**Bài 4: Security Testing – Injection**

**Web Application – Injection**

Kỹ thuật Injection bao gồm injecting một truy vấn SQL. Thực sự injection/injecting là một từ chuyên môn, miễn cưỡng dịch ra tiếng việt thì gọi là chúng ta tiêm vào một truy vấn SQL, tiêm từ bên ngoài vào thì gọi là injecting. Hoặc một câu lệnh  sử dụng field nhập liệu của ứng dụng. Chúng ta sẽ tập trung vào SQL injection ở bài học này.

 Một SQL injection mà thành công là ta có thể đọc, thay đổi dữ liệu từ database và nó cũng có thể xóa dữ liệu từ database.

Nó cũng cho phép hacker thực hiện quản trị các hoạt động trên cơ sở dữ liệu như shutdown hoặc xóa cả database.

Để dể dàng hiểu được phần thực hành phía dưới, AD xin tóm tắt lại một chút về SQL Injection.

**SQL Injection**

SQL injection là đặt một mã độc trong phát biểu SQL theo đường input của web page.

**SQL – Web Pages**

SQL injection thường xuyên xãy ra khi bạn yêu cầu người dùng input, giống như username/userid, user sẽ cho bạn một câu lệnh SQL mà bạn sẽ vô tình chạy trong database của bạn.

Nhìn vào ví dụ dưới đây, mà tạo một truy vấn select bằng việc thêm giá trị biến (txtUserId) để lấy thông tin user. Biến được truyền từ input của web page vào và được lấy bằng phương thức (getRequestString).

EX: txtUserId = getRequestString(“UserId”);

txtSQL = “SELECT \* FROM Users WHERE UserId = “ + txtUserId;

**SQL Injection Dựa Vào 1=1 Luôn Luôn Đúng**

Nhìn vào ví dụ ở trên. Múc đích của code là tạo một truy vấn SQL để select một user với user id nhập vào từ input.

Nếu như không có gì để ngăn chặn user đưa vào một input “sai”, thì user có thể đưa vào một số input thông minh giống như sau:

UserId: 105 OR 1=1

Khi đó cấu phát biểu SQL giống như sau:

SELECT \* FROM Users WHERE UserId = 105 OR 1=1;

Câu phát biểu này có giá trị và sẽ trả về tất cả các dòng từ table Users, bởi vì 1=1 luôn luôn đúng.

Ví dụ này nguy hiễm không? Nếu table Users chứa đựng tên và password thì sao?

Mọi thứ đều được phơi bày ra, nguy hiễm hơn nếu table admin cùng với table của user, và hacker có thể login admin để điều khiển web site mà không cần biết pass.

**SQL Injection Dựa Vào “”=”” Luôn Luôn Đúng**

EX: user login vào web site:

Username : dammelaptrinh

Password : myPass

Chúng ta có sql statement như sau :

uName = getRequestString(“username”);  
uPass = getRequestString(“userpassword”);

sql = ‘SELECT \* FROM Users WHERE Name =”‘ + uName + ‘” AND Pass =”‘ + uPass + ‘”‘

Kêt quả: ***SELECT \* FROM Users WHERE Name = “dammelaptrinh” AND Pass = “myPass”***

Hacker có thể truy cập tới user trong database bằng cách đưa vào ” OR “”=” trong username input hoặc ô nhập password:

User Name: ” or “”=”

Password: ” or “”=”

Kết quả: SELECT \* FROM Users WHERE Name =”” or “”=”” AND Pass =”” or “”=””

Với cấu SQL này là hacker có thể login vào hệ thống mà không cần biết gì về account cả. Chết mày chưa hehe.

**SQL Injection Dựa Vào Batched SQL Statement**

Hầu hết các database đầu hổ trợ batched SQL statement.

Một batch của SQL statements là một nhóm 2 hay nhiều cấu lệnh SQL tách biệt bởi dấu (;).

Phát biểu dưới đây sẽ trả về tất cả các dòng table user, sau đó xóa bảng Supplies.

EX: SELECT \* FROM Users; DROP TABLE Supplies

Như ví dụ đầu tiên nếu ta input vào User Id như sau:

