BÀI THỰC HÀNH SỐ 8

KIỂM THỬ LỖ HỔNG SQL INJECTION

***Họ và tên: Nguyễn Thanh Trường***

***MSSV: 1050080082***

**Câu 1*(3.5 điểm)***

Kiểm thử lỗ hổng SQL Injection trên trang web http://webvul.bkcs.vn/register.php

* Xác định các tham số đầu vào và cách thức chúng được gửi tới server **(0.25 điểm)**
* Trang register.php yêu cầu người dùng nhập:
  + username
  + password
  + confirm\_password
* Phân tích và phán đoán kiểu truy vấn **(0.25 điểm)**
  + Dựa vào chức năng, ta có thể phán đoán câu truy vấn dạng:
    - INSERT INTO users (username, password) VALUES ('$username', '$password');
    - Trong đó, $username và $password là các biến lấy trực tiếp từ đầu vào người dùng.
* Phân tích và phán đoán vị trí của các giá trị tham số đầu vào được sử dụng trong câu truy vấn **(0.5 điểm)**
  + $username và $password được sử dụng trực tiếp trong truy vấn SQL, không qua xử lý hay kiểm tra đầu vào kỹ lưỡng.
  + Điều này có thể tạo điều kiện để chèn thêm các câu lệnh SQL thông qua giá trị username.
* Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào **(2.5 điểm)**
  + testuser -> Kiểm tra đăng ký hợp lệ -> Thành công, người dùng được thêm
  + testuser');-- -> Chèn dấu ' và comment để kết thúc câu truy vấn -> SQL báo lỗi nếu không có filter
  + testuser', '123');-- -> Tạo SQL hoàn chỉnh: INSERT INTO users (username, password) VALUES ('testuser', '123');--') -> Có thể đăng ký thành công dù không đúng logic
  + ' OR 1=1-- -> Mục tiêu chèn để bỏ qua kiểm tra trùng lặp username -> Nếu không xử lý đúng, có thể gây trùng lặp, phá vỡ dữ liệu
  + abc'); DROP TABLE users;-- -> Thử phá hủy bảng users -> Nếu thành công => lỗ hổng nghiêm trọng

**Câu 2 *(3.5 điểm)***

Kiểm thử lỗ hổng SQL Injection trên trang web http://webvul.bkcs.vn/login.php

* Xác định các tham số đầu vào và cách thức chúng được gửi tới server **(0.25 điểm)**
* Phân tích và phán đoán kiểu truy vấn, phân tích và phán đoán vị trí của các tham số đầu vào được sử dụng trong câu truy vấn **(0.25 điểm)**
* Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào **(3 điểm)**

*Lưu ý:*

* *Nói rõ mục đích sử dụng các giá trị kiểm thử*
* *Giải thích rõ các phán đoán và suy luận từ kết quả khi sử dụng mỗi giá trị kiểm thử*

**Câu 3 *(3 điểm)***

Kiểm thử lỗ hổng SQL Injection trên trang web http://webvul.bkcs.vn/index.php

* Xác định các tham số đầu vào và cách thức chúng được gửi tới server **(0.25 điểm)**
* Phân tích và phán đoán kiểu truy vấn, vị trí của các tham số đầu vào được sử dụng trong câu truy vấn **(0.25 điểm)**
* Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào **(2.5 điểm)**

*Lưu ý:*

* *Nói rõ mục đích sử dụng các giá trị kiểm thử*
* *Giải thích rõ các phán đoán và suy luận từ kết quả khi sử dụng mỗi giá trị kiểm thử*

**4 Sử dụng công cụ hỗ trợ kiểm thử Burpsuite**

Khi thực hiện kiểm thử SQL Injection, các giá trị kiểm thử không phải lúc nào cũng có thể truyền qua form nhập liệu hoặc tham số trên địa chỉ URL. Khi đó, việc sử dụng các công cụ hỗ trợ cho phép phát hiện dễ dàng hơn các điểm nhận giá trị đầu vào của ứng dụng Web và thay đổi các giá trị đó. Trong hầu hết các trường hợp, việc sử dụng tốt các công cụ hỗ trợ sẽ giúp quá trình kiểm thử thực hiện nhanh

14

chóng hơn. Chúng ta sẽ làm quen với công cụ Burpsuite để hỗ trợ kiểm thử lỗ hổng SQL Injection cho website.

