

# BÁO CÁO THỰC HÀNH

Môn học: Bảo mật web và ứng dụng

Lab 1: Tổng quan các lỗ hổng bảo mật web thường gặp

GVHD: Nghi Hoàng Khoa

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.P11.ATCL.1

STT	Họ và tên	MSSV	Email
1	Tôn Thất Bình	21520639	2152xxxx@gm.uit.edu.vn
2	Nguyễn Văn Hào	20521293	2052xxxx@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Kết quả tự đánh giá
1	Bài tập 1	100%
2	Bài tập 2	100%
3	Bài tập 3	100%
4	Bài tập 4	100%
5	Bài tập 5	100%
6	Bài tập 6	100%

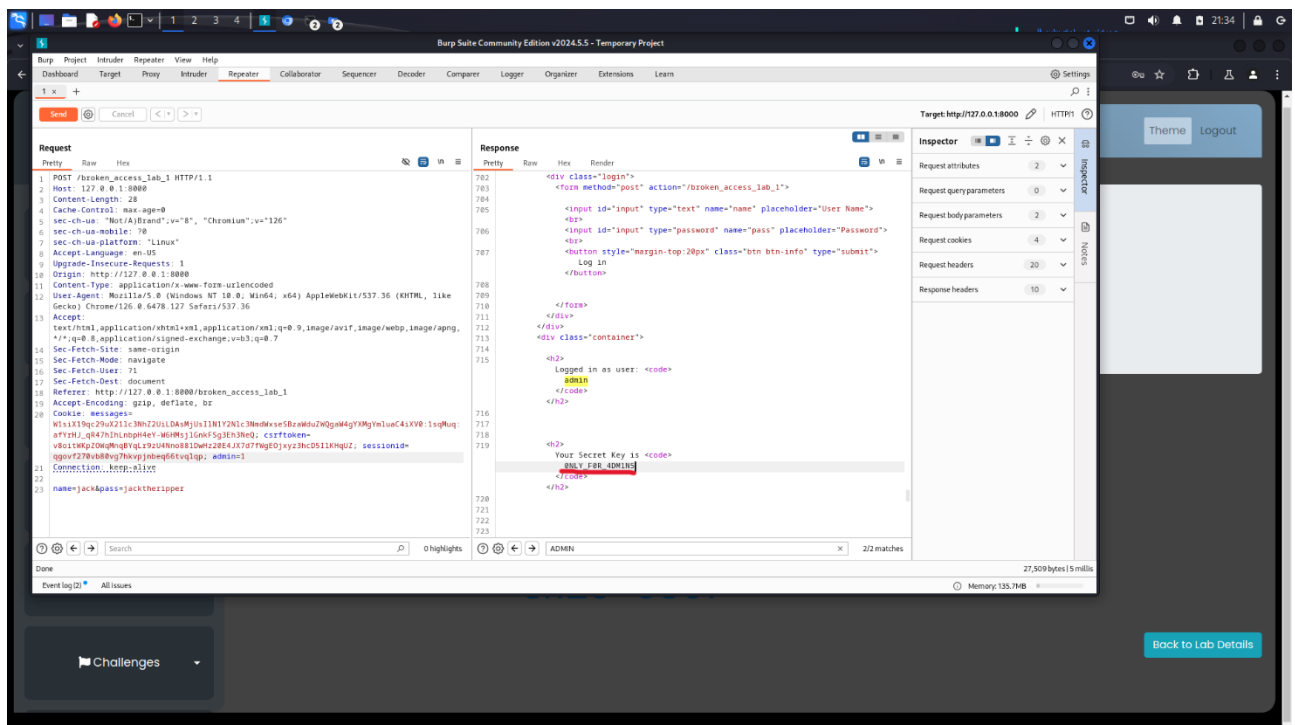
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

