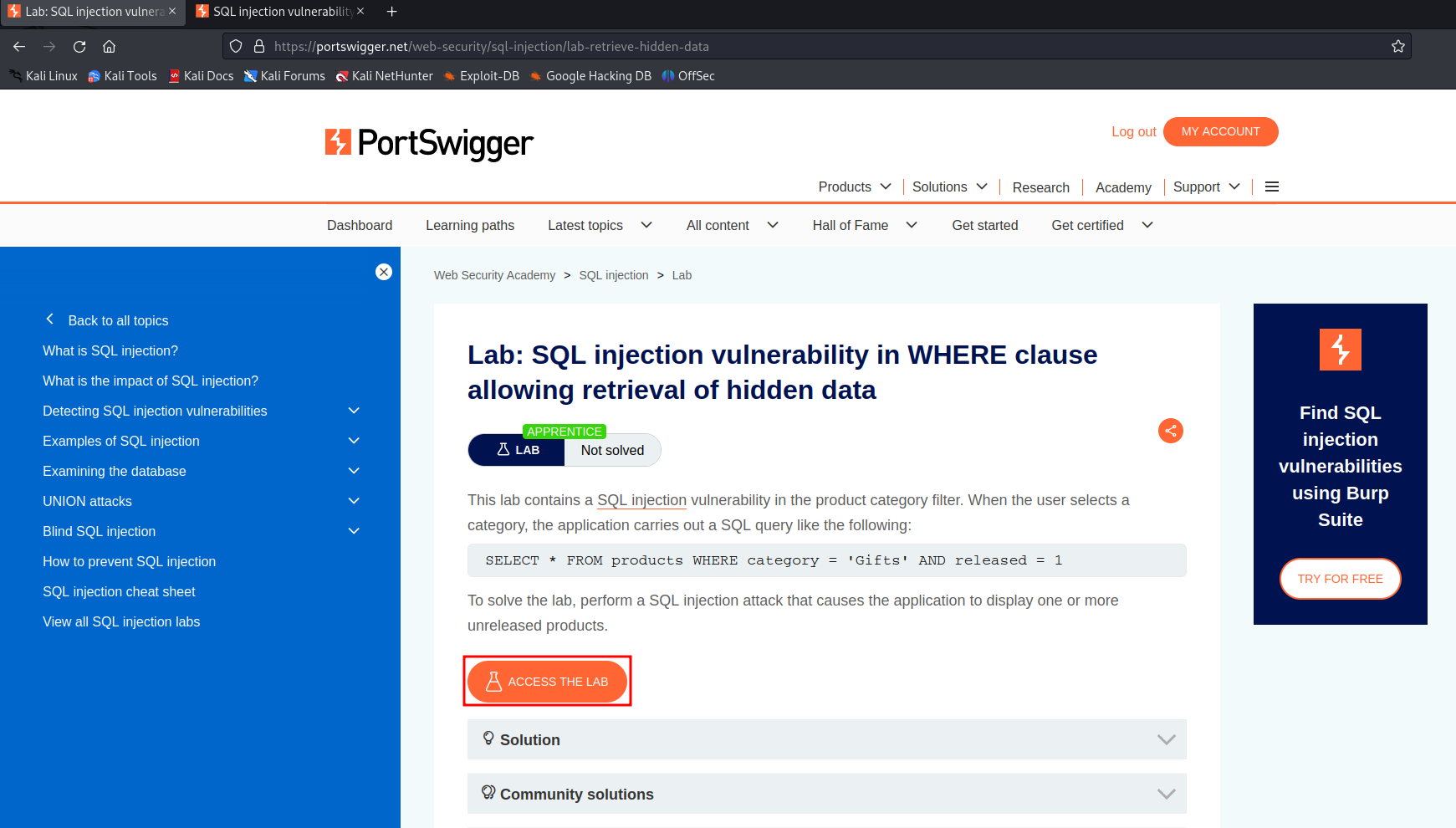