Burpsuite là một ứng dụng được tích hợp nhiều tính năng phục vụ kiểm tra bảo mật ứng dụng web. Các tính năng này sẽ phục vụ kiểm tra bảo mật các thành phần khác nhau trong ứng dụng web hiện đại ngày nay. Burpsuite có thể giúp người dùng đánh giá các tiêu chí bảo mật web như: Kiểm tra cơ chế xác thực, kiểm tra các vấn đề về phiên người dùng hoặc liệt kê và đánh giá các tham số đầu vào của ứng dụng web v.v… Chương trình không những hỗ trợ mạnh mẽ trong quy trình đánh giá bảo mật thủ công mà còn bao gồm công cụ quét lỗ hỗng bảo mật được tích hợp trong phiên bản có phí.

Burp được phát triển bởi Công ty PortSwigger Ltd và được phân phối thành hai phiên bản là Burp Free và Burp Professional. Download công cụ tại địa chỉ sau:

https://portswigger.net/burp/freedownload

Mặc dù trong phiên bản thương mại được tích hợp chức năng quét lỗ hổng ứng dụng tự động và một số tính năng nâng cao, tuy nhiên với sự kết hợp thành thạo các tính năng trong phiên bản miễn phí sẽ giúp người dùng tận dụng tối đa hiệu quả trong đánh giá bảo mật ứng dụng mà không cần đầu tư chi phí cho công cụ.

**4.1. Hướng dẫn cấu hình cơ bản**

Người dùng Windows có thể thực thi chương trình bằng cách mở tập tin burpsuite\_free\_vxx.jar sau khi đã download và bảo đảm rằng Java Runtime đã được cài đặt trên máy tính.

