




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

To Access the Lab, Click Access the Lab Button.

Web Security Academy > SQL injection > Lab



Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

APPRENTICE  **LAB**  Solved 


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 one or more unreleased products.

The Below is the Homepage of the Lab1, In the Description of the Lab1 it is mentioned that the Lab1 contains SQL Injection Vulnerability in the product Category Filter, Try Accessing the Product Category Filter.


WebSecurity Academy SQL injection vulnerability in WHERE clause allowing retrieval of hidden data **LAB** Not solved 

[Back to lab home](#) [Back to lab description](#)


WE LIKE TO **SHOP** 

Tech gifts


Refine your search:
[All](#) [Accessories](#) [Food & Drink](#) [Lifestyle](#) [Tech gifts](#)



All-in-One Typewriter
★★★★★
\$48.65 [View details](#)

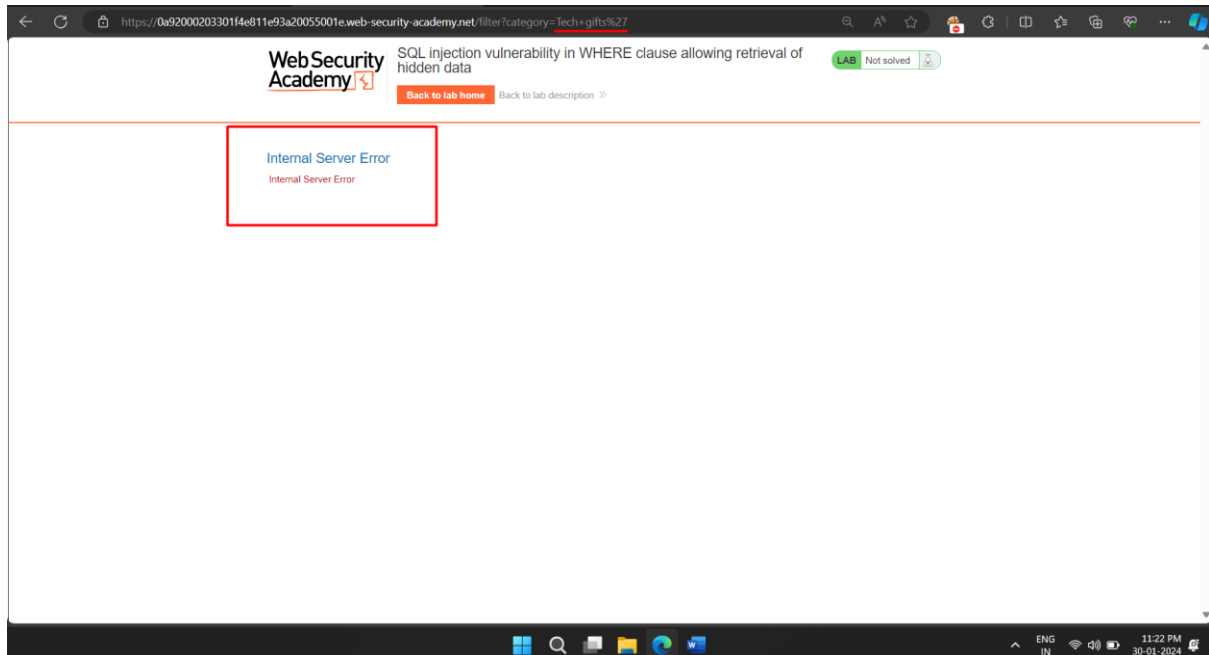


Eye Projectors
★★★★★
\$73.62 [View details](#)



Picture Box
★★★★★
\$85.05 [View details](#)

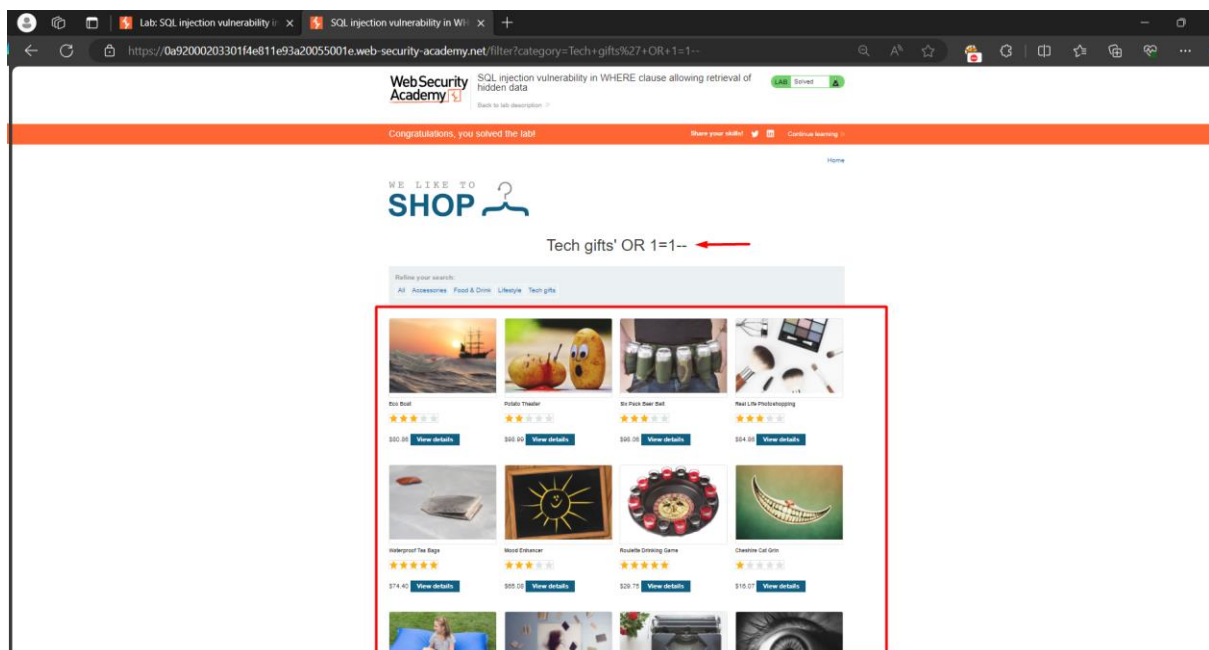
While trying to access the Tech gifts category, Released Items are only 3 and our goal is to perform SQLi Vulnerability and display hidden data i.e. Display all unreleased items also, we can see the URL Which sends the SQL Query to the Database to Retrieve data. Let's try to perform the SQLi Vulnerability in the URL.



In the URL while adding the single quote (') at the end gives us Internal Server Error, we can Confirm that this website is Vulnerable to SQLi Attacks.

<https://0a92000203301f4e811e93a20055001e.web-security-academy.net/filter?category=Tech+gifts%27+OR+1=1-->

Here %27 Denotes Single Quote ('), The Response for the Above SQL Query is,



Initially there are 3 items in the Tech gifts Category, After Performing SQLi Attack we can able to see all the items in the Particular Category.