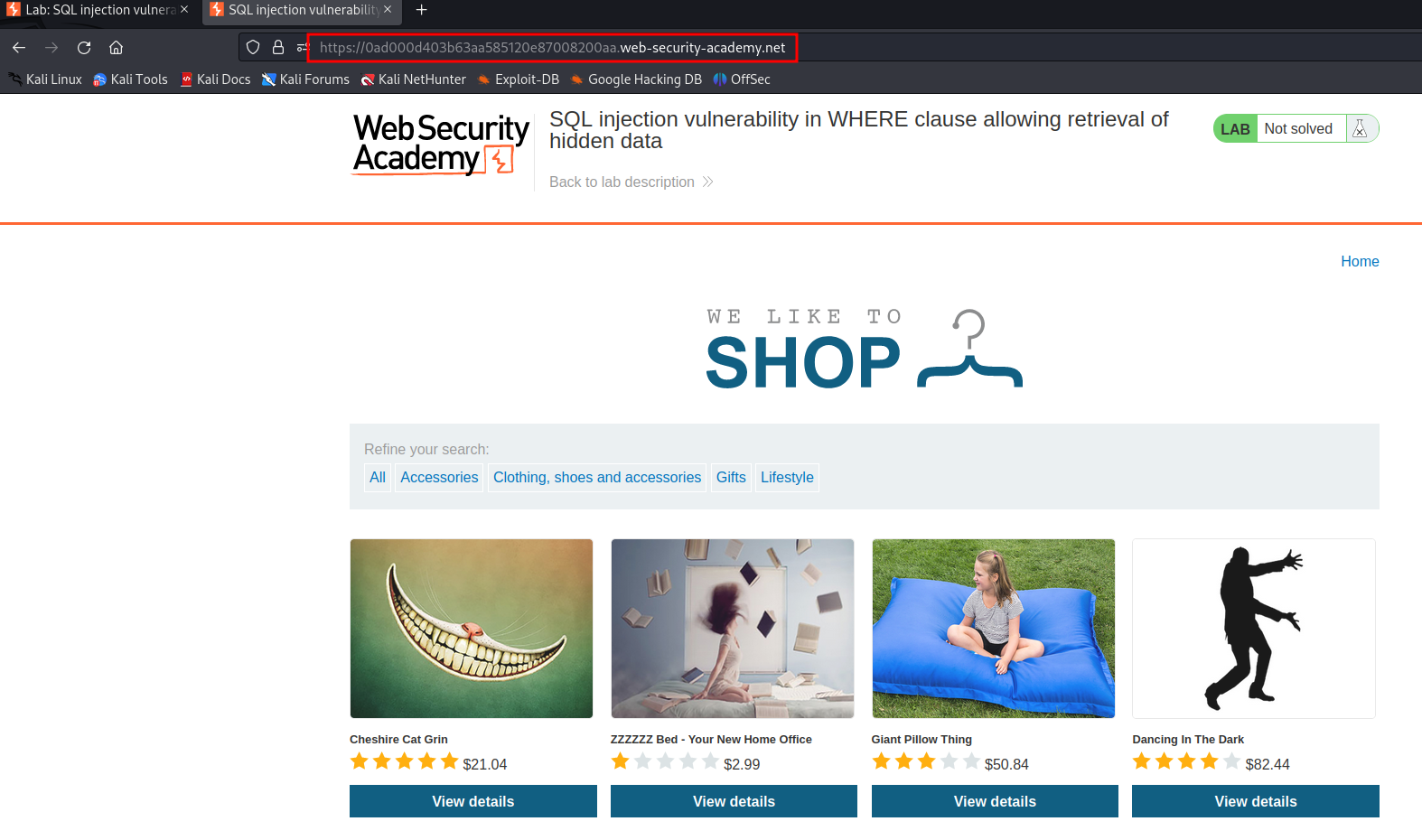
To access the lab –

