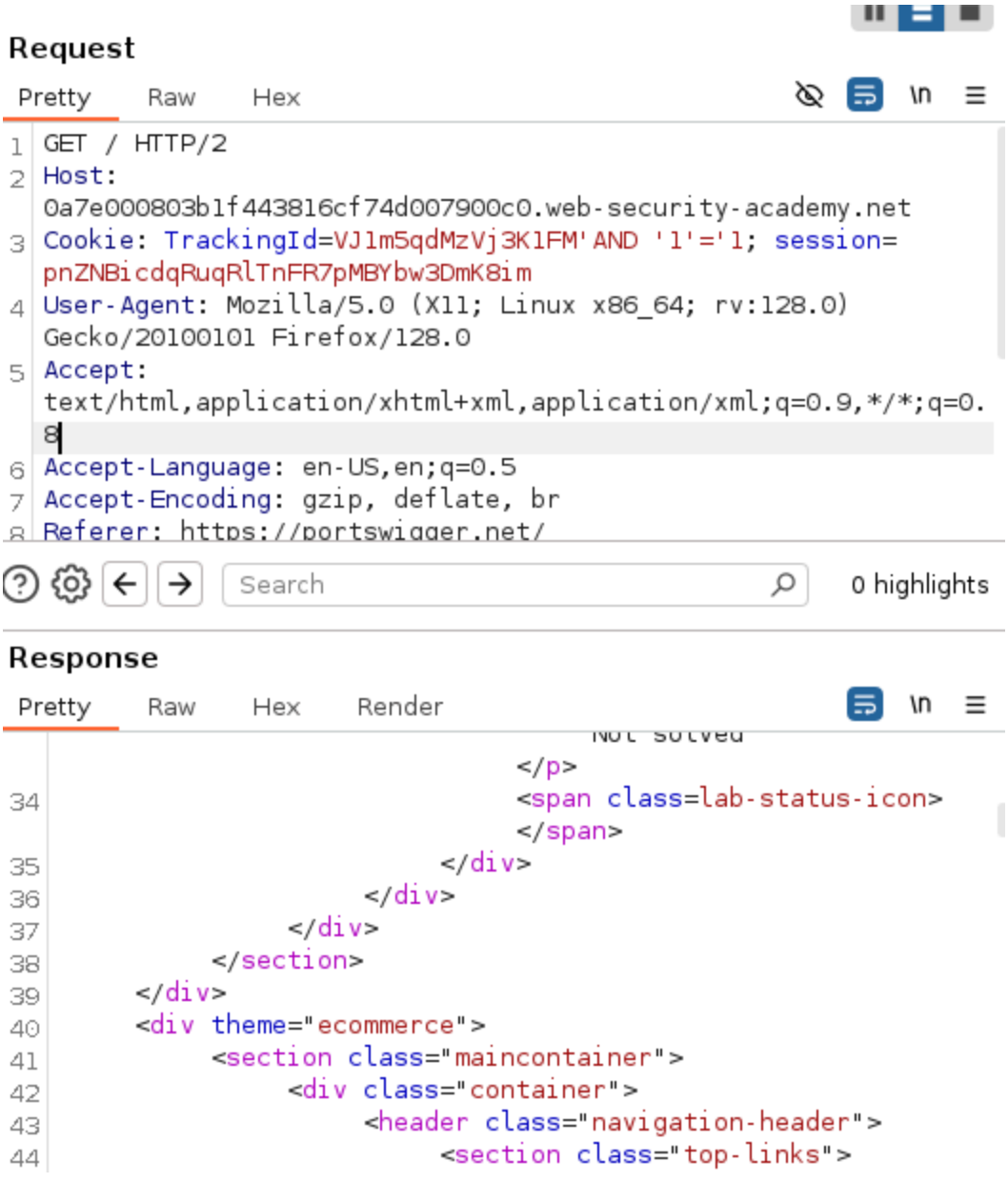
9 Lab Blind SQL injection with conditional responses

EL primer paso es hacer el modificado del TrackingID y comprobar que este campo es vulnerable, par ello implantaremos en el campo TrackingID lo siguiente:

``'AND '1'='1

Utilizamos esta sentencia ya que el Backend comprobaria el valor de este TrackerId con esta sentencia (mas o menos):

``SELECT Tracking_id FROM Tracking_table WHERE TrackingId = 'VJ1m5qdMzVj3K1FM'

