

# SQL Injection

Refer for theory: <https://portswigger.net/web-security/sql-injection>

## Vulnerability Labs (Apprentice):

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

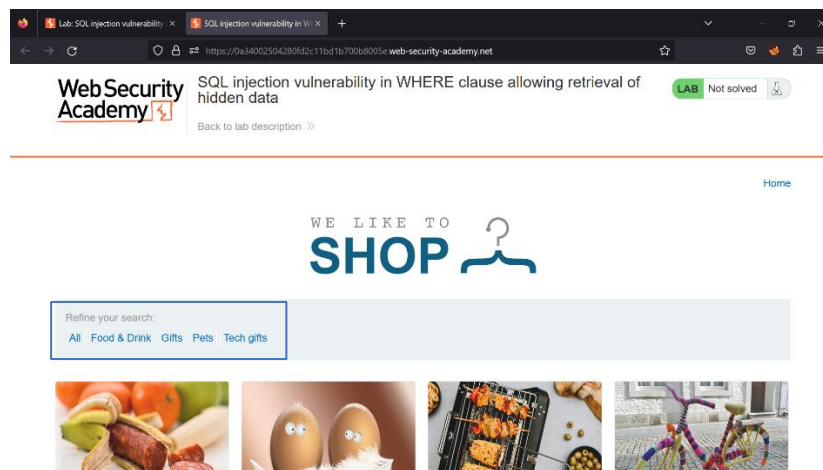
This lab contains a SQL injection vulnerability in the product category filter. When the user selects a category, the application carries out a SQL query like the following:

```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```

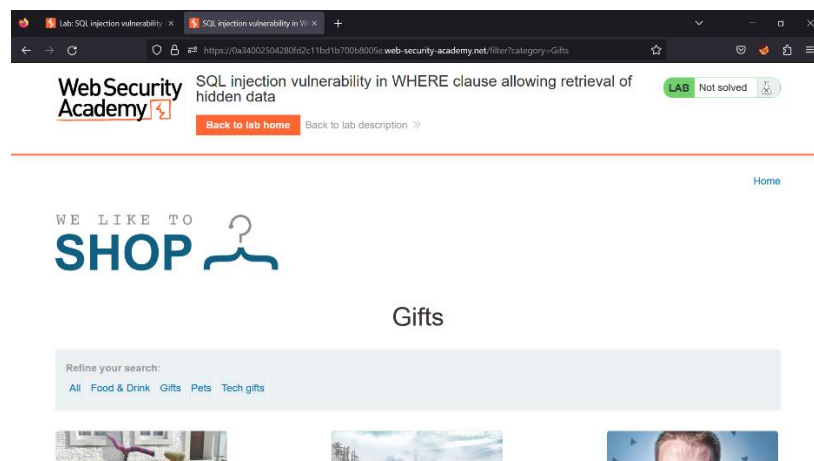
To solve the lab, perform a SQL injection attack that causes the application to display details of all products in any category, both released and unreleased.

Solution: -

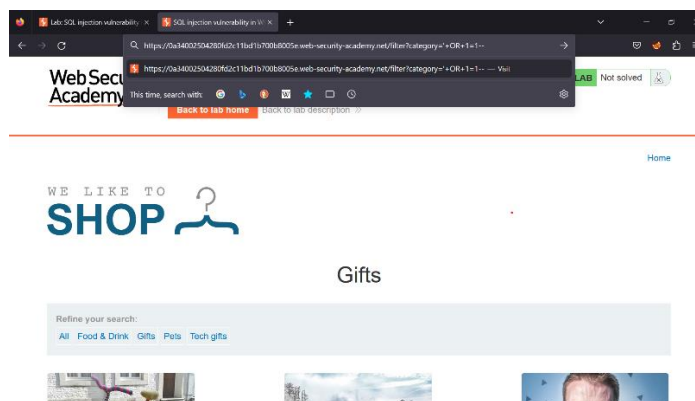
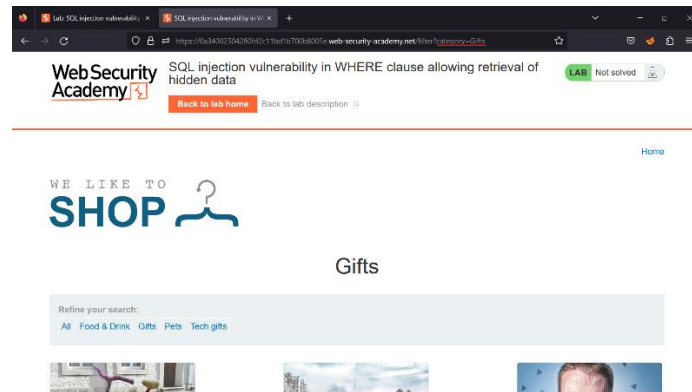
- Click on any of the categories shown in the blue box in the below picture.



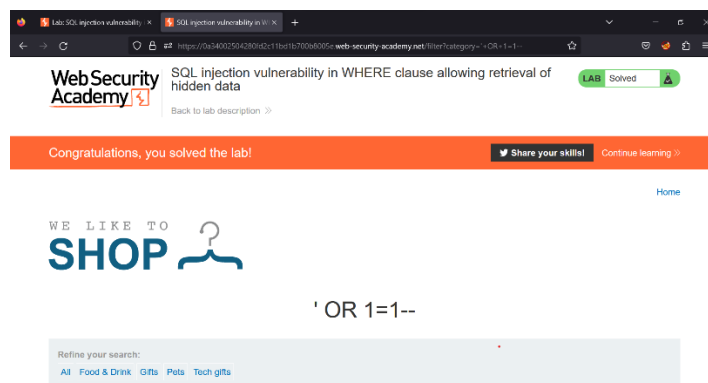
- Once a category is selected, the site will be redirected.



- Notice the url of the page. The category is already assigned to some value. Change it to '+OR+1=1--



- Once submitted, the sql injection attack will be successful.



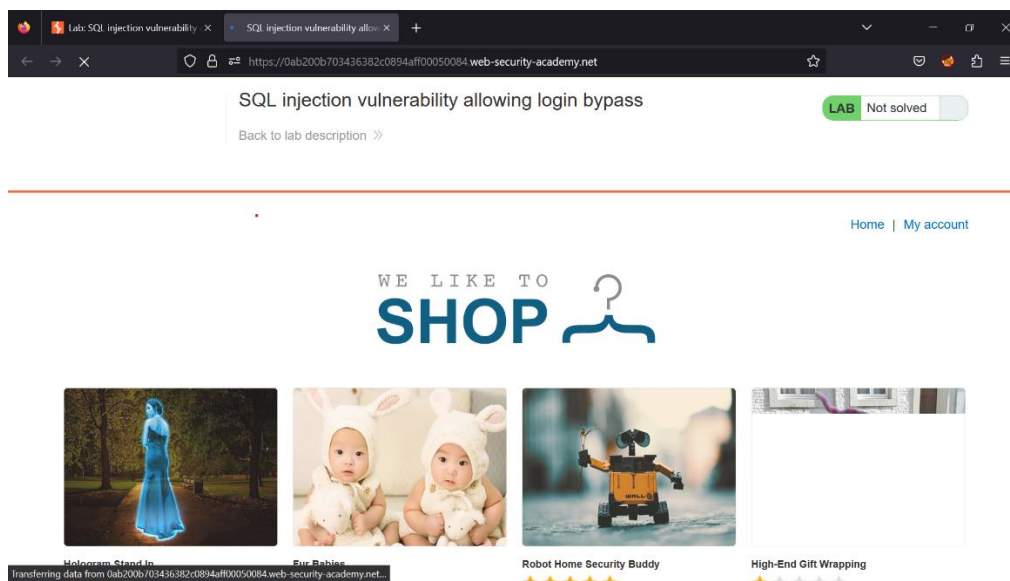
