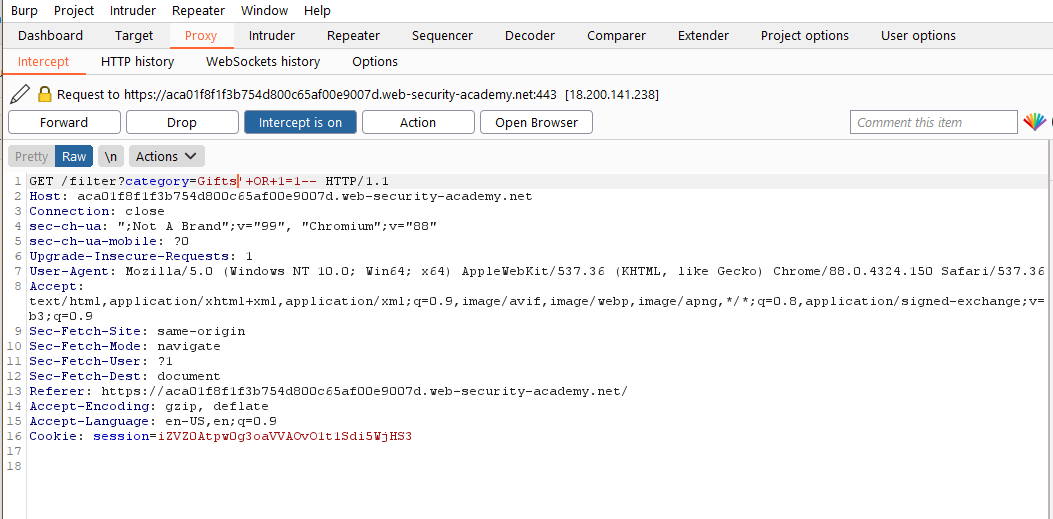
# Lab 3 - SQL Injection with Burp Suite Proxy

|  |
| --- |
| * This is due tonight. * Use the following naming convention: homework, underscore, last name, first initial, and extension (e.g., Lab\_SQLi\_ImG.docx). * Zoom in your screenshots, please. * Try to finish four tasks. Three are acceptable. |

## Tasks

### 1. Retrieving hidden data

* Take a screenshot of the content of injection that is displayed on the proxy.

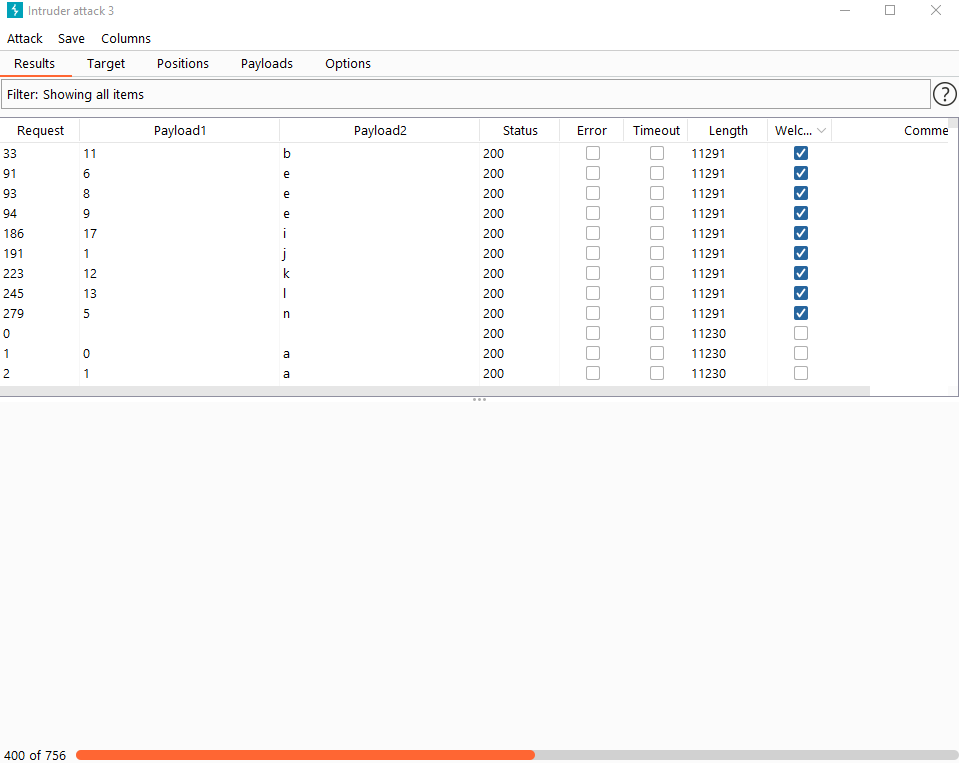


* Take a screenshot of the outcome.