# BÁO CÁO CHI TIẾT

## a) A01:2021-Broken Access Control

**Bài tập 1:** Sử dụng repeater để thực hành bài tập trên



Kết quả trả về Password: **ONLY\_FOR\_4DM1N5**

**Bài tập 2:** Báo cáo lỗ hổng đang được thực hành.

#Tiêu đề: **Lỗ hổng Broken Access Control - Mất kiểm soát truy cập**

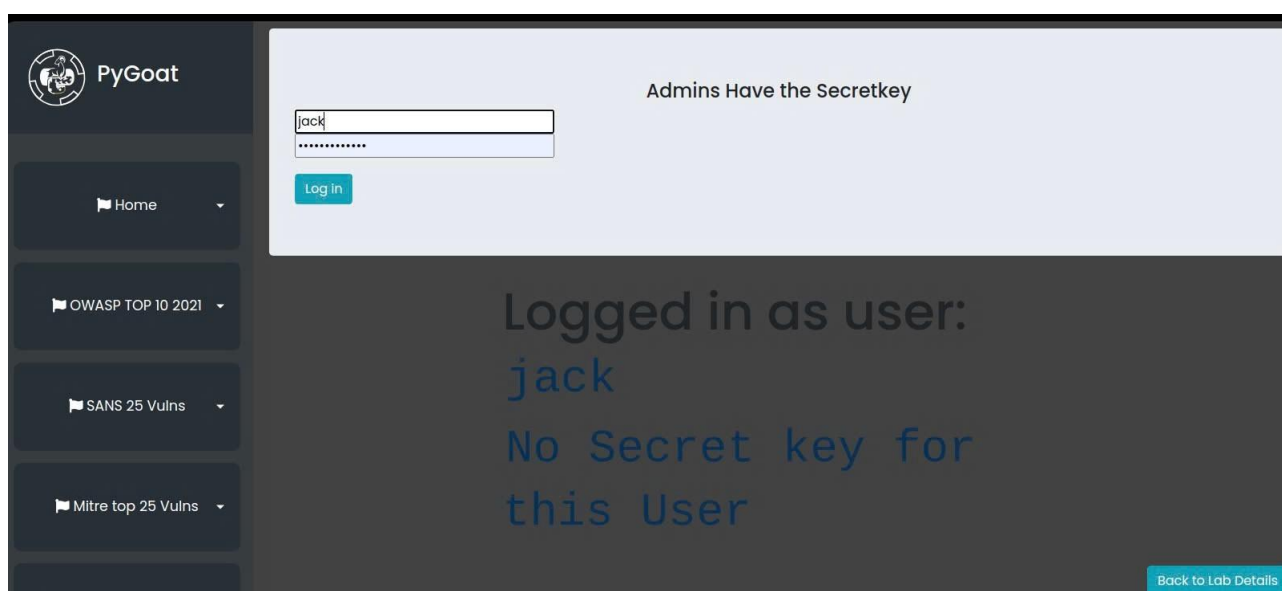
#Mô tả lỗ hổng: Lỗ hổng Broken Access Control xảy ra khi các chính sách kiểm soát truy cập không được thực thi đúng cách, cho phép người dùng thực hiện các hành động

mà họ không được phép. Điều này có thể dẫn đến việc lộ thông tin trái phép, thay đổi dữ liệu hoặc thậm chí phá hủy các tài nguyên quan trọng.

**### Tóm tắt:** Lỗ hổng này xuất hiện khi hệ thống không đảm bảo việc hạn chế quyền truy cập của người dùng một cách chính xác. Những ví dụ phổ biến bao gồm việc cho phép người dùng chỉnh sửa tài khoản người khác, thay đổi URL để truy cập các tài nguyên bị hạn chế, hoặc thực hiện các yêu cầu API không có kiểm soát truy cập thích hợp.