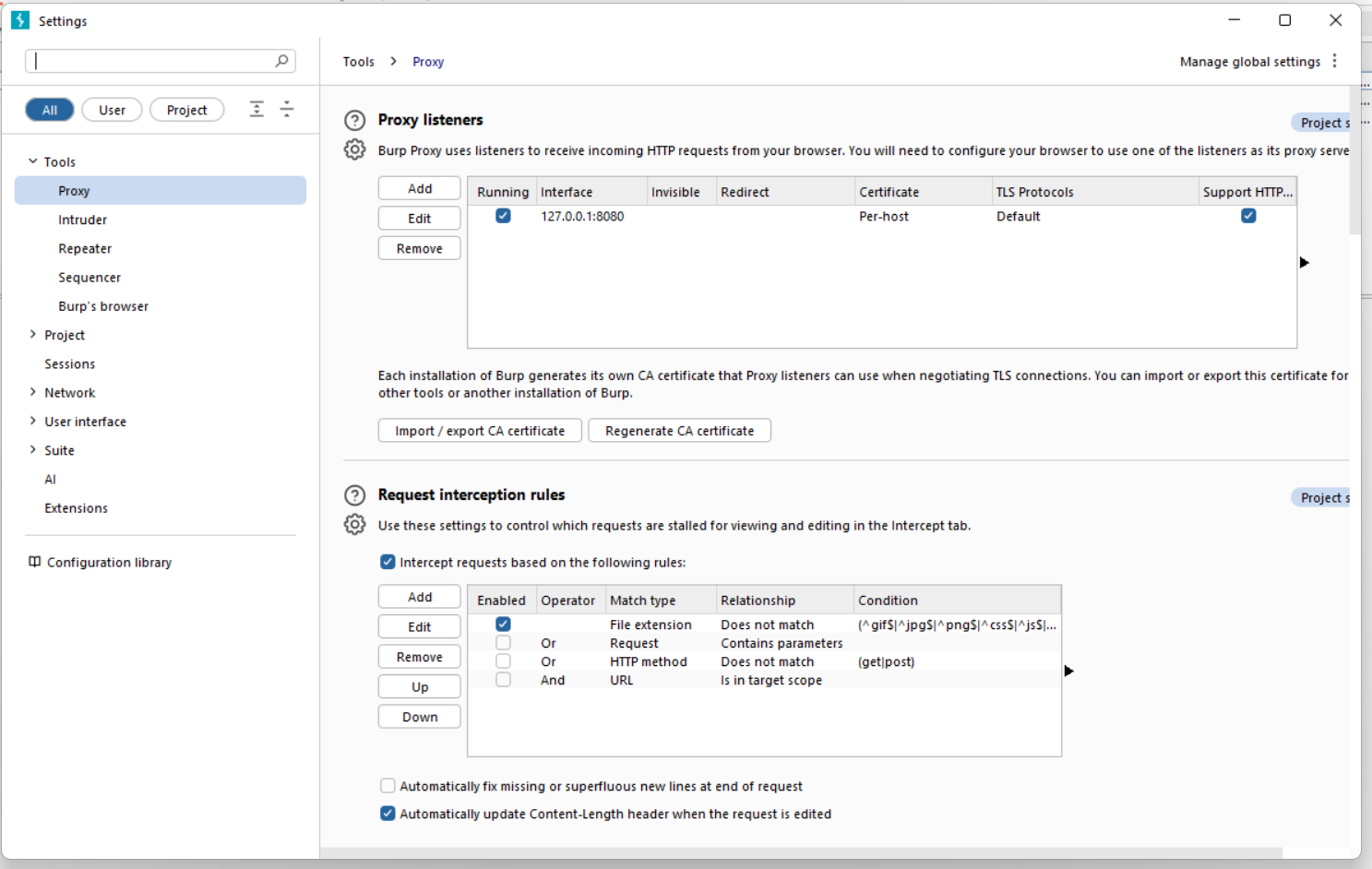
**Kiểm tra hoạt động Burp**

Burp Proxy đóng vai trò là chương trình trung chuyển các HTTP Request/Respone giữa trình duyệt và ứng dụng web, gọi là Intercepting Proxy. Burp cho phép người dùng toàn quyền điều khiển việc gởi/nhận dữ liệu HTTP/s đến máy chủ và trình duyệt phục vụ việc đánh giá bảo mật ứng dụng web một cách cụ thể cho từng lỗ hổng bảo mật.