User id: 105; DROP TABLE Supplies

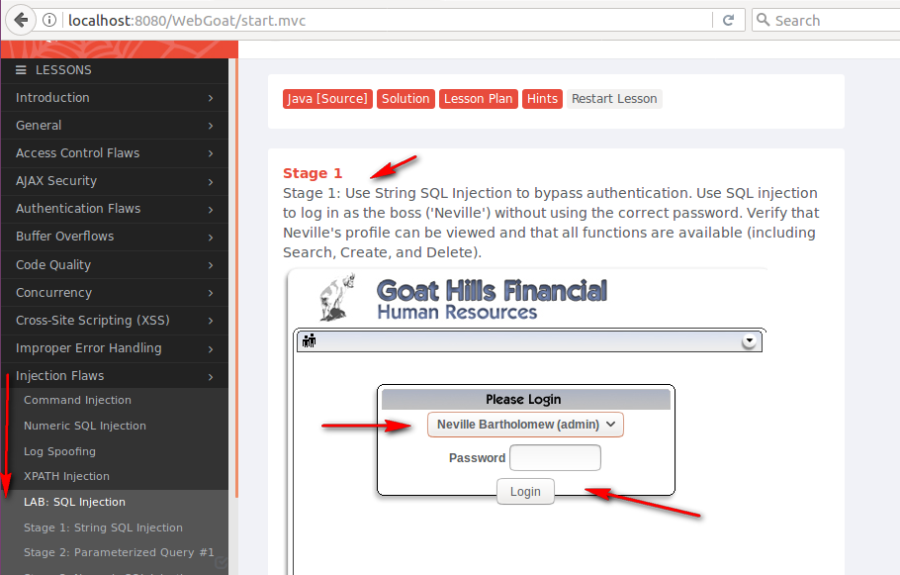
Kết quả sẽ là : SELECT \* FROM Users WHERE UserId = 105; DROP TABLE Suppliers;

Tanh banh web luôn.

**Thực Hành**

Đến phần mong đợi rồi đây quý vị.

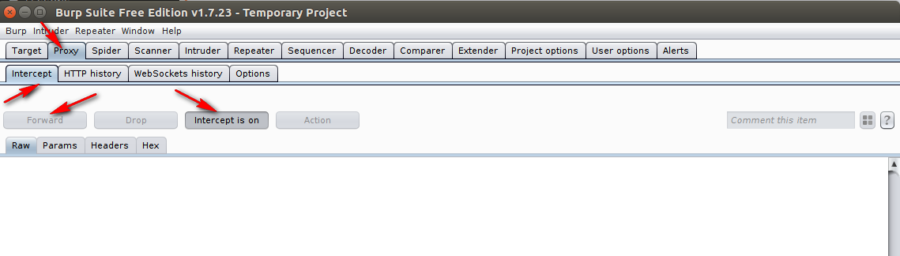
1. Mở ứng dụng mẩu của chúng ta ra (WebGoat) , sử dụng acc guest/guest để login vào hệ thống và tìm đến mục Inject Flaws -> LAB: SQL Injection

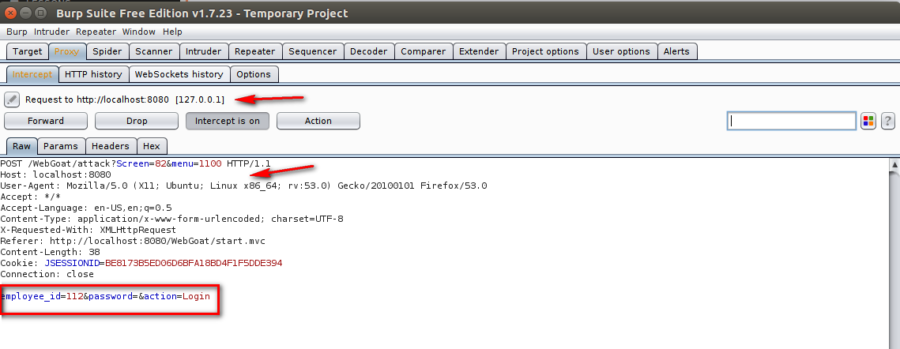


1. (Neville) mà không cần nhập pass đúng. Nếu thành công chúng ta có thể xem profile của Neville và tất cả chức năng liên quan acc này.

1. Chúng ta sẽ dựa vào ‘1’=’1’ luôn đúng.

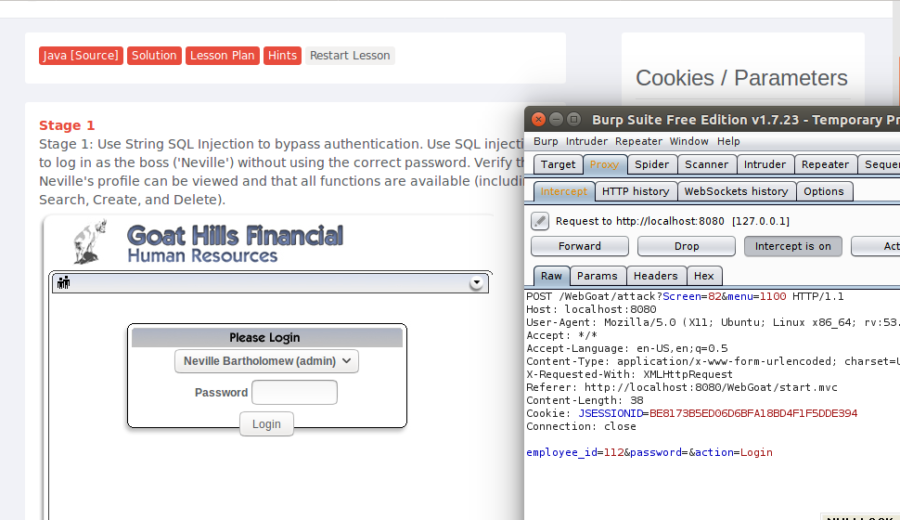
1. Mở đồ chơi của chúng ta ra Burp với cấu hình đã thiết lập ở bài trước, bây giờ truy cập vào tab proxy -> intercept , quan sát tab “Intercept is on” nếu các bạn thấy chữ này có nghĩa là Burp đang lắng nghe, và khi bạn truy cập web, web của bạn sẽ bị burp chặn lại mà không thể load hoàn tất, sau đó từ màn hình Proxy của burp bạn sẽ thấy các giá trị mà client gửi tới server, nếu bạn click vào nút Forward thì web sẽ tiếp tục load page hoàn tất. Khi không muốn cho Burp đánh chặn web thì bạn click vào Intercept is on, nó sẽ biến thành Intercept is off. Nhìn hình thôi.