### ### Các bước để thực hiện lại và bằng chứng:

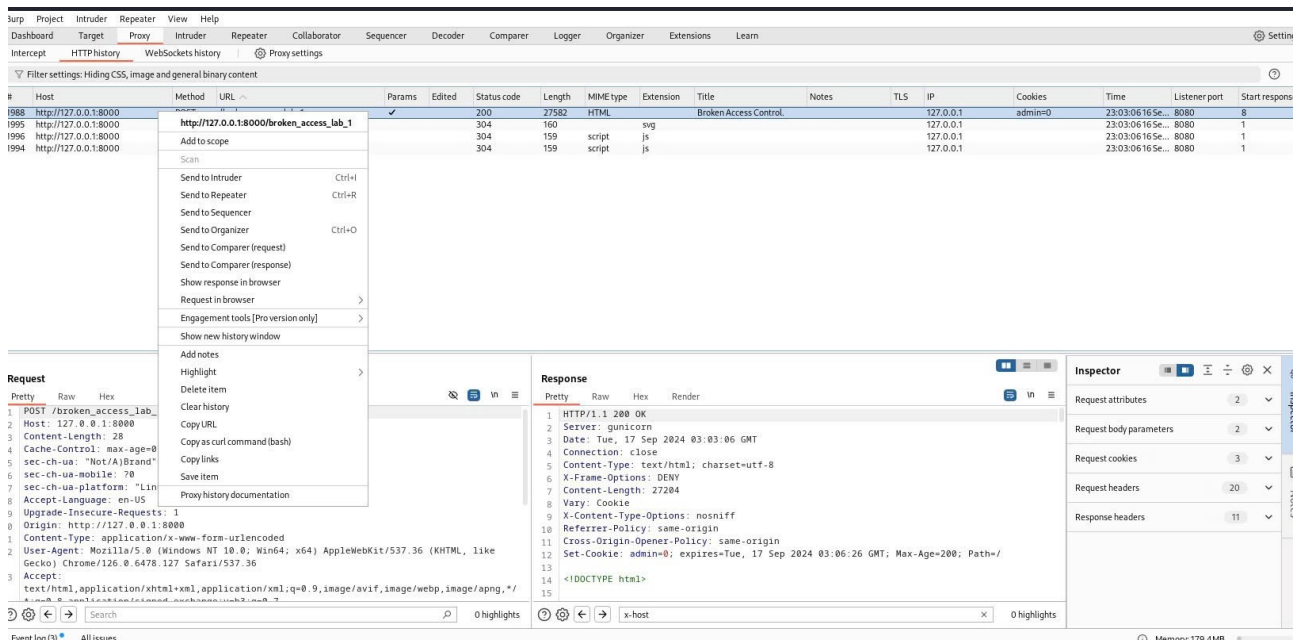
- **Bước 1:** Đăng nhập tài khoản người dùng:



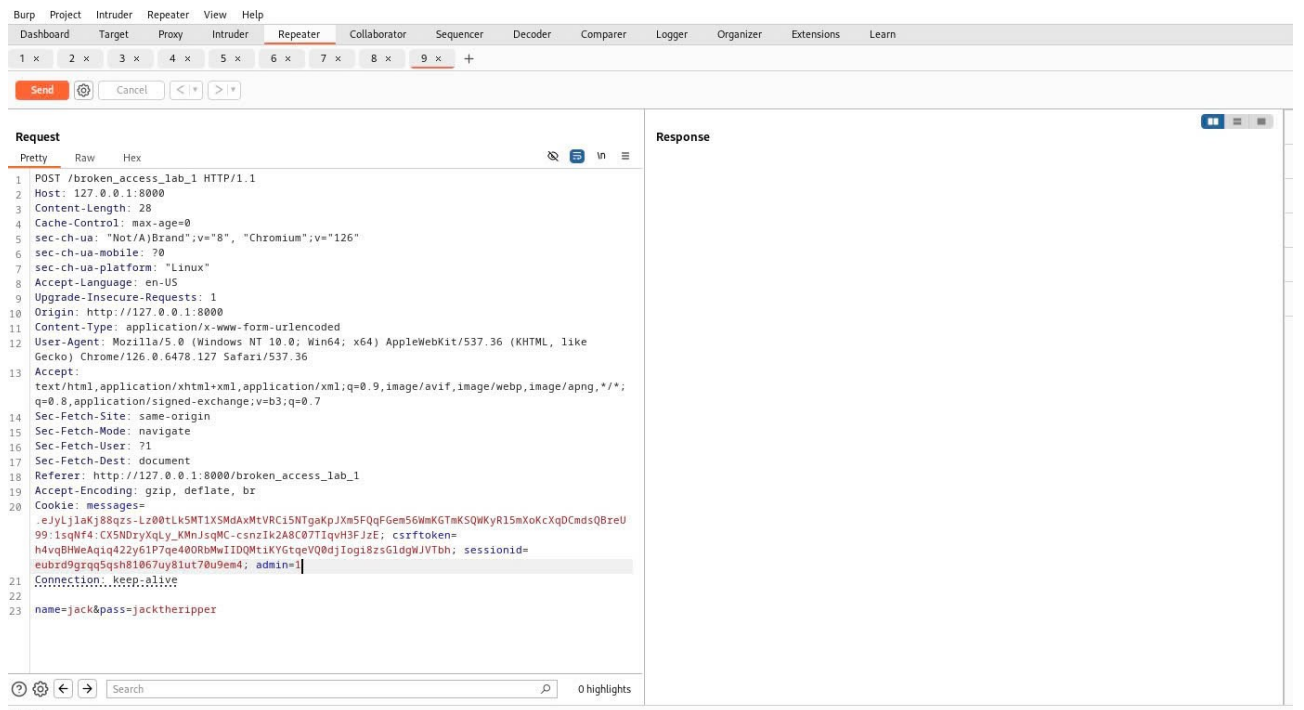
- **Bước 2:** Chọn **Proxy** > **HTTP history** > chuột phải vào tập tin **POST** > **Send to Repeater** :

