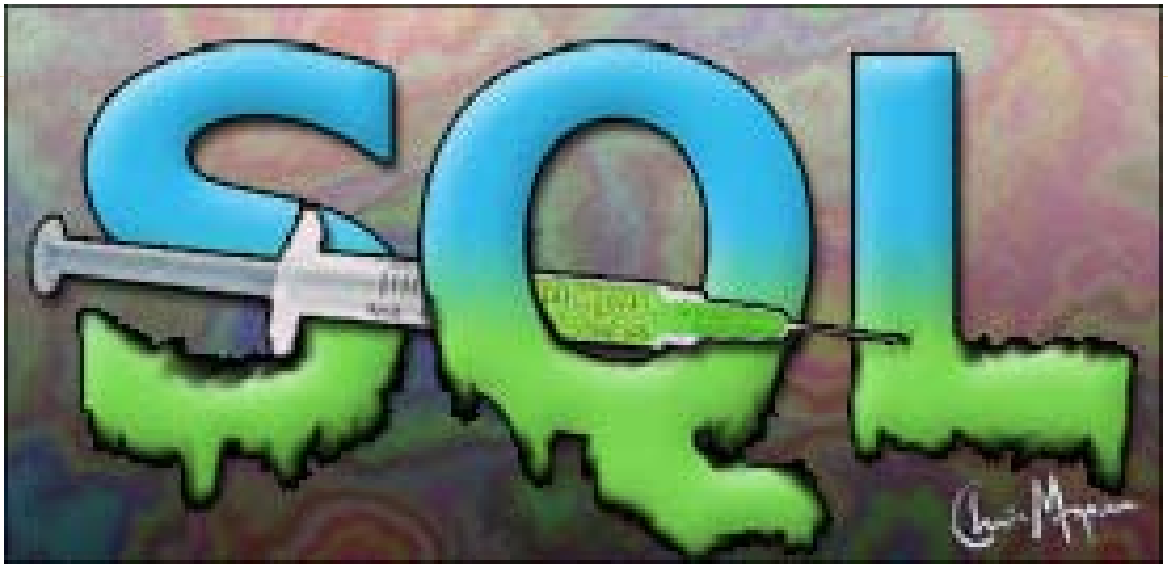
SQL Injection
và
Cách phòng tránh

Trần Quang Khải

Nội dung

1. Giới thiệu.
2. Các dạng tấn công thường gặp.
3. Cách phòng tránh.
4. SQL Injection trong Joomla.
5. Tài liệu tham khảo.
6. Hỏi đáp.

Giới thiệu



Giới thiệu (tt)

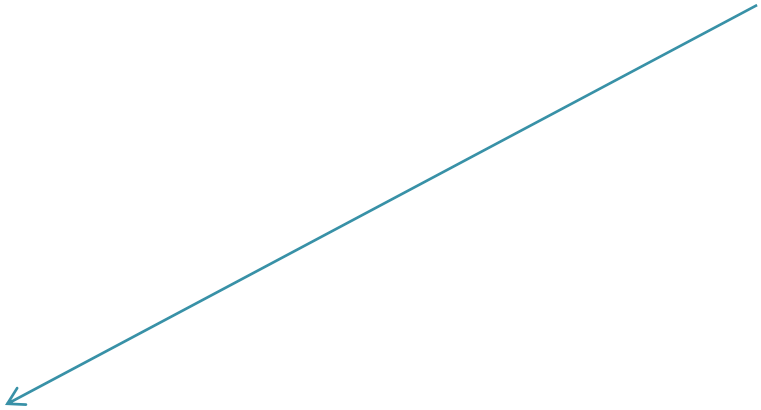
- SQL Injection là gì?
  - Lợi dụng các lỗ hổng liên quan đến câu truy vấn SQL **trong ứng dụng**.
    - Kiểm tra dữ liệu nhập.
    - Các thông báo lỗi.
    - Thói quen đặt tên bảng dữ liệu.
  - Tạo và thực thi câu lệnh SQL "bất hợp pháp".

Giới thiệu (tt)

- Ví dụ 1:

www.abc.com/product.aspx?**id=1**

```
SELECT  *
FROM  Product
WHERE  id = {id}
```



Giới thiệu (tt)

- Ví dụ 1(tt):

…/product.aspx?**id=1 UNION DROP TABLE Product--**

```
SELECT  *
FROM  Product
WHERE  id = 1 UNION DROP TABLE Product--
```

Giới thiệu (tt)

- Một số dạng tấn công thường gặp:
  - Vượt qua truy cập.
  - Lợi dụng câu lệnh SELECT.
  - Lợi dụng câu lệnh INSERT.
  - Lợi dụng STORED PROCEDURE.
- Các DBMS thường bị tấn công:
  - My SQL, SQL Server, Oracle, DB2, Sysbase.

