**BÁO CÁO BÀI THỰC HÀNH SỐ 8**

**KIỂM THỬ LỖ HỔNG SQL INJECTION**

***Họ và tên: Đào Ngọc Hòa\_1050080050\_CNPM 1***

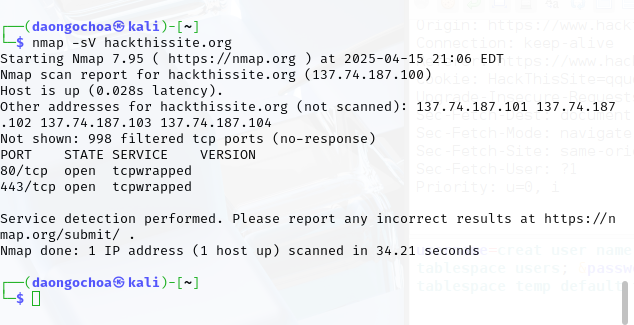
***Yêu cầu kết quả thực hành:***

Báo cáo kết quả thực hành có tên theo định dạng HoTenSV\_MSSV\_Lab08.docx

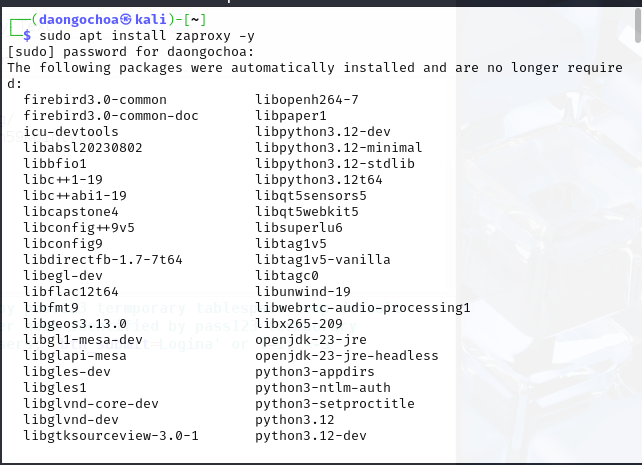
**Câu 1*(3.5 điểm)***

Kiểm thử lỗ hổng SQL Injection trên trang web <https://hackthissite.org/>

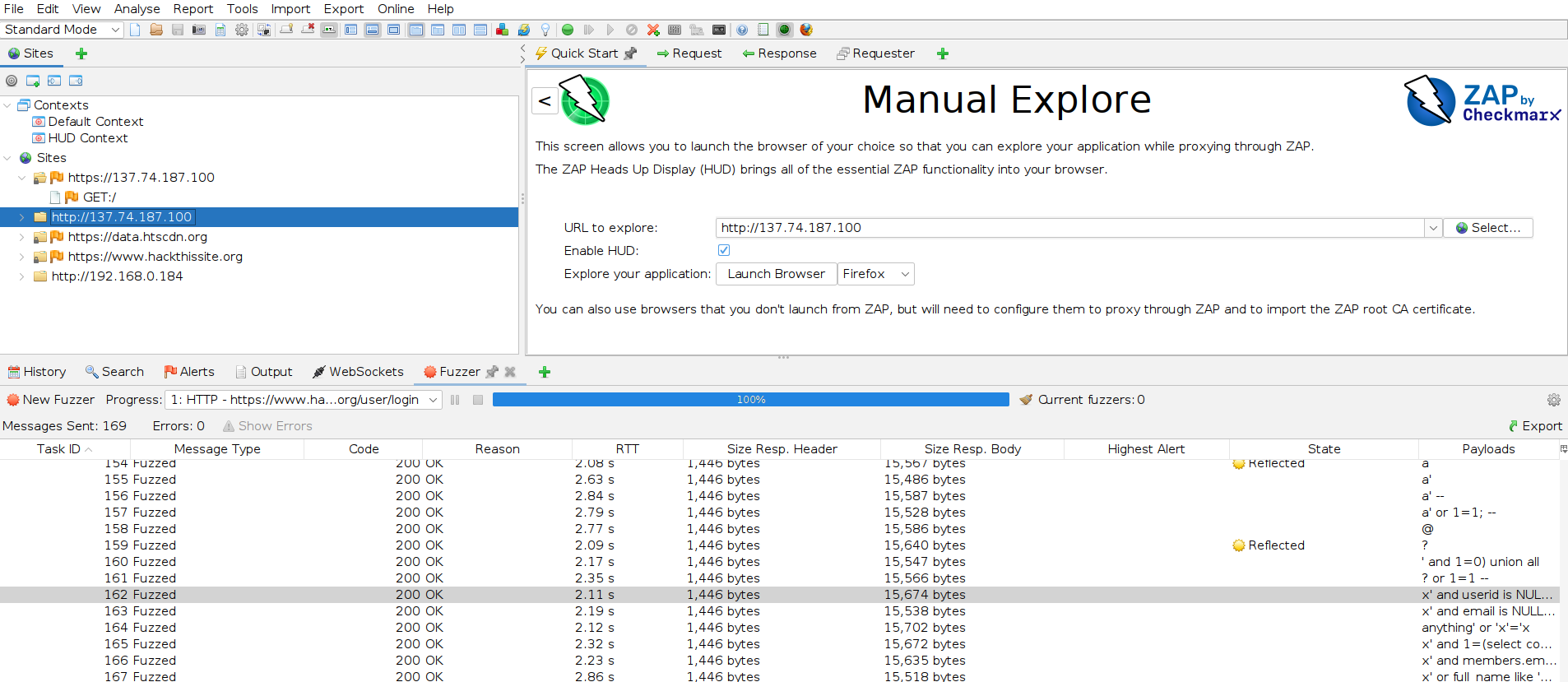
* Sử dụng nmap để quét địa chỉ máy chủ



