**BÁO CÁO BÀI THỰC HÀNH SỐ 8**

**KIỂM THỬ LỖ HỔNG SQL INJECTION**

Họ và tên: Lưu Thy Thy

Yêu cầu kết quả thực hành:

Báo cáo kết quả thực hành có tên theo định dạng HoTenSV\_MSSV\_Lab08.docx

Câu 1(3.5 điểm)

Kiểm thử lỗ hổng SQL Injection trên trang web <http://webvul.bkcs.vn/register.php>

* Xác định các tham số đầu vào và cách thức chúng được gửi tới server (0.25 điểm)
* Phương thức gửi dữ liệu: POST
* Tham số đầu vào:
  + username
  + password
  + email
* Dạng dữ liệu gửi: application/x-www-form-urlencoded
* Phân tích và phán đoán kiểu truy vấn (0.25 điểm)
* INSERT INTO users (username, password, email) VALUES ('$username', '$password', '$email');
* 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)
* Các tham số username, password, và email được chèn trực tiếp vào câu lệnh SQL. Nếu không có biện pháp bảo vệ như sử dụng prepared statements hoặc escaping, thì các giá trị này có thể được khai thác để chèn mã SQL độc hại
* Vị trí khả thi:
  + Username/Email: Thường xuất hiện trong mệnh đề WHERE của truy vấn SELECT hoặc VALUES của INSERT.
  + Password: Thường nằm trong VALUES của INSERT.
* Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào (2.5 điểm)
* Tham số username:
  + Mục đích: Kiểm tra khả năng bypass kiểm tra trùng lặp username.
  + Phân tích: Nếu ứng dụng không xử lý đúng, có thể cho phép đăng ký nhiều tài khoản với cùng username hoặc truy cập trái phép.
* Tham số email:
  + Mục đích: Kiểm tra khả năng chèn mã SQL qua trường email.
  + Phân tích: Có thể dẫn đến việc chèn dữ liệu không hợp lệ hoặc truy vấn sai lệch
* Tham số password:
  + Mục đích: Kiểm tra khả năng bypass xác thực mật khẩu.
  + Phân tích: Nếu ứng dụng sử dụng mật khẩu trong truy vấn SQL mà không xử lý đúng, có thể cho phép truy cập trái phép.

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://webvul.bkcs.vn/login.php>

* Xác định các tham số đầu vào và cách thức chúng được gửi tới server (0.25 điểm)
* Phương thức gửi dữ liệu: POST
* Tham số đầu vào:
  + username
  + password
* Dạng dữ liệu gửi: application/x-www-form-urlencoded
* 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)
* SELECT \* FROM users WHERE username = '$username' AND password = '$password';
* Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào (3 điểm)
* Tham số username:
  + Mục đích: Kiểm tra khả năng bypass xác thực bằng cách luôn đúng điều kiện.
  + Phân tích: Nếu ứng dụng không xử lý đúng, có thể cho phép truy cập trái phép vào hệ thống.
* Tham số password:
  + Mục đích: Tương tự như trên, kiểm tra khả năng bypass xác thực.
  + Phân tích: Có thể dẫn đến việc truy cập trái phép nếu không có biện pháp bảo vệ.

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://webvul.bkcs.vn/index.php>

* Xác định các tham số đầu vào và cách thức chúng được gửi tới server (0.25 điểm)
* Phương thức gửi dữ liệu: GET
* Tham số đầu vào: Có thể là id, page, search, hoặc các tham số khác tùy thuộc vào chức năng của trang.
* Dạng dữ liệu gửi: Tham số được truyền qua URL, ví dụ: http://webvul.bkcs.vn/index.php?id=1
* 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)
* SELECT \* FROM products WHERE id = '$id';
* Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào (2.5 điểm)
* Tham số id:
  + Mục đích:
    - Kiểm tra khả năng truy vấn trả về tất cả các bản ghi
    - Kiểm tra khả năng thực thi lệnh SQL bổ sung.
    - Kiểm tra khả năng lấy dữ liệu từ bảng khác.
  + Phân tích:
    - Nếu ứng dụng không xử lý đúng, có thể cho phép truy cập và hiển thị toàn bộ dữ liệu trong bảng.
    - Nếu ứng dụng không xử lý đúng, có thể dẫn đến việc xóa bảng users trong cơ sở dữ liệu.
    - Nếu ứng dụng không xử lý đúng, có thể cho phép kẻ tấn công truy cập thông tin nhạy cảm như tên người dùng và mật khẩu.

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