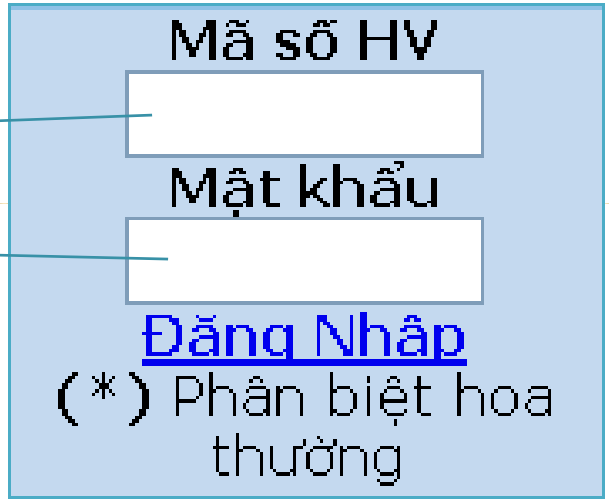
Giới thiệu (tt)

- Tác hại: kẻ tấn công có thể
  - biết được cấu trúc của database,
  - thêm, xóa, sửa dữ liệu của ứng dụng,
  - tệ hơn: có toàn quyền trên database của server.

Ở Việt Nam, đa số các vụ tấn công website gần đây đều theo kiểu SQL Injection.

Các dạng tấn công

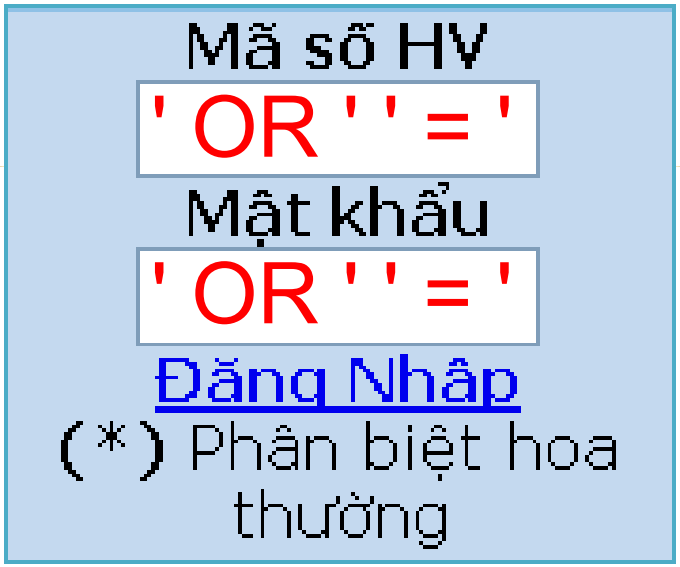
- Vượt qua truy cập:




```
String usrName;
String pw;
……
String sql;
sql = “SELECT *  FROM USERS” +
“WHERE username= '” + usrName +
“' AND password= '” + pw + “'”;
```

Các dạng tấn công (tt)

- Vượt qua truy cập (tt):




```
SELECT *
FROM USERS
WHERE username = '' OR '' = ''
    AND password = '' OR '' = '';
```

Các dạng tấn công (tt)

- Lợi dụng câu lệnh SELECT:
  - Kẻ tấn công có khả năng:
    - Hiểu và lợi dụng các thông báo lỗi.
    - Tìm các yếu điểm khởi đầu việc tấn công.
  - Ví dụ 2:

http://…/product.aspx?**id=1 OR 1=1**

SELECT * FROM Product
WHERE id=1 OR 1=1

Các dạng tấn công (tt)

- Lợi dụng câu lệnh SELECT (tt):
  - Cách xác định ứng dụng bị lỗi này:

```
' UNION SELECT ALL
SELECT OtherField
FROM OtherTable WHERE ' '='
```

Nếu báo lỗi không thấy “OtherTable”

→Câu SELECT sau UNION đã được thực thi.

Các dạng tấn công (tt)

- Lợi dụng câu lệnh SELECT (tt):
  - Liệt kê tên các bảng, cột trong SQL Server:

    Lợi dụng **sysobjects** và **syscolumns**

```
' UNION SELECT name
FROM sysobjects WHERE xtype = 'U'
```

Các dạng tấn công (tt)

- Lợi dụng câu lệnh INSERT:
  - Người dùng là thành viên, có thể:
    - Xem thông tin cá nhân.
    - Thay đổi thông tin cá nhân.
  - Ứng dụng không kiểm tra dữ liệu nhập khi người dùng thay đổi.

