**BÁO CÁO BÀI THỰC HÀNH SỐ 8**

**KIỂM THỬ LỖ HỔNG SQL INJECTION**

***Họ và tên:***

***Yêu cầu kết quả thực hành:***

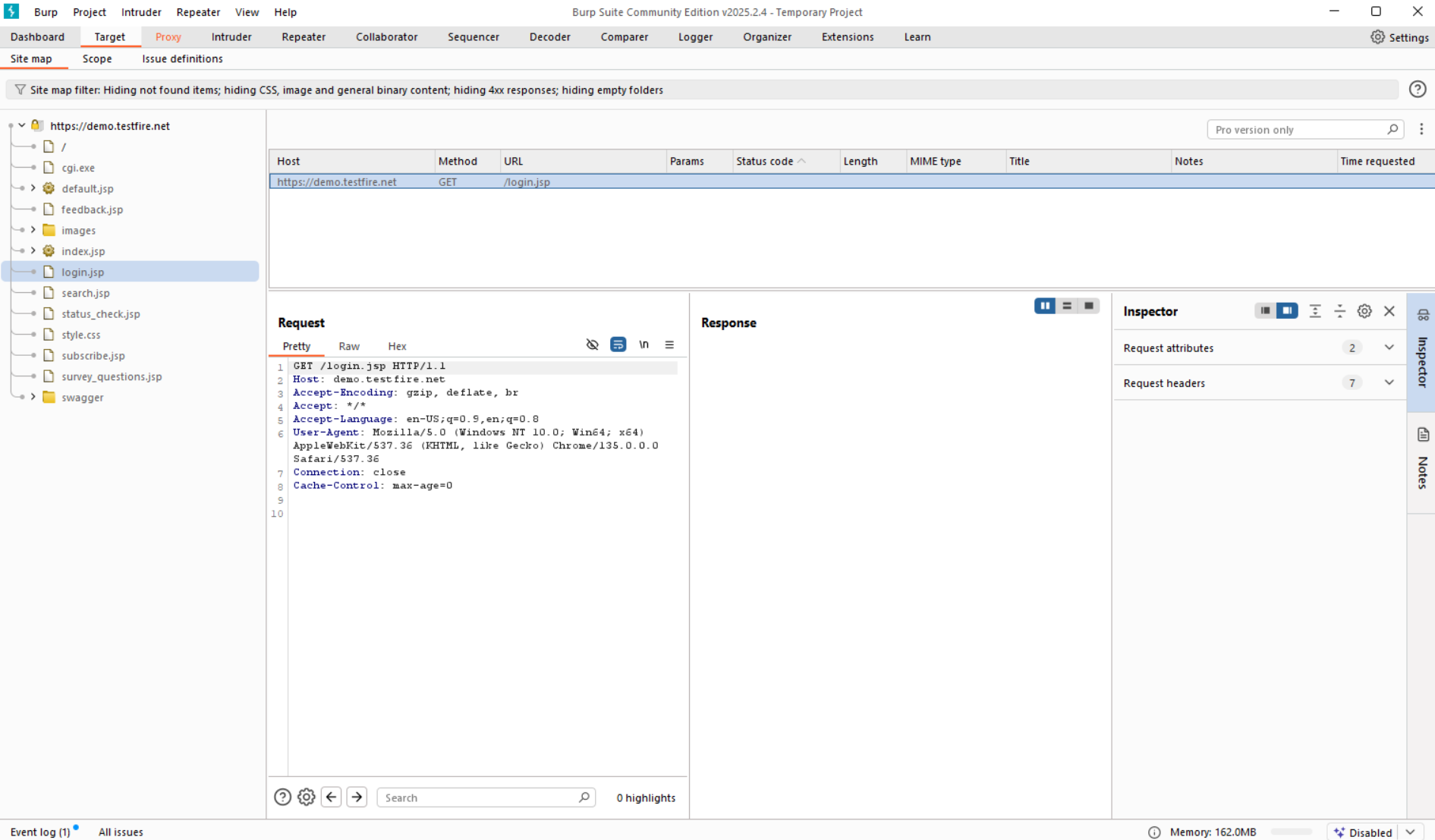
Báo cáo kết quả thực hành có tên theo định dạng DaoNgocQui\_1050080113\_Lab08.docx