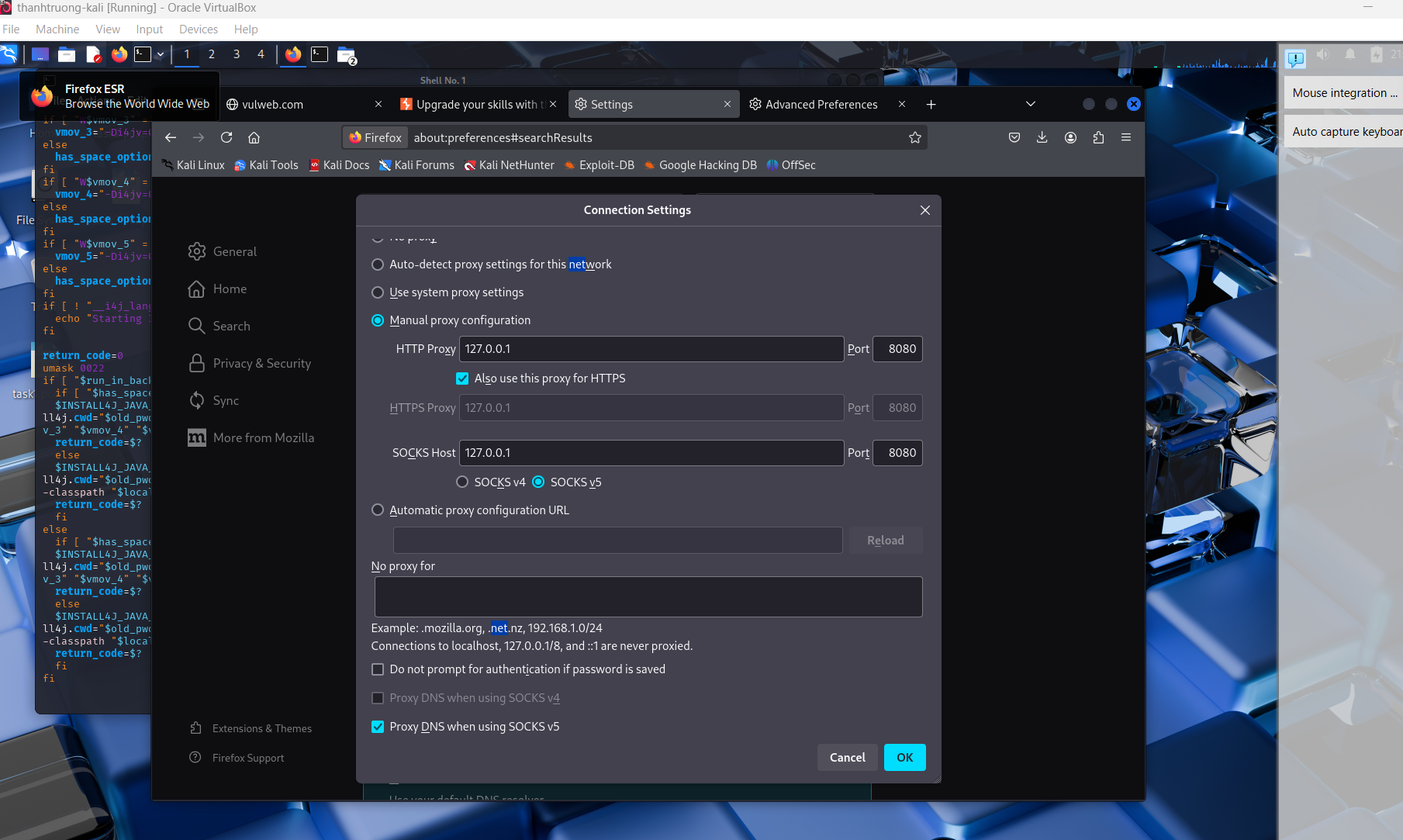
**Cấu hình tại Burp Proxy**

15

Theo mặc định, Burp Proxy được cấu hình lắng nghe trên cổng 8080/TCP. Để kiểm tra chắc chắn rằng không có chương trình hoặc dịch vụ nào khác đang lắng nghe trên cùng cổng 8080/TCP, bạn thực hiện kiểm tra tại thẻ Proxy | Options.