### 2. Blind SQL injection

* Take a screenshot of the outcome.

Results: 

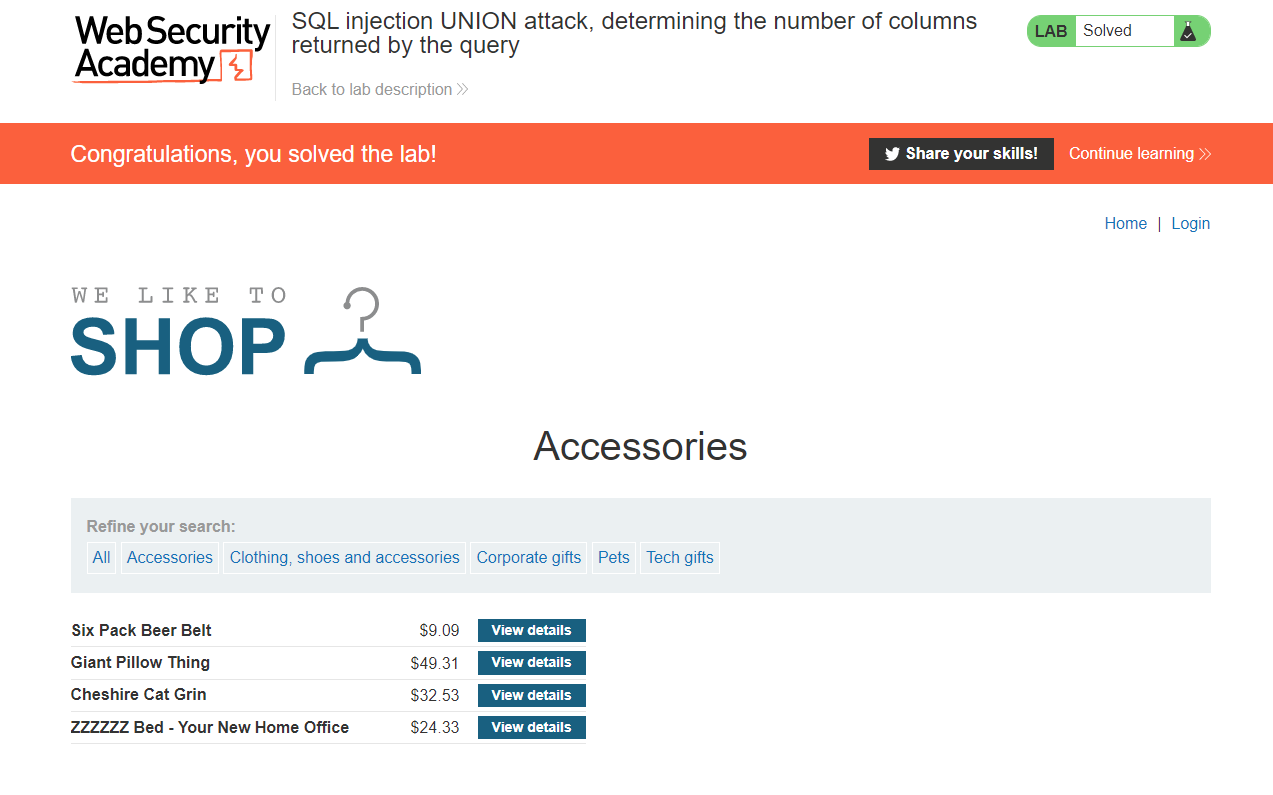
Username: Administrator

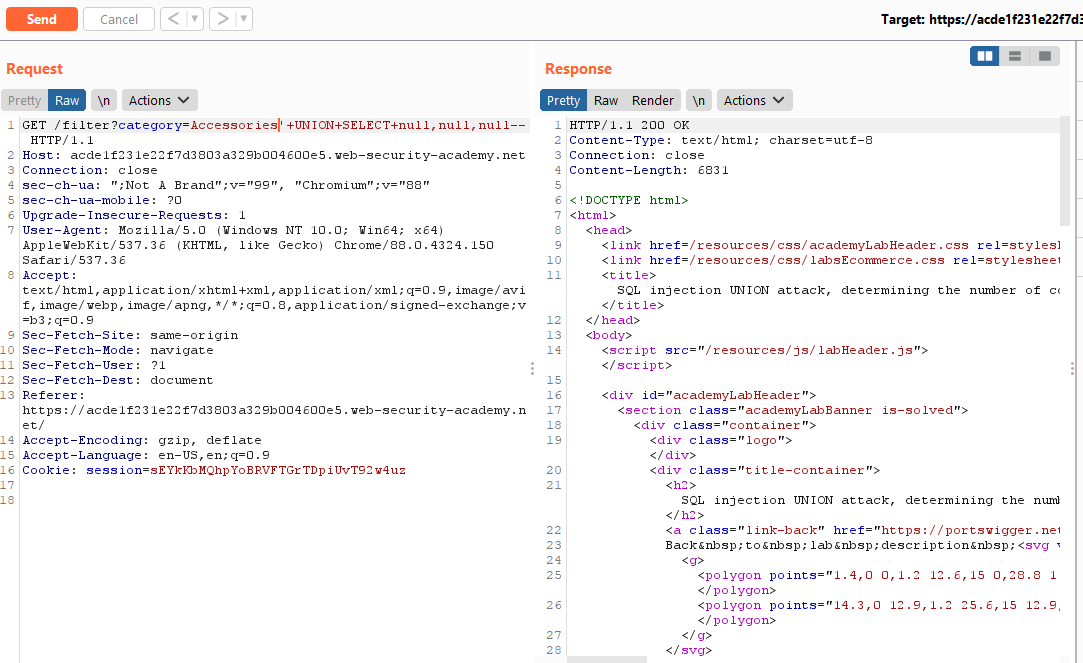
And Password was: takes forever to attack

