**BÁO CÁO BÀI THỰC HÀNH SỐ 8**

**KIỂM THỬ LỖ HỔNG SQL INJECTION**

***Họ và tên: Nguyễn Minh Nhật Đan***

***MSSV: 1050080046***

***Lớp :10\_ĐH\_CNPM1***

**Câu 1*(3.5 điểm)***

Kiểm thử lỗ hổng SQL Injection trên trang web <http://testasp.vulnweb.com/Register.asp?RetURL=%2FDefault%2Easp%3F>

Xác định các tham số đầu vào và cách thức chúng được gửi tới server **:**

Các tham số đầu vào và cách thức chúng được gửi tới server:

Tham số đầu vào trong http request:Các tham số được người dùng gửi qua phương thức POST:

+frmRegister

+tfUname

+tfRname

+tfEmail

+tfUpass

-Cách thức gửi tới server: Nhập thông tin vào các ô trong html và request đến server để tiến hành đăng kí thôn qua phương thức http post

Phân tích và phán đoán kiểu truy vấn**:**

Dựa trên các tham số và phương thức cách chúng được gửi tới server thì kiểu truy vấn là :  
+Create : các giá trị tham số sẽ được tạo thành các bảng lưu trữ dữ liệu người dùng

+Insert into: mỗi giá trị được tạo ra sẽ được đưa vào các bảng tương ứng với người dùng

Phân tích và phán đoán vị trí của các giá trị tham số đầu vào được sử dụng trong câu truy vấn :

Dựa trên thông tin trang đăng kí của người dùng có thể đưa ra phân tích sau :

+Mỗi người dùng sau khi nhập thông tin và điền đầy đủ thông tin trang sẽ trải qua một giai đoạn kế tiếp là kiểm tra độ chính xác của dữ liệu :tức là các giá trị có thể bị ảnh hưởng bởi các quy tắc của hệ thống hay không

+Và dựa vào các mức độ giá trị ảnh hưởng có thể thử nghiệm như sau:

A screenshot of a computer

AI-generated content may be incorrect.

Giá trị kiểm thử :

+UserName :1231231$%^^ :Chuỗi tên không hợp lệ, chứa nhiều kí tự đặc biệt

+RealName:231312^^$%%&: Chuỗi tên chứa nhiều kí tự đặc biệt

+Email:nahtgmail.com :sai định dạng email

+Password:123456 :mật khẩu đơn giản

Kết quả khi trả về:

A screenshot of a computer

AI-generated content may be incorrect.  
Đăng kí thành công :

Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào Mức độ ảnh hưởng của lỗ hỏng trên mỗi giá trị đầu vào:

+frmRegister: Không gây ảnh hưởng nghiêm trọng vì phụ thuộc chủ yếu vào các giá trị còn lại

+tfUname :Gây ảnh hưởng nghiêm trọng vì không kiểm tra giá trị hợp lệ

+tfRname:Không gây ảnh hưởng vì không có đủ khả năng để tác động đến khả năng đăng nhập

+tfEmail: Gây ảnh hưởng nghiêm trọng vì không xác thực chính xác giá trị đầu vào của email, không có cơ sở để có khả năng lấy được mật khẩu khi không đăng nhập thành công

+tfUpass: Gây ảnh hưởng nghiêm trọng vì không kiểm tra chất lượng của nguồn mật khẩu hay có ràng buộc ,dễ dàng bị brute force

**Câu 2 *(3.5 điểm):***

Kiểm thử lỗ hổng SQL Injection trên trang web : <http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F>

Xác định các tham số đầu vào và cách thức chúng được gửi tới server **:**

Các tham số đầu vào:  
+tfUName

+tfUPass

+Login

Cách thức chúng được gửi tới server: thông qua phương thức http:postDựa trên các thông số đàu vào và phương thức mà chúng được gửi tới server thì có thể phán đoán kiểu truy vấn là :  
+WHERE: Được sử dụng cho tham số tfUPass với điều kiện tại giá trị đầu vào à tfUName

+SELECT:Được sử dụng cho tham số đầu vào là tfUName với điều kiện giá trị Login được request đến Server qua phương thức POST

Kiểm tra các giá trị đầu vào cụ thể để xác định lỗ hổng SQL Injection và đánh giá mức độ ảnh hưởng dựa trên khả năng truy xuất, sửa đổi, hoặc xóa dữ liệu.

**Phương pháp kiểm thử:**

Sử dụng các kỹ thuật SQL Injection phổ biến để kiểm tra các tham số tfUName, tfUPass. Các giá trị kiểm thử bao gồm:

1. **Gây lỗi cú pháp** (Error-based): Để phát hiện lỗi cơ sở dữ liệu.
2. **Boolean-based**: Để kiểm tra phản hồi dựa trên điều kiện đúng/sai.
3. **UNION-based**: Để trích xuất dữ liệu từ bảng khác.
4. **Time-based**: Để phát hiện Blind SQL Injection.
5. **Bypass đăng nhập**: Để kiểm tra khả năng vượt qua xác thực.

**Câu 3 *(3 điểm)***

Kiểm thử lỗ hổng SQL Injection trên trang web [http://testasp.vulnweb.com/](http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F)

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

Các tham số đầu vào:  


Dựa trên tham số đầu vào thì có thể phán đoán kiểu truy vấn là :

Select: thứ tự của tham số dựa trên id của bài viết

Mức độ ảnh hưởng của hệ thống: lộ id của điểm dữ liệu dễ bị truy vấn thông tin của bài viết