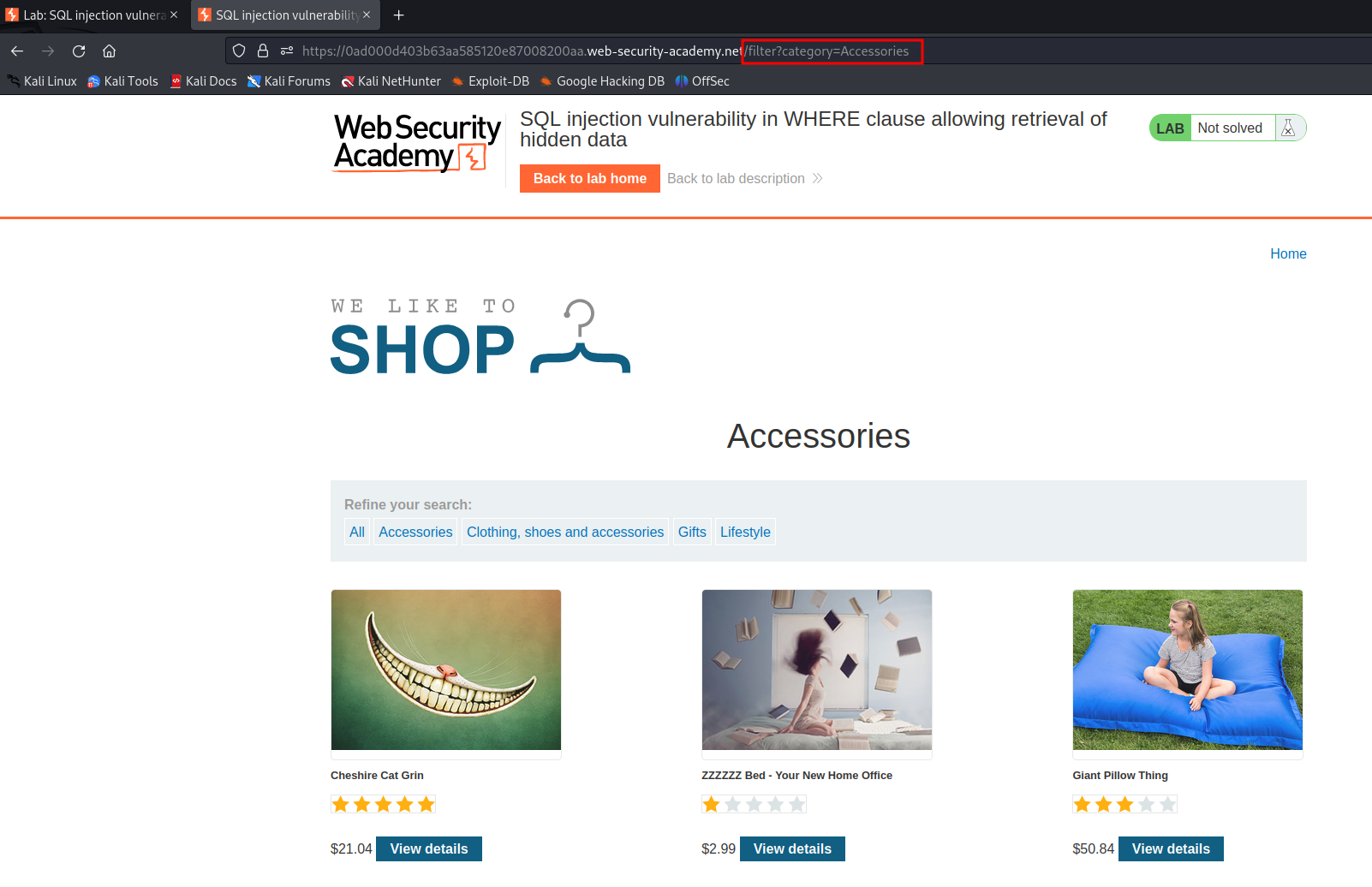


Click on the access lab.



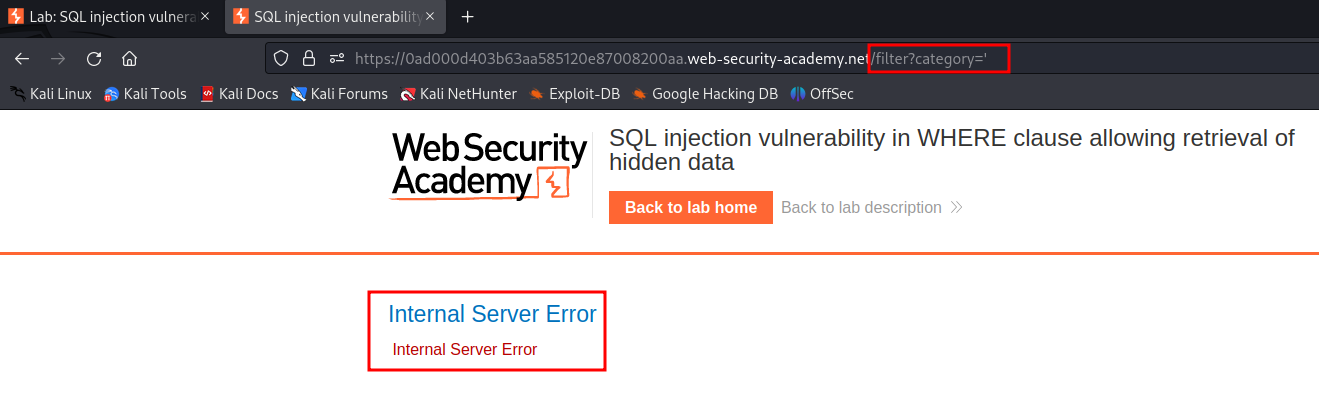
Here, the attacker can see some sort of a shopping store with the highlighted URL.