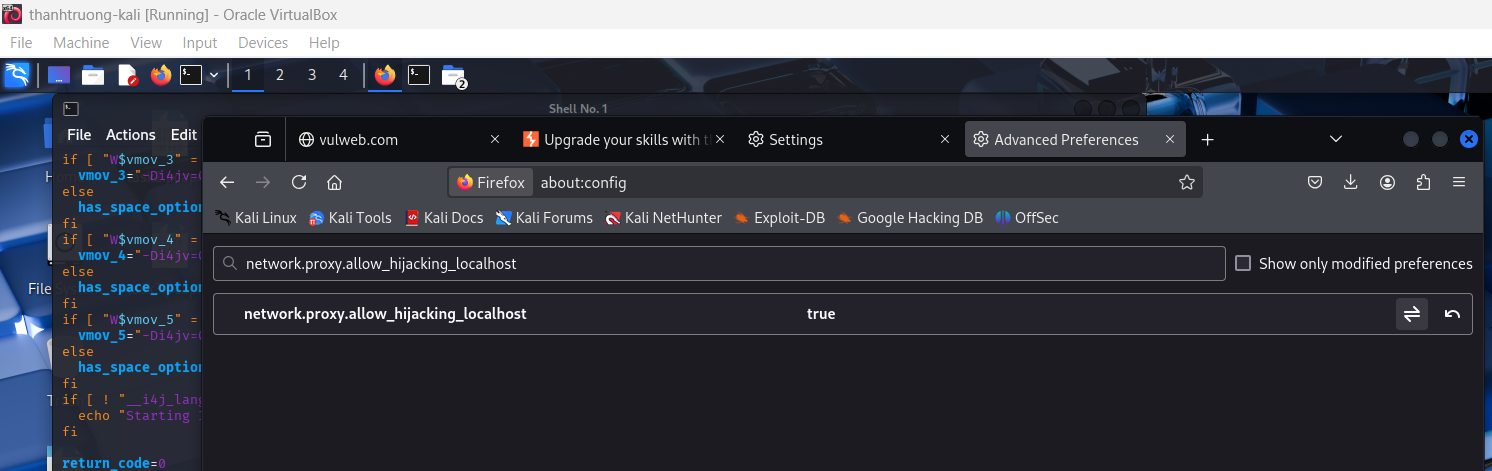
**Cấu hình tại trình duyệt**

Thực hiện cấu hình Proxy tại trình duyệt Firefox như ảnh minh họa



Thiết lập cấu hình để cho phép proxy hoạt động với các các lưu lượng cục bộ (localhost): - Bước 1: Mở một tab mới và truy cập tới trang about:config. Bỏ qua các cảnh báo nếu có

- Bước 2: Điền giá trị network.proxy.allow\_hijacking\_localhost vào ô tìm kiếm và thiết lập giá trị **true** cho nó

**4.2. Sử dụng Burpsuite hỗ trợ kiểm thử SQL Injection**

Phần này sẽ minh họa việc sử dụng Burpsuite để tương tác với website khi kiểm thử SQL Injection

- Bước 1: Cấu hình và khởi động Burpsuite như hướng dẫn ở phần trước

- Bước 2: Trên cửa sổ công cụ Burpsuite, mở thẻ Proxy → Intercept và chắc chắn tính năng Intercept is on đã được bật

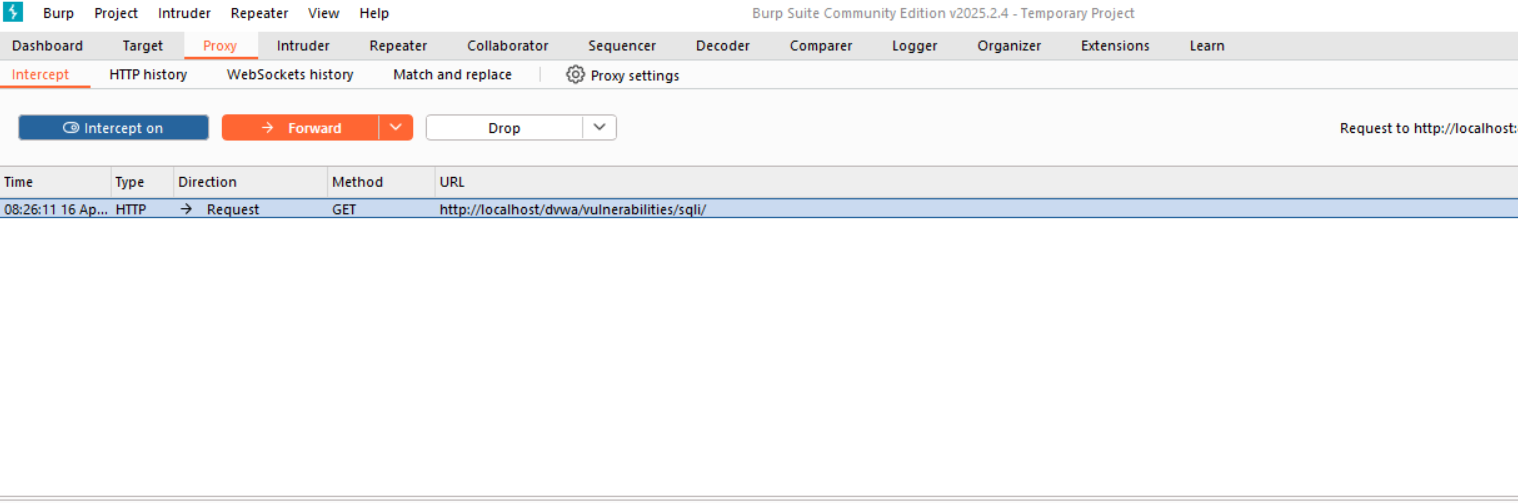
- Bước 3: Mở địa chỉ trang Web cần kiểm thử. Ví dụ dưới đây là giao diện kiểm tra lỗ hổng SQL Injecion trên website DVWA.