### 3. SQL injection UNION attacks

### 3.1 Determining the number of columns required in an SQL injection UNION attack

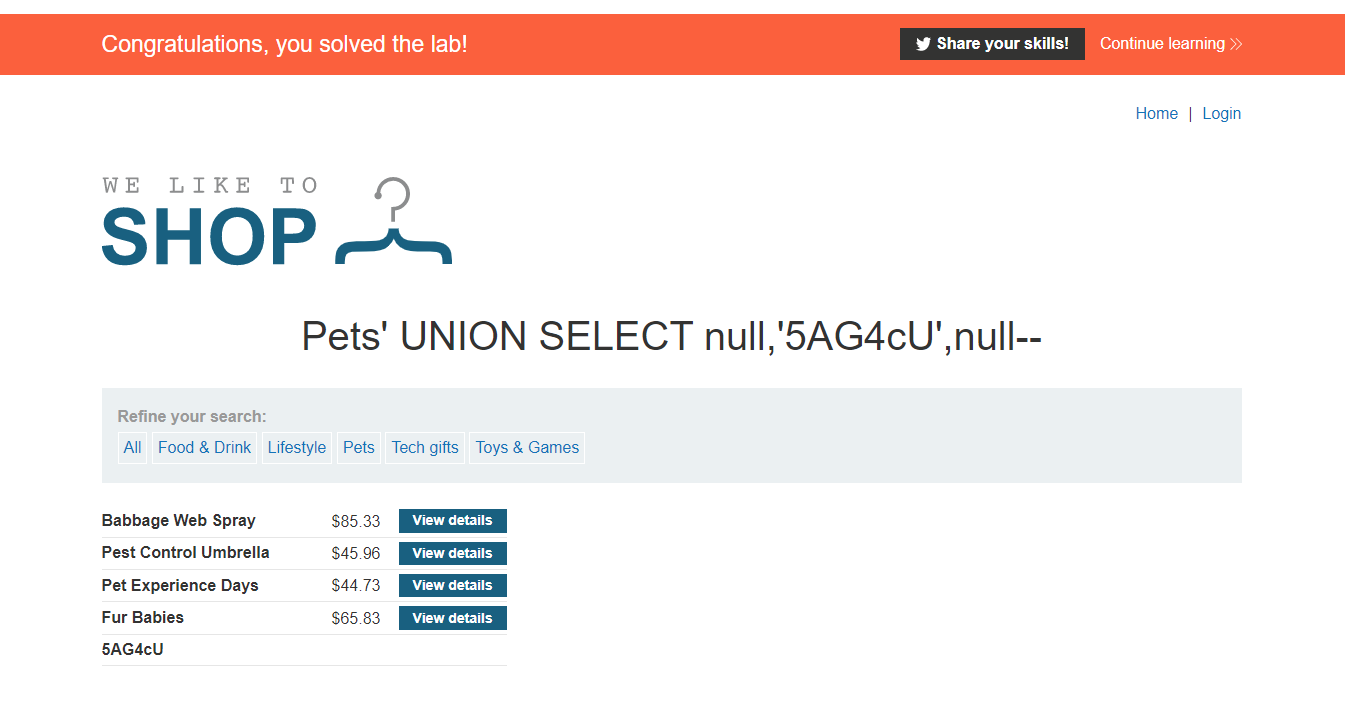
* Take a screenshot of the outcome.