**Câu 1*(3.5 điểm)***

Kiểm thử lỗ hổng SQL Injection trên trang web <https://demo.testfire.net/>

* Xác định các tham số đầu vào và cách thức chúng được gửi tới server **(0.25 điểm)**

Không có tham số đầu vào vì toàn bộ là GET chứ không phải là POST



* Phân tích và phán đoán kiểu truy vấn **(0.25 điểm)**

Không có truy vấn SQL nào liên quan đến CSDL

* 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)**

Vì là GET nên không có tham số truyền vào

* Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào **(2.5 điểm)**

Không thể xác định được mức độ tham số đầu vào

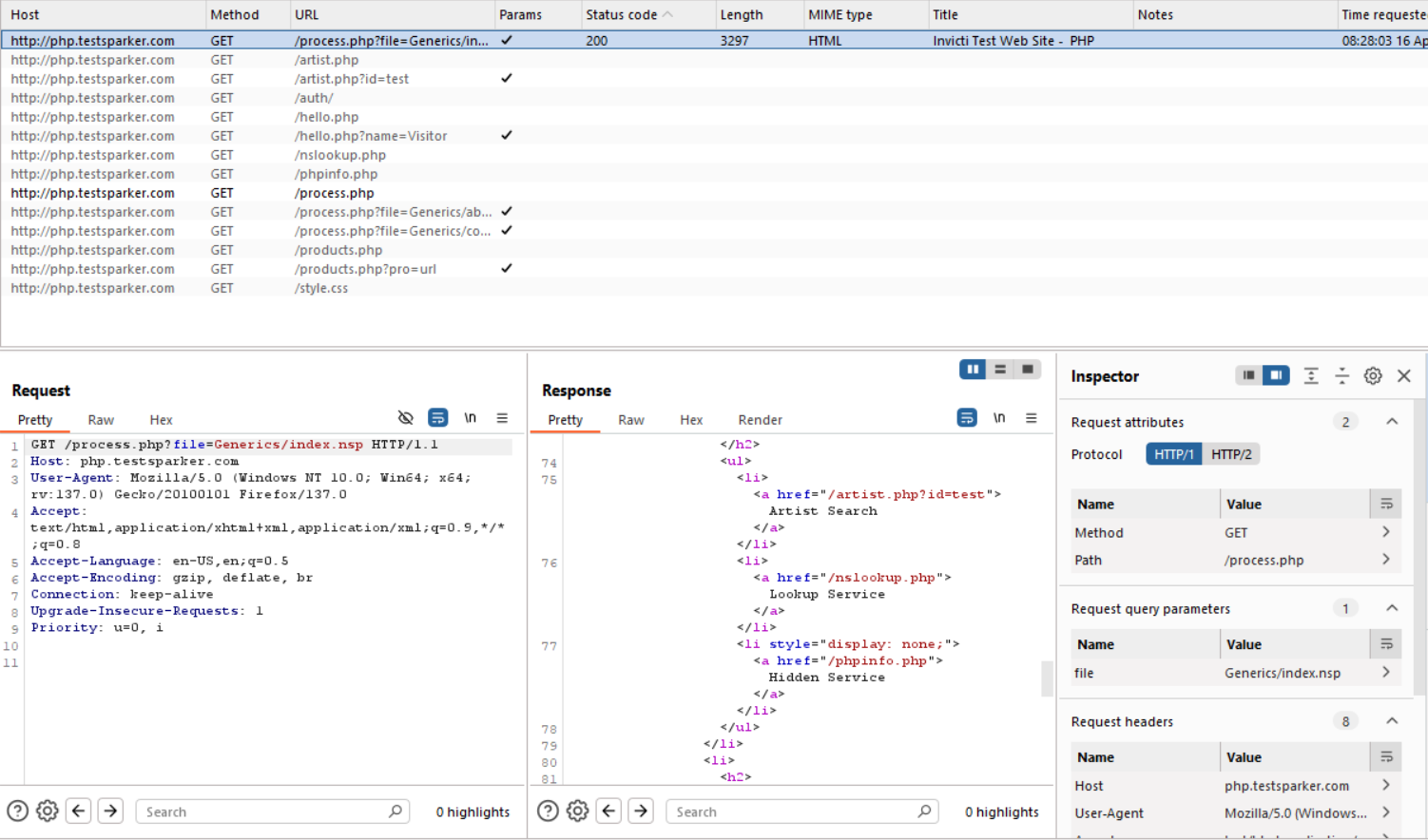
*Lưu ý:*

* *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 2 *(3.5 điểm)***

Kiểm thử lỗ hổng SQL Injection trên trang web php.testsparker.com/process.php?file=Generics/index.nsp

**1. Xác định các tham số đầu vào và cách thức chúng được gửi tới server (0.25 điểm)**

****

Cách thức xác định: Quan sát dòng đầu tiên và URL trong phần "Request" của yêu cầu được chọn trong Burp Suite.

Kết quả:

Phương thức gửi: GET (như thấy ở dòng GET /process.php?... HTTP/1.1)

URL đích: /process.php

