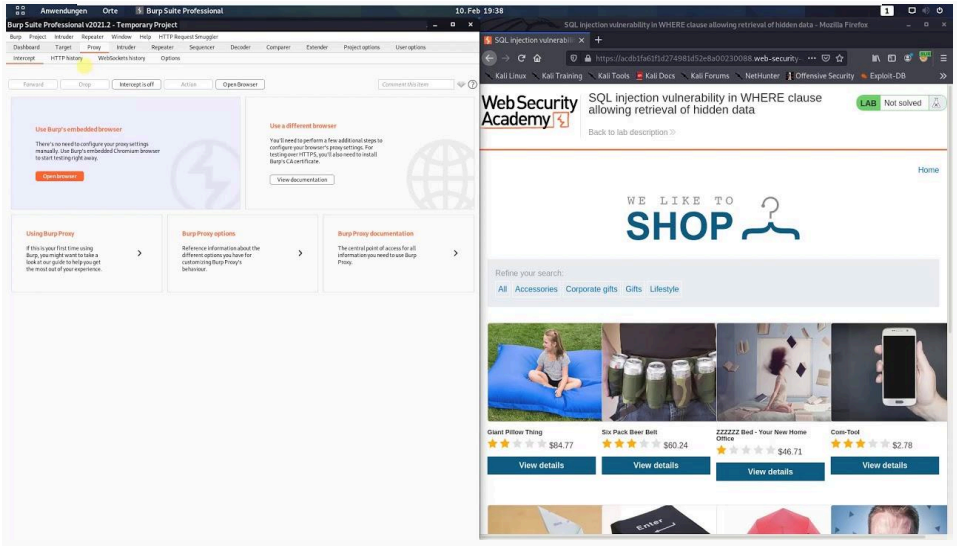
01 Lab: SQL Injection Vulnerability in WHERE clause allowing retrieval of hidden data

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 this lab we have to to display one or more unreleased products. and it is given that SQLi vulnearability is in the product category filter.

So first choose Lifestyle category and observe the url. We can see that Category filter has been added as category=Gifts :



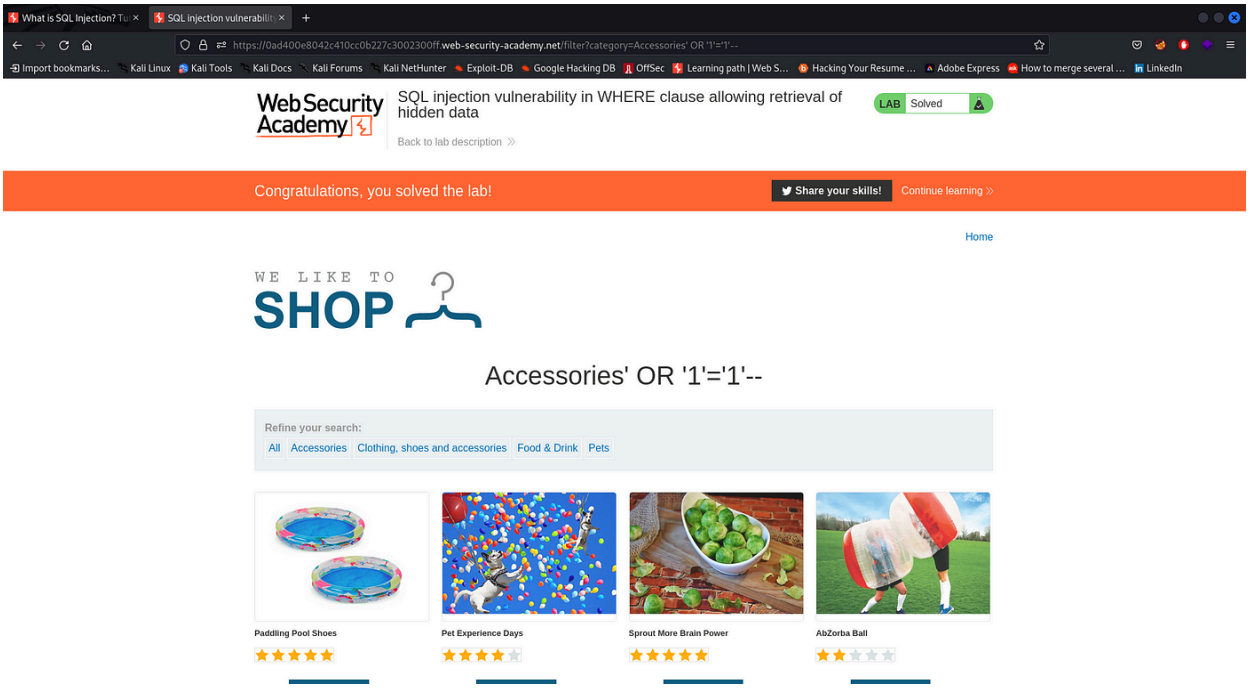
So the query will be following for the given parameters: `SELECT * FROM products WHERE category = 'Gifts' AND released = 1`

But instead of Lifestyle we will add some SQL characters to comment out rest of the query and retrieve the hidden data.

We can do that by just adding category=’ OR 1=1--’

Query will be following : `SELECT * FROM products WHERE category = '' OR 1=1`

Here, the condition “1=1” always evaluates to true and ‘--’ will comment out the rest of the SQL query allowing us to retrieve all the released and unreleased products, regardless of their category.



Your lab should be solved at this point.