Burp đã sẳn sang và bây giờ trở ra màn hình webgoad, click vào button login ,thích thì nhập pass, không thì nhấn submit Burp sẽ bay lên chặn ngay. Hình đây.

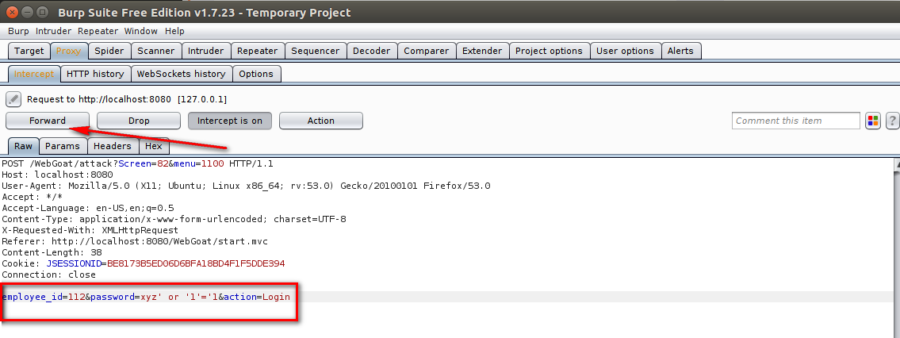


Các bạn chú ý hình chữ nhật màu đỏ trên hình, đó là thông tin mà chúng ta input vào web page, và cũng là cái cũng ta sẽ thay đổi giá trị để hack.

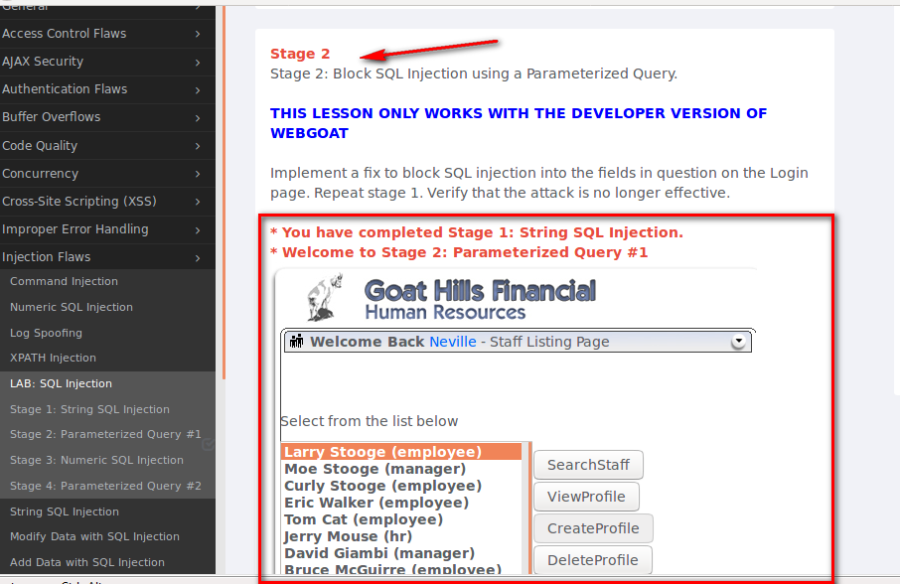
Lúc bây giờ burp đang đánh chặn website , nên ở ngoài webgoat khung đăng nhập vẩn chưa có kết quả trả về, nếu không bạn sẽ thấy trạng thái login vào thành công hoặc là sẽ gặp thông báo lổi.



1. Bây giờ chúng ta sẽ thay đổi giá trị trong ổ chữ nhật màu đỏ.



1. Sau khi thay đổi nội dung đăng nhập ,ta cho web tiếp tục gửi thông tin tới server bằng cách click Forward, nếu thành công các bạn sẽ thấy login thành công và như màn hình sau:



Xin chúc mừng bạn đã hack thành công và có thể sử dụng chức năng như account Boss Neville.

**Ngăn Chặn SQL Injection**

Có rất nhiều cách để ngăn chặn SQL Injection. Khi developer ghi code thì nên bảo đảm rằng bạn phải xử lý các ký tự đặc biệt tương ứng. Sau đây một số kỹ thuật để ngăn chặn cách tấn công này:

* Sử dụng đối số cho truy vấn
* Escape tất cả input cung cấp
* Bật thuộc tính tối thiểu database cho user