

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

[Home](#)

WE LIKE TO
SHOP



Gifts'or 1=1--

Refine your search:

[All](#) [Accessories](#) [Corporate gifts](#) [Food & Drink](#) [Gifts](#)

The screenshot shows the Burp Suite interface with a request and response captured. The request is a GET request to the URL `/filter?category=Gifts'or 1=1--`. The response is an HTTP 200 OK status with a content type of `text/html; charset=utf-8`. The response body contains HTML code, including a `<title>` tag with the text `SQL injection vulnerability in WHERE clause allowing retrieval of hidden data`. The request is highlighted with a red circle, and the response is highlighted with a blue circle.