## 2. SQL injection vulnerability allowing login bypass

This lab contains a SQL injection vulnerability in the login function.

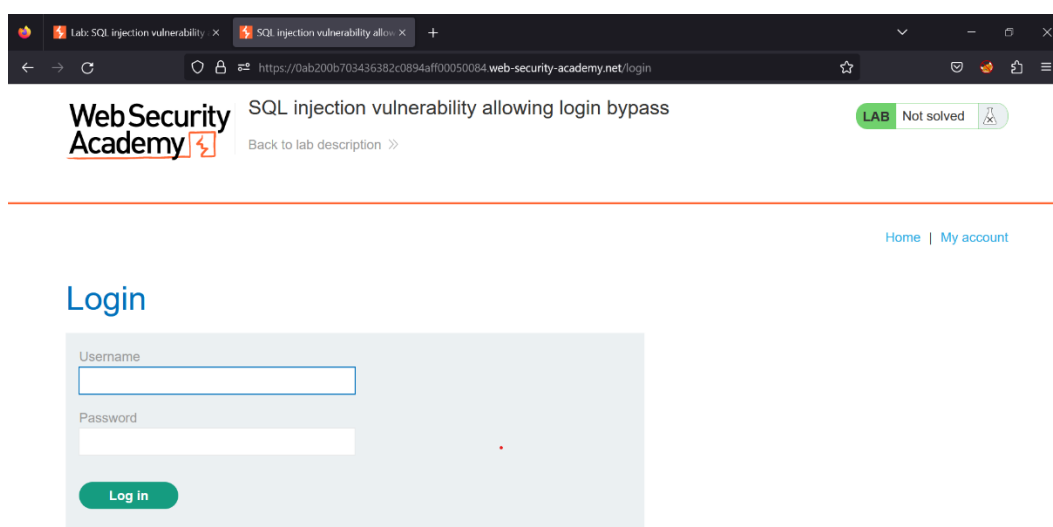
To solve the lab, perform a SQL injection attack that logs in to the application as the administrator user.

Solution:

- Once the lab is accessed, a shopping site is opened.

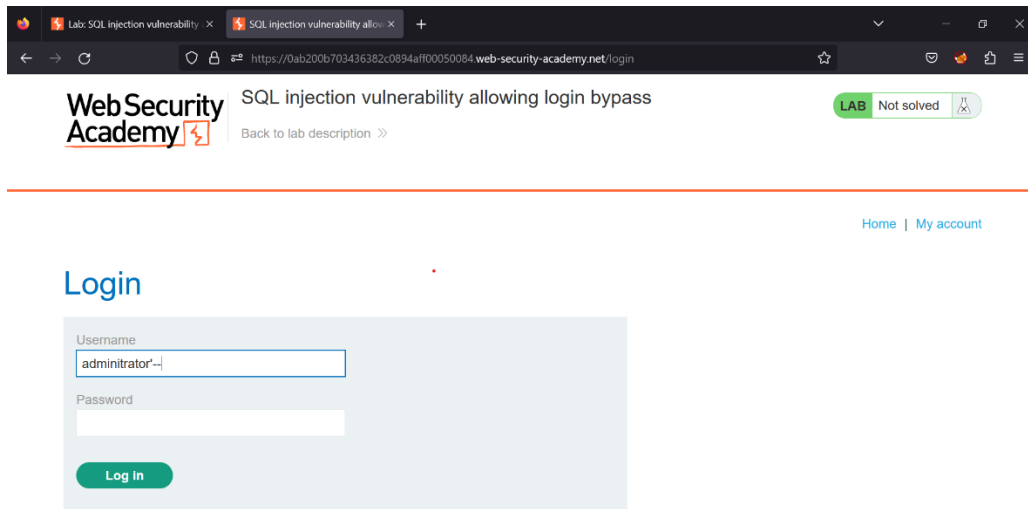


- Click on the My account option which is on the top right corner of the site. We need to access the administrator's account without authentication.



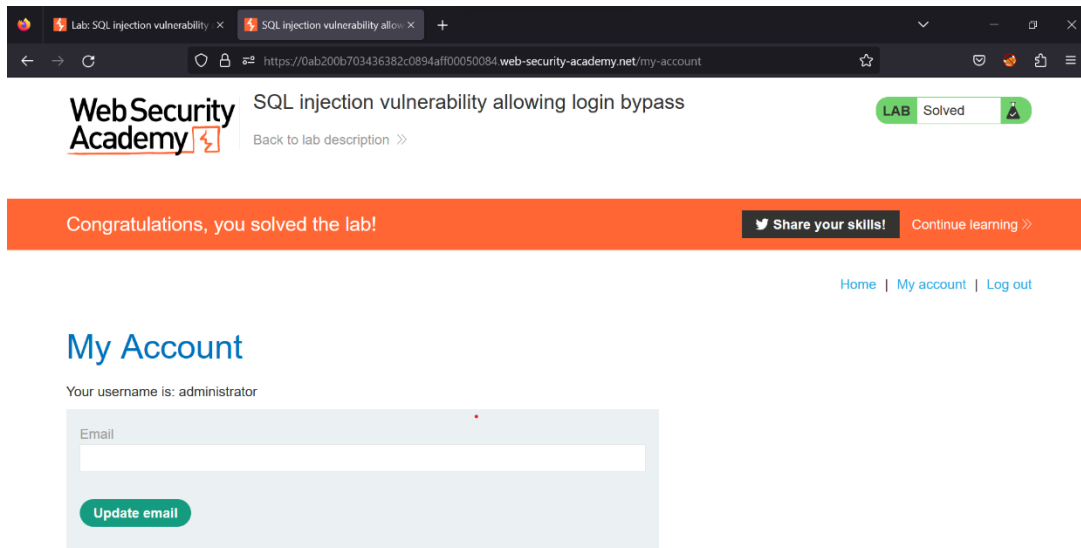
- A login form will be visible. We know that the username is administrator. Since we do not know the password we are going to do perform sql injection to bypass the password field.
- Enter the following code snippet into the username text field :

**administrator'--**



The screenshot shows a web browser window with two tabs: 'Lab: SQL injection vulnerability' and 'SQL injection vulnerability allow...'. The address bar shows the URL 'https://0ab200b703436382c0894aff00050084.web-security-academy.net/login'. The page title is 'SQL injection vulnerability allowing login bypass'. The Web Security Academy logo is on the left, and a 'LAB Not solved' badge is on the right. Below the header, there are links for 'Home' and 'My account'. The main heading is 'Login'. The login form has a 'Username' field containing 'administrator'--' and an empty 'Password' field. A green 'Log In' button is at the bottom of the form.

- The above code will comment out the rest of the sql query by using comments (--).
- Enter a random password as it's a requirement and hit log in. Your lab will be solved.



The screenshot shows the 'My Account' page of the Web Security Academy. The address bar shows the URL 'https://0ab200b703436382c0894aff00050084.web-security-academy.net/my-account'. The page title is 'SQL injection vulnerability allowing login bypass'. The Web Security Academy logo is on the left, and a 'LAB Solved' badge is on the right. Below the header, there are links for 'Home', 'My account', and 'Log out'. A green banner at the top says 'Congratulations, you solved the lab!' with a 'Share your skills!' button and a 'Continue learning >>' link. The main heading is 'My Account'. Below the heading, it says 'Your username is: administrator'. The 'Email' field is empty. A green 'Update email' button is at the bottom of the form.