→"Tiêm" mã độc vào các field nhập.

Các dạng tấn công (tt)

- Lợi dụng câu lệnh INSERT (tt):
  - Ví dụ 3:

```
INSERT INTO Table1 VALUES('Value1',
  'Value2', 'Value3')
```

Nếu nhập Value1 là:

```
'+(SELECT TOP 1 Field1 FROM Table1)+'
```

Các dạng tấn công (tt)

- Lợi dụng câu lệnh INSERT (tt):
  - Ví dụ 3(tt):

```
INSERT INTO Table1
VALUES(' ' + (SELECT TOP 1 Field1
FROM Table1) + ' ', 'abc', 'def')
```

→Khi thực hiện lệnh xem thông tin, xem như đã yêu cầu thực hiện lệnh:

```
SELECT TOP 1 Field1 FROM Table1
```

Các dạng tấn công (tt)

- Lợi dụng Stored Procedure:
  - Nếu ứng dụng có quyền "**sa**".
  - Đoạn mã "tiêm":

```
' ; EXEC xp_cmdshell 'cmd.exe dir C: '
```

→Liệt kê thư mục ổ C: của server.

→Việc phá hoại tùy vào lệnh đằng sau **cmd.exe**.

Cách phòng tránh

- Kiểm soát chặt chẽ dữ liệu nhập:
  - Tất cả dữ liệu từ đối tượng **Request**:
    - Input do người dùng submit.
    - Các tham số từ URL.
    - Các tham số từ cookies.
  - Loại bỏ các ký tự, từ khóa đặc biệt:

    ' " / \ -- % # null select insert xp_
  - Giá trị số: cần kiểm tra, ép kiểu.
- Cẩn thận khi đặt tên bảng dữ liệu.

Cách phòng tránh (tt)

- Cấu hình an toàn cho DBMS:
  - Phân quyền:
    - Ứng dụng thông thường nên tránh các quyền DBO hay SA.
    - Quyền càng hạn chế, tác hại càng ít.
  - Kiểm soát các thông báo lỗi, nhằm tránh hiển thị:
    - Tên và phiên bản của DBMS.
    - Tên database.
    - Tên bảng và các cột trong bảng.

Cách phòng tránh (tt)

- Cấu hình an toàn cho DBMS (tt):
  - Xóa các stored procedure không dùng đến:
    - xp_cmdshell.
    - xp_startmail.
    - xp_sendmail.
    - sp_makewebtask.

SQL Injection trong Joomla

- Chiếm 70% số lỗ hổng trong các ứng dụng Joomla (năm 2009).
  - Nằm trong các thành phần mở rộng: component/module/template/plugin...
- Phòng tránh:
  - Vô hiệu hóa tài khoản admin mặc định, tạo tài khoản khác thay thế.
  - Cẩn thận với bảng "**jos_users**".

SQL Injection trong Joomla

- Phòng tránh (tt):
  - Tên bảng: không dùng tiền tố "**jos_**".
  - Cẩn thận khi cài đặt các thành phần mở rộng của một tổ chức thứ ba.
  - Hạn chế dùng lệnh JRequest::getVar()

    →Thay thế:

    JRequest::getString(), JRequest::getBool(), JRequest::getInt(), JRequest::getFloat() …

Tài liệu tham khảo

[1] Lê Đình Duy, ĐH KHTN Tp.HCM. Tấn công kiểu SQL Injection - Tác hại và phòng tránh.

[2] Wikipedia, URL: http://vi.wikipedia.org/wiki/SQL_injection

[3] SQL Injection và cách phòng tránh trong Joomla, URL: http://nsviet.com.vn/forum/showthread.php?p=253 http://vinaora.com/joomla/bao-mat-website-joomla/134-chong-tan-cong-sql-injection.html

[4] SQL Injection và cách phòng tránh trong ASP.NET, URL: http://dot.net.vn/Desktop.aspx/Articles/ADONET-Programming-Articles/Tan_cong_kieu_SQL_Injection_va_cac_phong_chong_trong_ASPNET/

Tài liệu tham khảo (tt)

[5] SQL Injection Attacks by Example, URL: http://unixwiz.net/techtips/sql-injection.html

[6] Chris Anley, NGSSoftware Ltd (2002). Advanced SQL Injection, URL: http://www.ngssoftware.com/papers/advanced_sql_injection.pdf http://www.ngssoftware.com/papers/more_advanced_sql_injection.pdf

Cảm ơn

- Hỏi đáp.

Phụ lục:

Truyện vui với SQL Injection

Name:

Robert');DROP TABLE Students;--