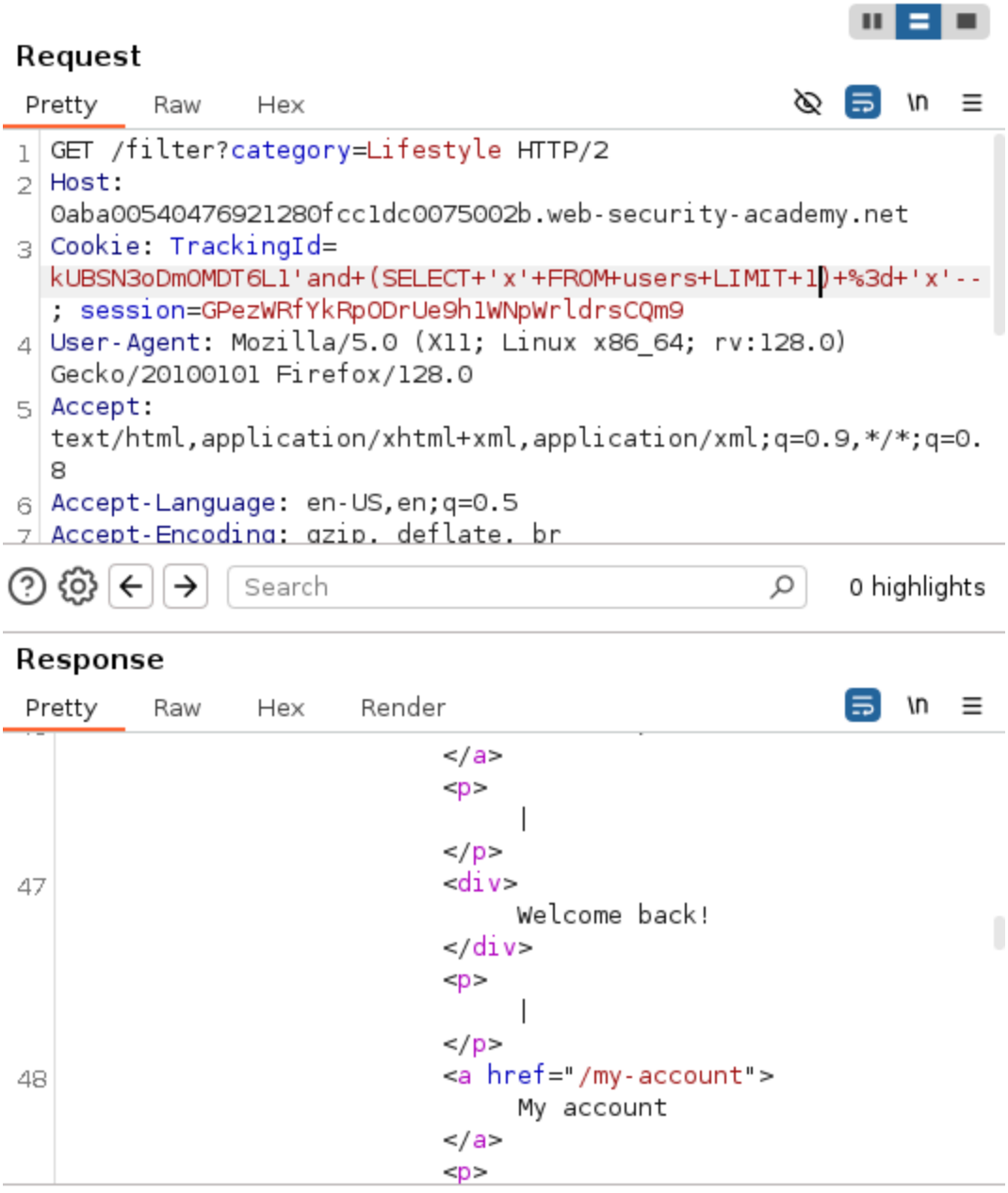


Como el campo TrackingId va a comprobar si es e valor es TRUE o no, vamos a usar esto para que se nos reporte información de la página web. si recibimos un "Welcome Back" será que la consulta es TRUE de lo contrario es FALSE:

Primero vamos a comprobar si existe una tabla users, para ello utilizaremos la siguiente sentencia en el TrackingID:

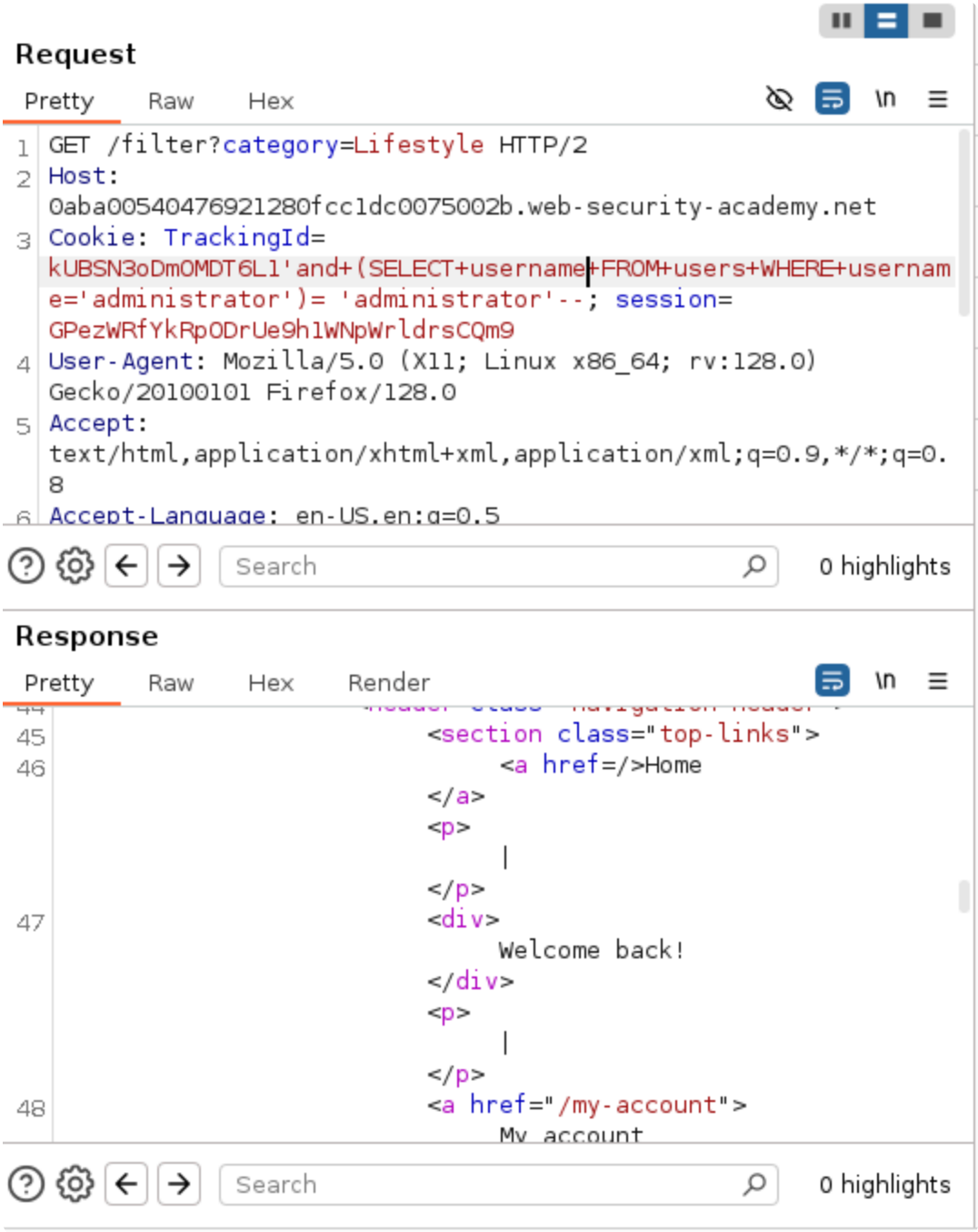
``'(SELECT+'x'+FROM+users+LIMIT+1)+%3d+'x'--

Vemos como nos responde con un TRUE, por lo que la tabla "users" existe:



Comprobamos que existe una columna llamada username que tiene un contenido llamado 'administrator':

`` 'and+(SELECT+username+FROM+users+WHERE+username='administrator')= 'administrator'--



Ahora que sabemos que funciona vamos a sacra la contraseña del usuario administrator creando un payload con Burpsuite, para ello mandamos la petición al Intruder con la siguiente sentencia:

``'+AND (SELECT+SUBSTRING(password,1,1)+FROM+users+WHERE+username+%3d+'administrator')+%3d+'a'--

Con esta sentencia buscamos palabra por palabra la contraseña del usuario, en caso de que la letra sea correcta el servidor nos devolverá un Welcome Back, por lo que en el Intruder creamos un ataque de tipo Cluster bomb para itirenar las posibles respuestas de numero (longitud de de la contraseña) y de letras y números (la contraseña en sí)