Tham số đầu vào: Có một tham số được gửi qua URL (Query String):

file: với giá trị hiện tại là Generics/index.nsp.

**2. Phân tích và phán đoán kiểu truy vấn (0.25 điểm)**

Phân tích chức năng: Tham số có tên là file và giá trị của nó (Generics/index.nsp) là một đường dẫn đến tệp tin. File có thể đang thực hiện chức năng đọc (read) hoặc bao gồm (include) nội dung của tệp được chỉ định bởi tham số file. Đây là dấu hiệu điển hình của các chức năng liên quan đến Local File Inclusion (LFI) hoặc Remote File Inclusion (RFI).

Phán đoán kiểu truy vấn SQL: Việc đọc/include tệp tin nên thường không có truy vấn CSDL

**3. 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**)

Tham số file được sử dụng cho các thao tác với hệ thống tệp chứ không phải trong truy vấn SQL,

Tham số file không được sử dụng trong mệnh đề WHERE hay bất kỳ phần nào khác của một câu truy vấn SQL. Nó có thể được sử dụng trực tiếp như một chuỗi trong các hàm xử lý tệp của ngôn ngữ lập trình phía server

**4. Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào (2.5 điểm)**

Đối với SQL Injection: It có khả năng liên quan trực tiếp đến SQL, nên chưa thể xác định được