## Lab 1: Tổng quan các lỗ hổng bảo mật web thường gặp

4

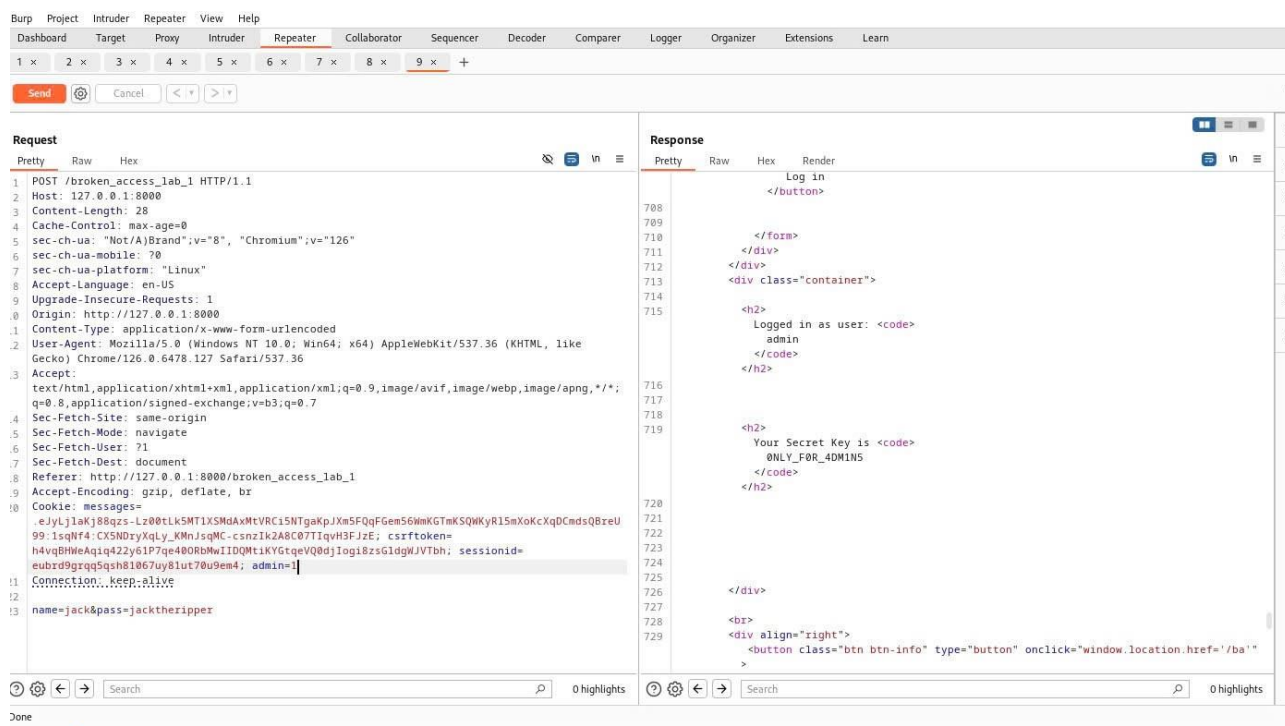


- **Bước 3: Sửa admin = 0 thành admin = 1 rồi chọn Send :**



- **Bước 4: Kết quả trả về password: ONLY\_FOR\_4DM1N5**

## Lab 1: Tổng quan các lỗ hổng bảo mật web thường gặp



**#Mức độ ảnh hưởng của lỗ hổng:** Lỗ hổng này cho phép kẻ tấn công có thể truy cập và thay đổi dữ liệu nhạy cảm, thậm chí chiếm quyền kiểm soát tài khoản người dùng hoặc tài khoản quản trị. Điều này có thể dẫn đến việc rò rỉ dữ liệu, phá hủy tài sản, và làm gián đoạn hoạt động của hệ thống.

### #Khuyến cáo khắc phục:

1. Áp dụng nguyên tắc phân quyền tối thiểu (least privilege), đảm bảo người dùng chỉ có thể thực hiện các hành động mà họ được phép.