http://localhost/dvwa/vulnerabilities/sqli/

- Bước 4: Điền các giá trị bất kỳ nào đó và gửi yêu cầu từ trình duyệt

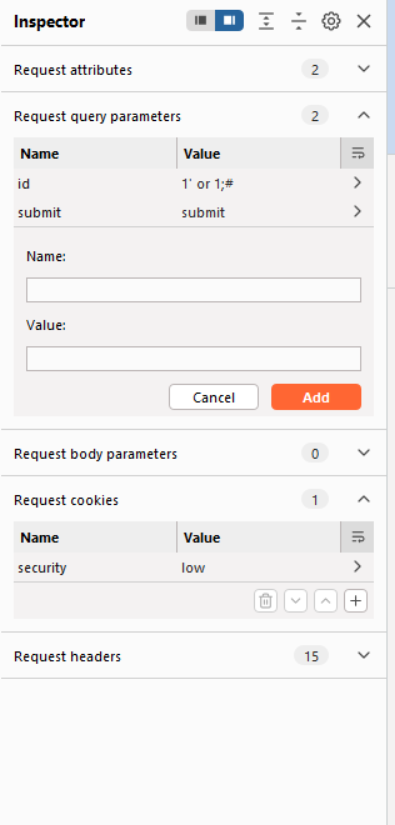
- Bước 5: Trên thẻ Proxy → Intercept, nhấn nút Forward để chuyển tiếp yêu cầu

17



- Bước 6: Mở thẻ Proxy → HTTP history, chúng ta sẽ thấy danh sách các thông điệp HTTP mà Burpsuite đã bắt được. Chọn thông điệp HTTP Request tương ứng ở bước 4, nhấn chuột phải và chọn Send to Repeater

