|  |
| --- |
| **HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  **KHOA CÔNG NGHỆ THÔNG TIN 2**  🙞🙞🙞🕮🙜🙜🙜    **BÁO CÁO CHUYÊN ĐỀ KHOA HỌC**  **CẤP HỌC VIỆN**  **SQL INJECTION - CÁC PHƯƠNG PHÁP KHẮC PHỤC**  **Báo cáo viên: ThS. Lưu Nguyễn Kỳ Thư**  **Năm học: 2020-2021**  *Thành phố Hồ Chí Minh, tháng 10/2021* |

**Phần 1: Giới thiệu mở đầu**

Mục tiêu của chuyên đề:

1. Tìm hiểu cách tấn công vào cơ sở dữ liệu qua SQL Injection và đưa ra các phương pháp khắc phục.
2. Nội dung:   
   - SQL Injection   
   - Các phương pháp khắc phục
3. Kết quả:

* Báo cáo nội dung nghiên cứu

- Chương trình demo minh họa

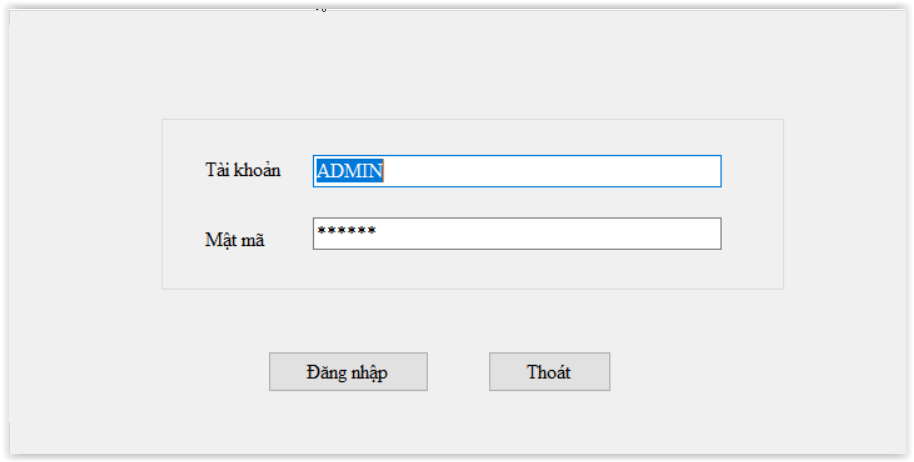
**Phần 2: Nội dung chuyên đề khoa học**

1. **SQL INJECTION:** **SQL Injection** là một kỹ thuật lợi dụng những lỗ hổng về câu truy vấn của các ứng dụng bằng cách chèn thêm một đoạn SQL để làm sai lệch đi câu truy vấn ban đầu, từ đó có thể khai thác dữ liệu từ database. **SQL injection** có thể cho phép những kẻ tấn công thực hiện các thao tác như một người quản trị web trên cơ sở dữ liệu của ứng dụng.

Ví dụ, trong form đăng nhập, người dùng nhập dữ liệu, hoặc trong trường tìm kiếm người dùng nhập văn bản tìm kiếm. Tất cả các dữ liệu được chỉ định này đều đưa vào cơ sở dữ liệu. Thay vì nhập dữ liệu đúng, kẻ tấn công lợi dụng lỗ hổng để insert và thực thi các câu lệnh SQL bất hợp pháp để lấy dữ liệu của người dùng…

1. **SỰ NGUY HIỂM CỦA SQL INJECTION**
   * Người dùng có thể đăng nhập vào ứng dụng với tư cách người dùng khác, ngay cả với tư cách quản trị viên. Từ đó, có thể thay đổi dữ liệu của cơ sở dữ liệu
   * Người dùng có thể xem thông tin cá nhân thuộc về những người dùng khác, ví dụ chi tiết hồ sơ của người dùng khác, chi tiết giao dịch của họ
   * Người dùng có thể kiểm soát máy chủ cơ sở dữ liệu và thực thi lệnh theo ý muốn.

