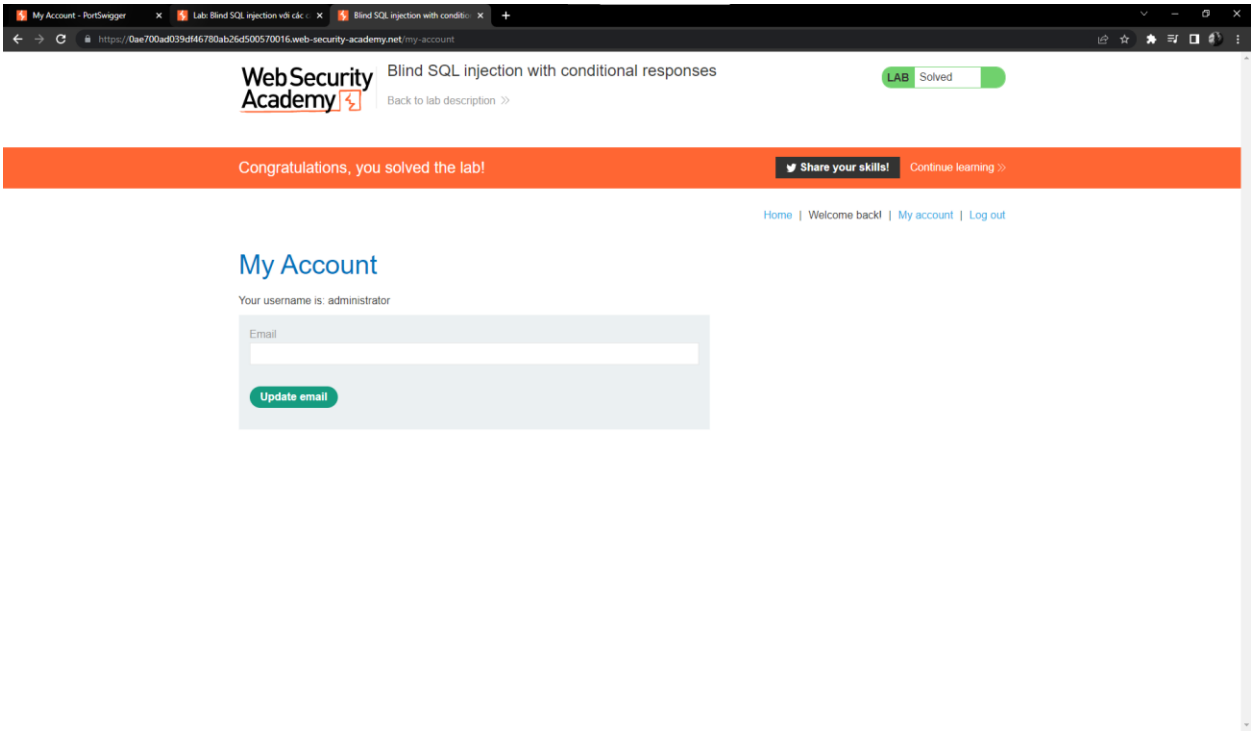


Kí tự 8 có xuất hiện Welcome back vậy kí tự đầu tiên của password là 8

Điều tiếp theo ta cần làm là thay đổi vị trí kí tự password cần tìm và sau khi tìm ở cả 20 vị trí ta được password là

8wbp8vtm7bs29srrxq3s

Vậy ta đã tìm được đủ 20 kí tự của password việc bây giờ ta làm sẽ là đăng nhập bằng user administrator với password là 8wbp8vtm7bs29srrxq3s xem có được không



Vậy là ta thành công đăng nhập bằng user administrator và khai thác thành công lỗ hổng Blind SQL injection