**BÁO CÁO BÀI THỰC HÀNH SỐ 3**

**KIỂM THỬ LỖ HỔNG SQL INJECTION**

***Họ và tên: Phạm Lê Nhật Quang***

***Mssv: 0850080037***

***Link Youtube:*** *https://youtu.be/m3ZzdoeF0dI*

***Yêu cầu kết quả thực hành:***

**Câu 1*(3.5 điểm)***

Kiểm thử lỗ hổng SQL Injection trên trang web http://www.vietfarmsfsf.com/?php=product\_detail&id=260

* Xác định các tham số đầu vào và cách thức chúng được gửi tới server **(0.25 điểm)**

Trên trang web http://www.vietfarmsfsf.com/?php=product\_detail&id=260, ta có các tham số đầu vào là php, id. Chúng được gửi tới server thông qua phương thức GET trong URL.

* Phân tích và phán đoán kiểu truy vấn **(0.25 điểm)**

Dựa vào URL trên, không thể xác định chính xác kiểu truy vấn được sử dụng trong trang web. Tuy nhiên, từ tiếng "product\_detail" trong URL, có thể suy đoán rằng trang web có thể có chức năng hiển thị chi tiết sản phẩm dựa trên một id nhất định.

* Phân tích và phán đoán vị trí của các giá trị tham số đầu vào được sử dụng trong câu truy vấn **(0.5 điểm)**

Trong URL trên, giá trị của tham số id là 260 và nằm trong vị trí cuối cùng của URL. Nó được sử dụng để định danh cho sản phẩm cần hiển thị chi tiết.

* Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào **(2.5 điểm)**

Dựa trên URL trên, không thể đánh giá được mức độ ảnh hưởng của lỗ hổng SQL Injection một cách chính xác. Điều này yêu cầu kiểm tra chi tiết các hàm xử lý yêu cầu trên phía server. Tuy nhiên, nếu giá trị của tham số id không được kiểm tra và xử lý đúng đắn, lỗ hổng SQL Injection có thể xảy ra. Tin tặc có thể sử dụng các kỹ thuật SQL Injection để thay đổi hoặc thực thi các câu truy vấn SQL không mong muốn, gây ảnh hưởng đến cơ sở dữ liệu và bảo mật hệ thống.

*Lưu ý:*

* *Nói rõ mục đích sử dụng các giá trị kiểm thử*
* *Giải thích rõ các phán đoán và suy luận từ kết quả khi sử dụng mỗi giá trị kiểm thử*

**Câu 2 *(3.5 điểm)***

Kiểm thử lỗ hổng SQL Injection trên trang web http://...........................[[1]](#endnote-1)

* Xác định các tham số đầu vào và cách thức chúng được gửi tới server **(0.25 điểm)**

Trên trang web http://funagamex.vn/lienhe.php?id\_menu=9, ta có một tham số đầu vào là id\_menu. Tham số này được gửi tới server thông qua phương thức GET trong URL.

* Phân tích và phán đoán kiểu truy vấn, phân tích và phán đoán vị trí của các tham số đầu vào được sử dụng trong câu truy vấn **(0.25 điểm)**

Dựa vào URL trên, không thể xác định chính xác kiểu truy vấn được sử dụng trong trang web. Tuy nhiên, từ tên tệp tin lienhe.php trong URL, có thể suy đoán rằng trang web này có chức năng liên hệ và id\_menu có thể được sử dụng để xác định danh mục liên hệ cụ thể.

Trong URL trên, giá trị của tham số id\_menu là 9 và nằm ở cuối URL. Có thể suy ra rằng giá trị này được sử dụng để xác định danh mục liên hệ.

* Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào **(3 điểm)**

Dựa vào thông tin hiện có, không thể đánh giá được mức độ ảnh hưởng của lỗ hổng bảo mật cụ thể trên trang web này. Để xác định mức độ ảnh hưởng của lỗ hổng, cần phân tích xem liệu giá trị của tham số id\_menu có được kiểm tra và xử lý đúng đắn trong ứng dụng hay không. Nếu không có kiểm tra và xử lý đúng đắn, lỗ hổng bảo mật như SQL Injection có thể xảy ra, gây nguy hiểm đến bảo mật và hiệu suất của ứng dụng web.

*Lưu ý:*

* *Nói rõ mục đích sử dụng các giá trị kiểm thử*
* *Giải thích rõ các phán đoán và suy luận từ kết quả khi sử dụng mỗi giá trị kiểm thử*

**Câu 3 *(3 điểm)***

Kiểm thử lỗ hổng SQL Injection trên trang web http://.........

* Xác định các tham số đầu vào và cách thức chúng được gửi tới server **(0.25 điểm)**

Trên trang web http://tapiocafeedfood.com/?php=product\_detail&id=295, ta có các tham số đầu vào là php, id. Chúng được gửi tới server thông qua phương thức GET trong URL.

* Phân tích và phán đoán kiểu truy vấn, vị trí của các tham số đầu vào được sử dụng trong câu truy vấn **(0.25 điểm)**

Dựa vào URL trên, không thể xác định chính xác kiểu truy vấn được sử dụng trong trang web. Tuy nhiên, từ tiếng "product\_detail" trong URL, có thể suy đoán rằng trang web có chức năng hiển thị chi tiết sản phẩm dựa trên một id nhất định.

Trong URL trên, giá trị của tham số id là 295 và nằm trong vị trí cuối cùng của URL. Nó được sử dụng để định danh cho sản phẩm cần hiển thị chi tiết.

* Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào **(2.5 điểm)**

Dựa trên URL trên, không thể đánh giá được mức độ ảnh hưởng của lỗ hổng SQL Injection một cách chính xác. Điều này yêu cầu kiểm tra chi tiết các hàm xử lý yêu cầu trên phía server. Tuy nhiên, nếu giá trị của tham số id không được kiểm tra và xử lý đúng đắn, lỗ hổng SQL Injection có thể xảy ra. Tin tặc có thể sử dụng các kỹ thuật SQL Injection để thay đổi hoặc thực thi các câu truy vấn SQL không mong muốn, gây ảnh hưởng đến cơ sở dữ liệu và bảo mật hệ thống.

*Lưu ý:*

* *Nói rõ mục đích sử dụng các giá trị kiểm thử*
* *Giải thích rõ các phán đoán và suy luận từ kết quả khi sử dụng mỗi giá trị kiểm thử*

1. [↑](#endnote-ref-1)