Ví dụ: ta có một Form đăng nhập như sau:



Và đoạn code xử lý của ta khi user click nút lệnh Đăng nhập

public static int KetNoi()

{

if (Program.conn != null && Program.conn.State == ConnectionState.Open)

Program.conn.Close();

try

{

Program.connstr = "Data Source=" + Program.servername + ";Initial Catalog=" +

Program.database + ";User ID=" +

Program.mlogin + ";password=" + Program.password;

Program.conn.ConnectionString = Program.connstr;

Program.conn.Open();

string strlenh = "SELECT NAME FROM [USER] WHERE USERNAME ='" + username +

"' AND PASSWORD='" + pass\_username + "'";

myReader = ExecSqlDataReader(strlenh);

if (myReader == null)

{

MessageBox.Show("Lỗi kết nối cơ sở dữ liệu.\nBạn xem lại user name và password.", "", MessageBoxButtons.OK);

return 0;

}

return 1;

}

catch (Exception e)

{

MessageBox.Show("Lỗi kết nối cơ sở dữ liệu.\nBạn xem lại user name và password.\n " + e.Message, "", MessageBoxButtons.OK);

return 0;

}

}

Lúc này, nếu như người dùng không nhập dữ liệu đăng nhập bình thường nữa mà nhập vào Text Tài khoản chuỗi sau : **ABC’ OR 1=1 ; --**

thì lúc này câu truy vấn của ta khi đưa vào hàm KetNoi sẽ được diễn dịch như sau:

SELECT NAME FROM [USER] WHERE **USERNAME='ABC' OR 1=1 --‘ AND password = ‘’**

Trong trường hợp này, rõ ràng điều kiện truy vấn của câu lệnh trên luôn luôn đúng, và như vậy chương trình sẽ xem như dữ liệu đăng nhập là hợp lý, và người dùng có thể sử dụng chương trình của ta.

Trong trường hợp khác, user nhập vào :

Tài khoản: ABC**‘ or 1=1**

Mật mã: abc’; drop table chi\_tiet\_phieu\_nhap

Lúc này, câu truy vấn của ta khi đưa vào hàm KetNoi sẽ được diễn dịch như sau:

SELECT NAME FROM [USER] WHERE **USERNAME=‘ABC’ or 1=1 and password=’abc’; drop table chi\_tiet\_phieu\_nhap**

Do Sql Server xử lý gói lệnh, mỗi lệnh cách nhau bởi ‘;’ nên lúc này form Đăng nhập sẽ xóa các mẫu tin trong table chi tiết phiếu nhập

Các phần dễ bị tấn công bao gồm:

* Form đăng nhập
* Form tìm kiếm
* Form nhận xét

## **III. CÁCH GIẢM THIỂU VÀ PHÒNG NGỪA SQL INJECTION**

Sql Injection xuất hiện trên form đăng nhập là do ta có table USER để lưu danh sách người dùng sẽ sử dụng phần mềm. Để tránh lỗi Sql Injection khi đăng nhập, ta nên ràng buộc thật kỹ dữ liệu người dùng nhập vào. Chẳng hạn như ta bắt lỗi nhập liệu không cho nhập dấu nháy đơn, chuỗi ‘ OR ‘, chuỗi --.. Hoặc ta tận dụng cơ chế quản lý tài khoản đăng nhập có sẵn của Hệ quản trị cơ sở dữ liệu để lưu tài khoản của người dùng.

Sql Injection không chỉ xuất hiện trong form đăng nhập, mà còn có thể xuất hiện trong Form Tìm kiếm dữ liệu. Do đó, ta nên ràng buộc thật kỹ dữ liệu người dùng nhập vào là hay hơn cả.

**Phần 3: Kết luận, đề xuất**

* Chuyên đề đã đề cập 1 lỗi thường gặp khi thực hiện thao tác nhập dữ liệu trên các form nhập liệu. Từ đó, đưa ra hướng khắc phục thích hợp.

Đề xuất (khuyến nghị) hướng vận dụng kết quả của báo cáo chuyên đề: kết quả nghiên cứu có thể áp dụng trong việc đào tạo, giới thiệu cho sinh viên biết trong các môn học có liên quan đến Lập trình cơ sở dữ liệu, Lập trình Web