If the attacker click on accessories,



The attacker gets the URL request of “filter?category=Accessories”. This just filters the items in the accessories.

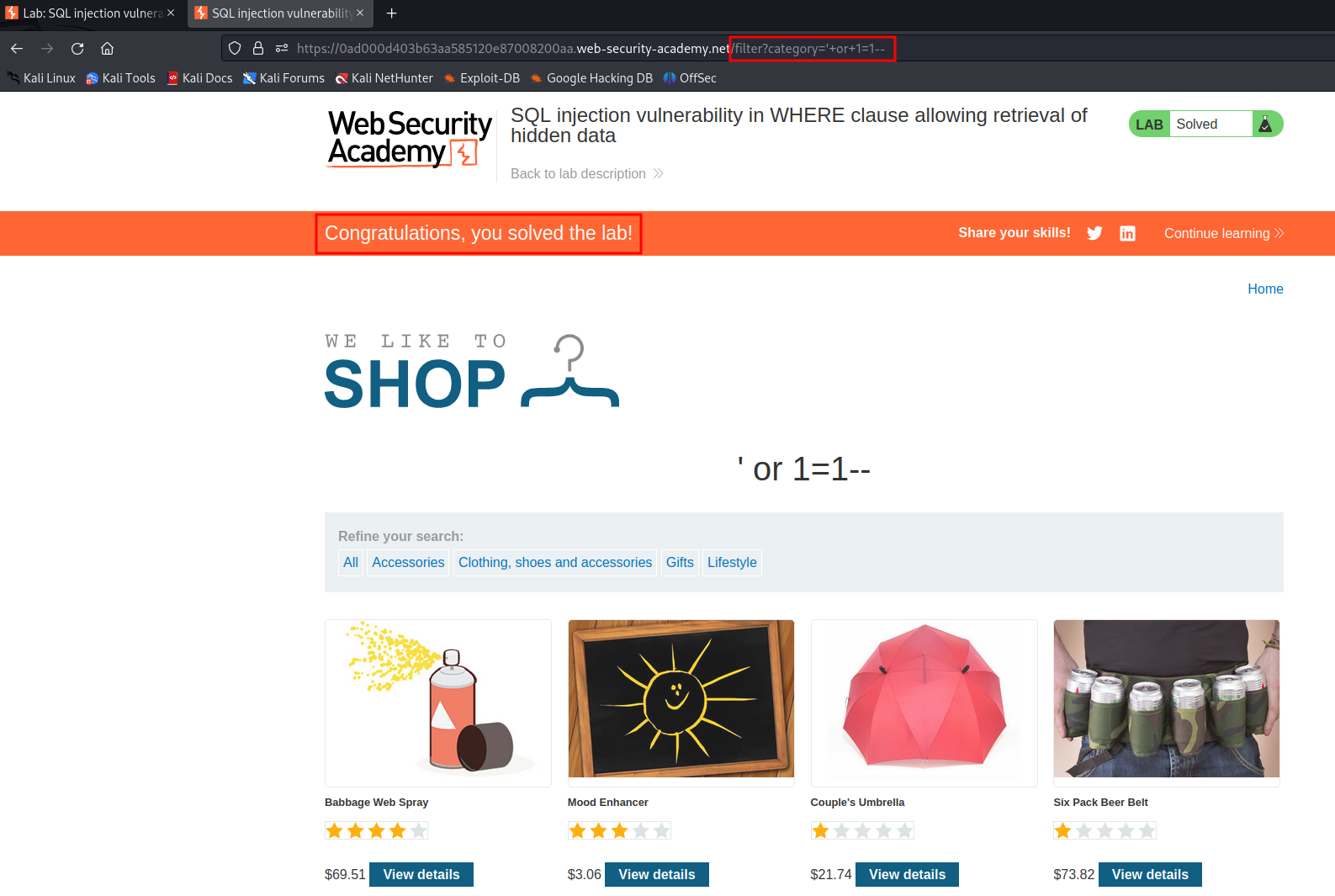
To check if this page is vulnerable to SQLi, the attacker will send a unidentified string which is a **‘** (single quote). This will cause the internal server to throw an error.



We can confirm that this website is vulnerable to SQLi.

To extract all the data from this website – we will just add a conditional statement – **'+or+1=1—**

This statement basically tells the system to always evaluate the truth (1=1) and – says that everything that comes after the 1=1 is a comment.



Here, we can see that all the data from this website has been leaked. This is because the 1=1 always holds true.