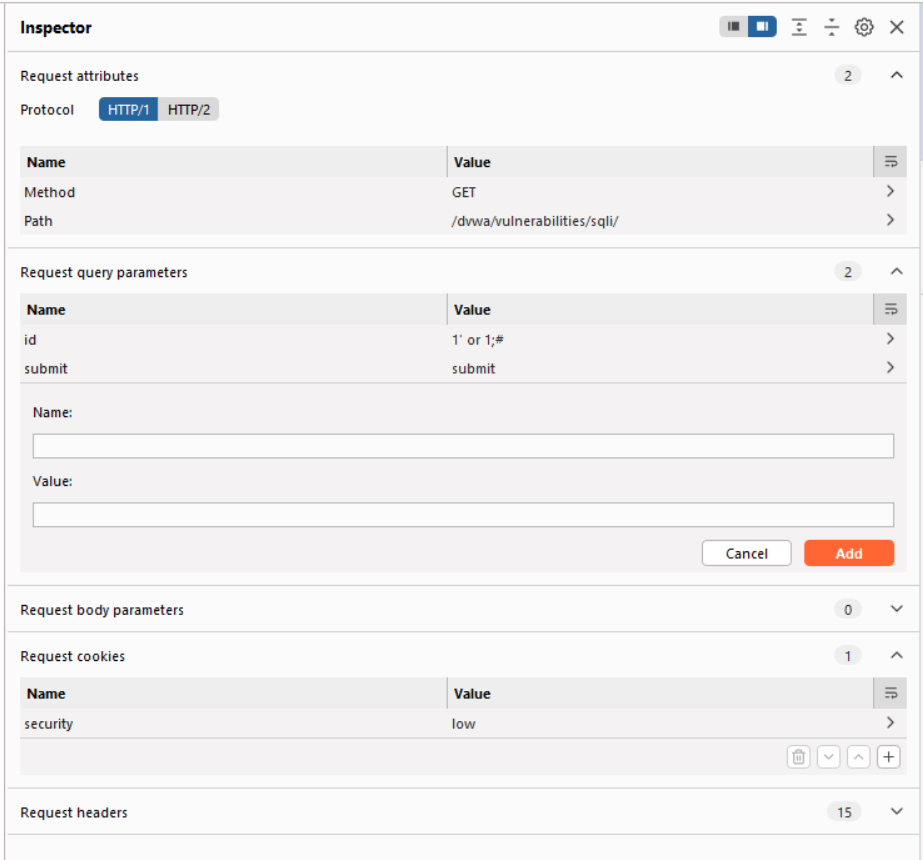
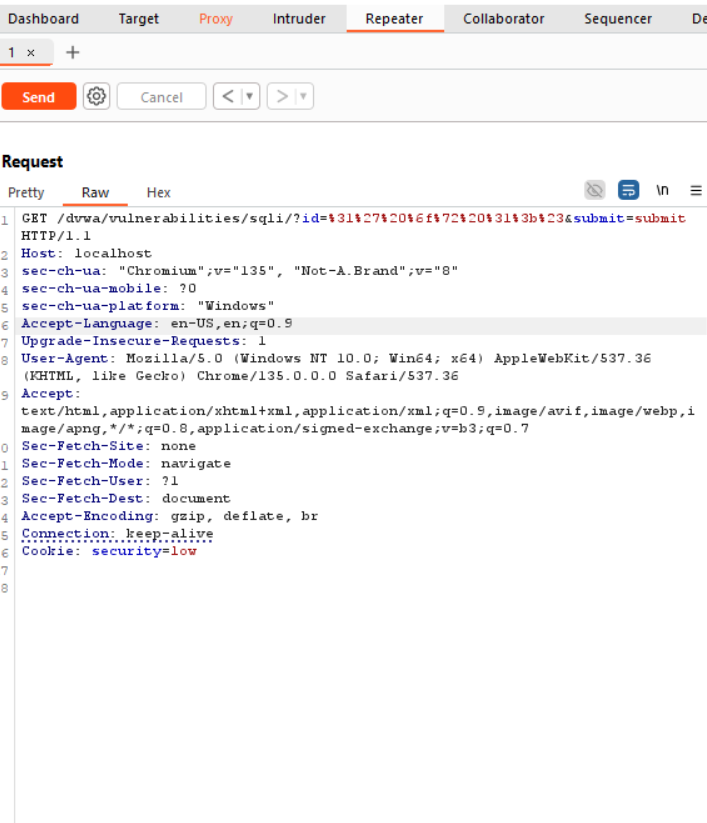
- Bước 7: Chọn thẻ Repeater. Thẻ này cho phép chúng ta thay đổi nội dung của HTTP Request và phát lại tới máy chủ. Thẻ con Params liệt kê danh sách các giá trị trên HTTP Header có thể là tham số đầu vào.



- Bước 8: Để thực hiện kiểm thử cho tham số đầu vào id chúng ta sẽ sửa trực tiếp trên thẻ con Raw. Chọn thẻ Decoder, điền chuỗi 1' or 1;# và chọn Encode as…→ URL. Kết quả encode cho chúng ta xâu %31%27%20%6f%72%20%31%3b%23. Chọn lại thẻ Repeater, thay xâu giá trị này vào cho tham số id và nhấn nút Go. Thông điệp HTTP Response trả về từ server được hiển thị theo nhiều dạng khác nhau trong phần Response.

*(Giá trị các tham số cũng có thể sửa trực tiếp từ thẻ Params mà không cần qua encode)*

18



**5. Minh họa cách thức kiểm thử hộp đen**

**5.1. Cài đặt môi trường**

- Bước 1: Download mã nguồn và cơ sở dữ liệu từ địa chỉ sau.

https://users.soict.hust.edu.vn/tungbt/it4263/lab05\_tut.zip

- Bước 2: Giải nén file download. Sử dụng WinSCP hoặc công cụ tương tự để upload thư mục lab05\_tut vừa giải nén được vào thư mục /home/bkcs của máy ảo

- Bước 3: Khởi động và truy cập vào máy ảo.

- Bước 4: Trên cửa sổ dòng lệnh, chuyển thư mục làm việc

cd /home/bkcs/lab05\_tut

- Bước 3: Sao chép thư mục sqli vào thư mục /var/www/html

sudo cp -rf sqli /var/www/html

- Bước 4: Tạo cơ sở dữ liệu có tên là webvul và import file webvul.sql vào. Tài khoản truy cập mysql là root và mật khẩu là 123456