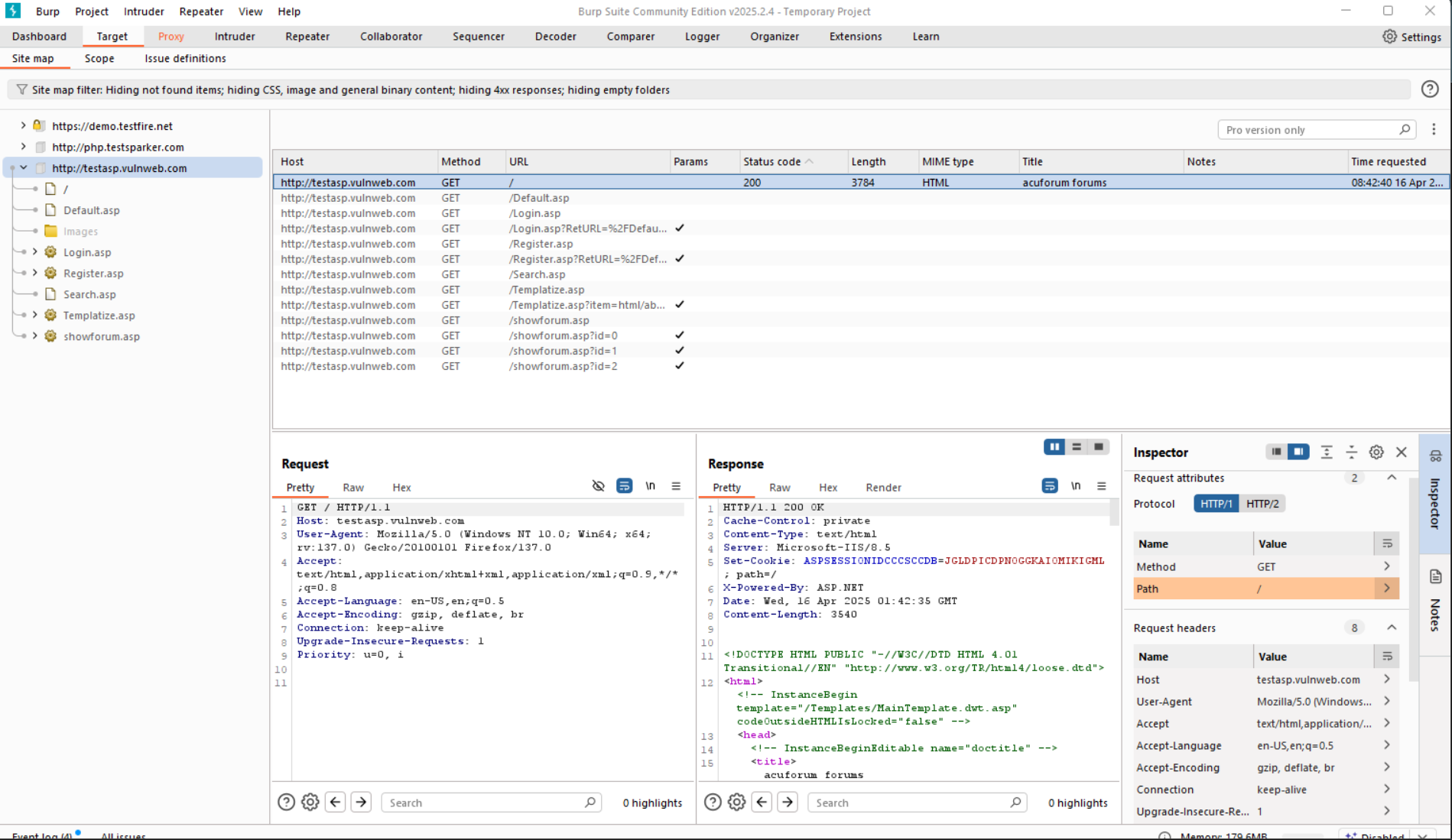
*Lưu ý:*

* *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://testasp.vulnweb.com/>

1. **Xác định các tham số đầu vào và cách thức chúng được gửi tới server (0.25 điểm**)



Cách thức xác định: Quan sát dòng đầu tiên và URL trong phần "Request".

Kết quả:

Phương thức gửi: GET (như thấy ở dòng GET / HTTP/1.1)

URL đích: /

Tham số đầu vào: Đối với yêu cầu GET / này, không có tham số nào được gửi kèm theo trong URL Do đó, yêu cầu cụ thể đang hiển thị trong hình không chứa tham số đầu vào nào được gửi từ client lên server.

**2. Phân tích và phán đoán kiểu truy vấn (0.25 điểm)**

Phân tích chức năng: Yêu cầu GET / là để tải trang chủ của diễn đàn "acuforum". Việc tải trang chủ có thể liên quan đến việc lấy dữ liệu từ cơ sở dữ liệu như: danh sách các chuyên mục diễn đàn, các bài viết mới nhất, thông tin người dùng đang đăng nhập (nếu có phiên), v.v.

Phán đoán kiểu truy vấn: có thể là câu lệnh SELECT trong SQL.

1. **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)**

Khó quán đoán do không có đường dẫn trực tiếp. Vì là phương thức GET

**4. Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào (2.5 điểm)**

Vì GET / này không có tham số đầu vào để kiểm thử, chúng ta không thể xác định mức độ ảnh hưởng của lỗ hổng SQL Injection

*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*