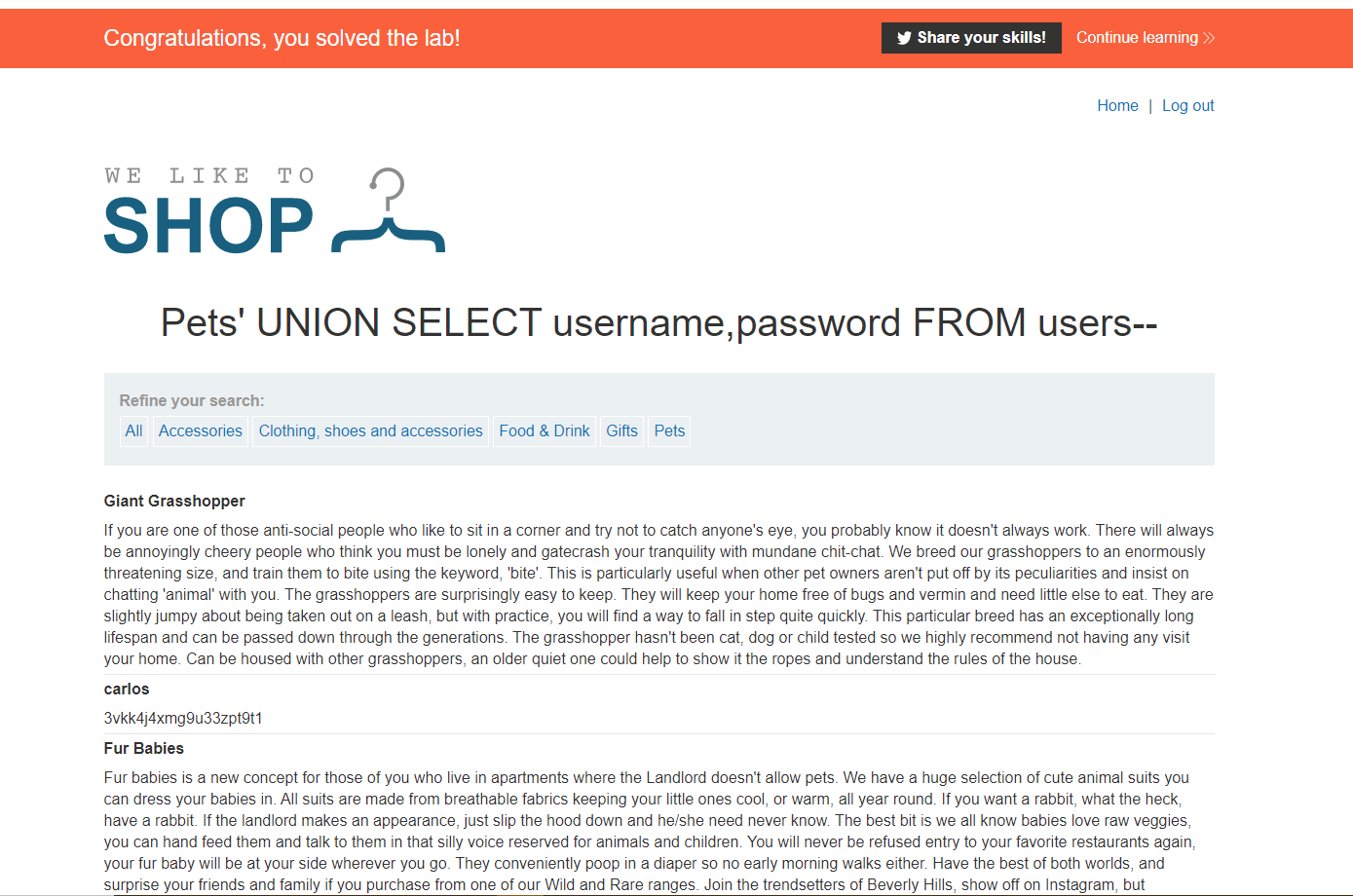


### 3.2 Finding columns with a useful data type in an SQL injection UNION attack

* Take a screenshot of the outcome.



### 3.3 Using an SQL injection UNION attack to retrieve interesting data

* Take a screenshot of the outcome.
* 

### 3.4 Retrieving multiple values within a single column

* Take a screenshot of the outcome.