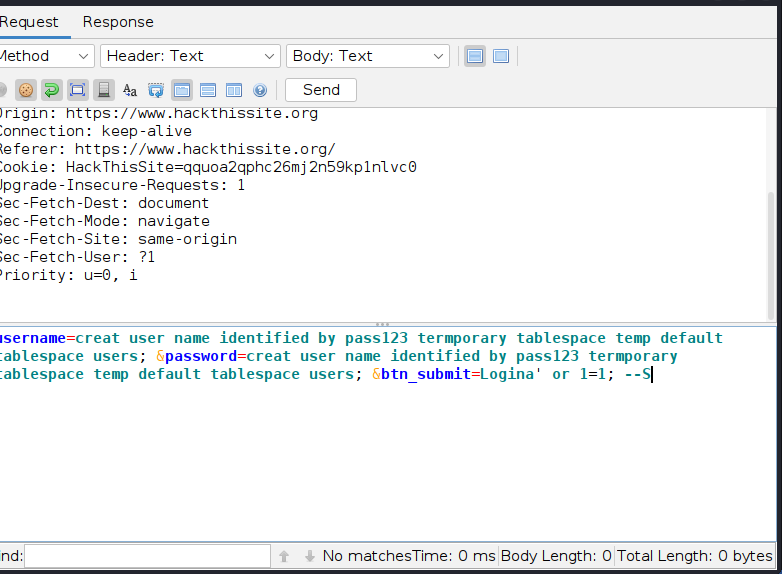
* Cài đặt zaproxy để quét địa chỉ



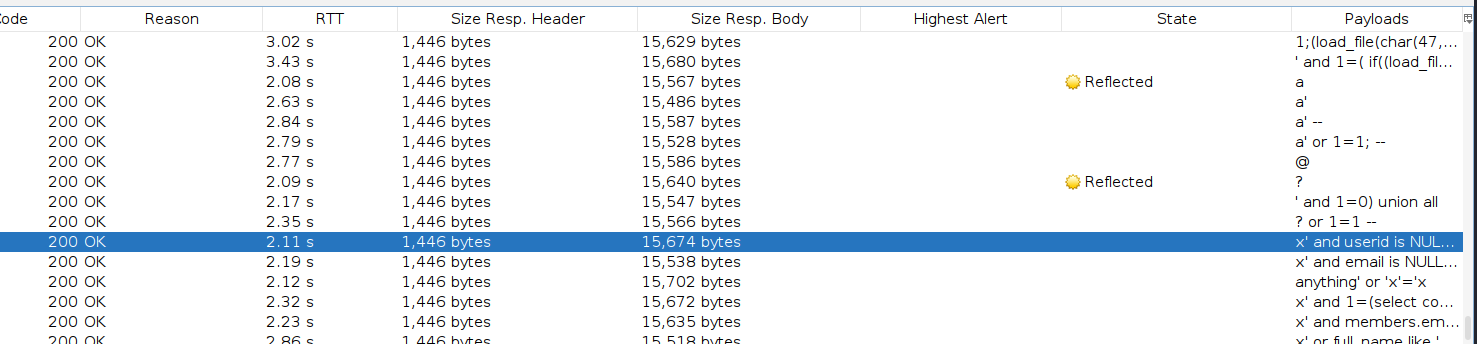
* Chạy zaproxy



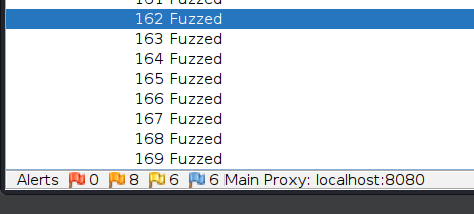
* Setup tham số đầu vào để tiến hành quét



* thử nghiệm các phương pháp SQL injection để tìm lỗ hổng trong hệ thống.



* 8 medium, 6 low cho cách cảnh báo bảo mật



*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 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*