2. Sử dụng kiểm tra quyền truy cập ở cả phía máy chủ và phía máy khách, tránh phụ thuộc vào các yếu tố như URL hoặc tham số API.

## b) A02:2021 – Cryptographic Failures

**Bài tập 3:** Báo cáo lỗ hổng đang được thực hành.

**#Tiêu đề: Lỗ hổng Cryptographic Failures - Thất bại trong bảo vệ dữ liệu**

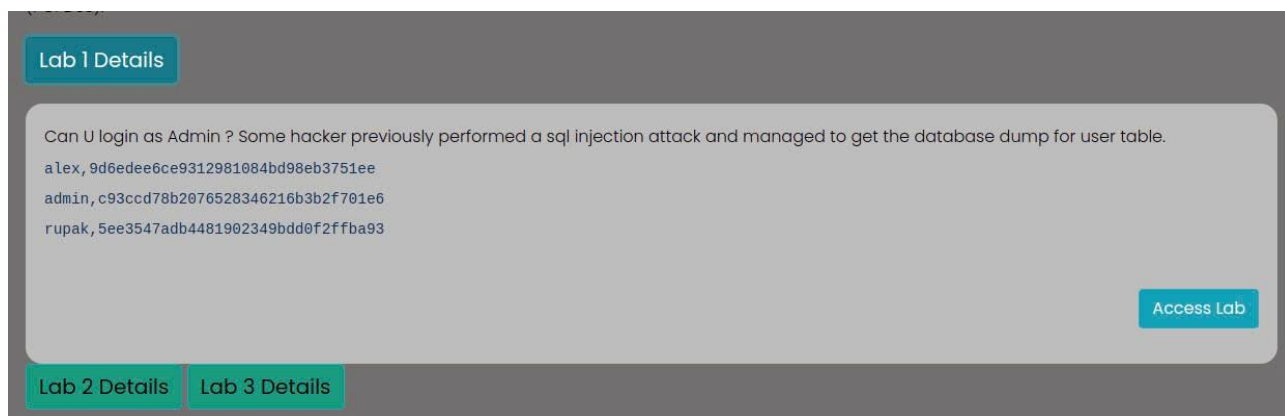
**#Mô tả lỗ hổng:** Lỗ hổng Cryptographic Failures xảy ra khi các cơ chế mã hóa dữ liệu

liệu không được thực thi đúng cách hoặc không được sử dụng đúng mục đích. Điều này có thể dẫn đến việc dữ liệu nhạy cảm bị lộ hoặc không được bảo vệ đầy đủ trước các tấn công. Lỗ hổng này chủ yếu xảy ra khi dữ liệu không được mã hóa, sử dụng thuật toán mã hóa yếu, hoặc quản lý khóa kém.

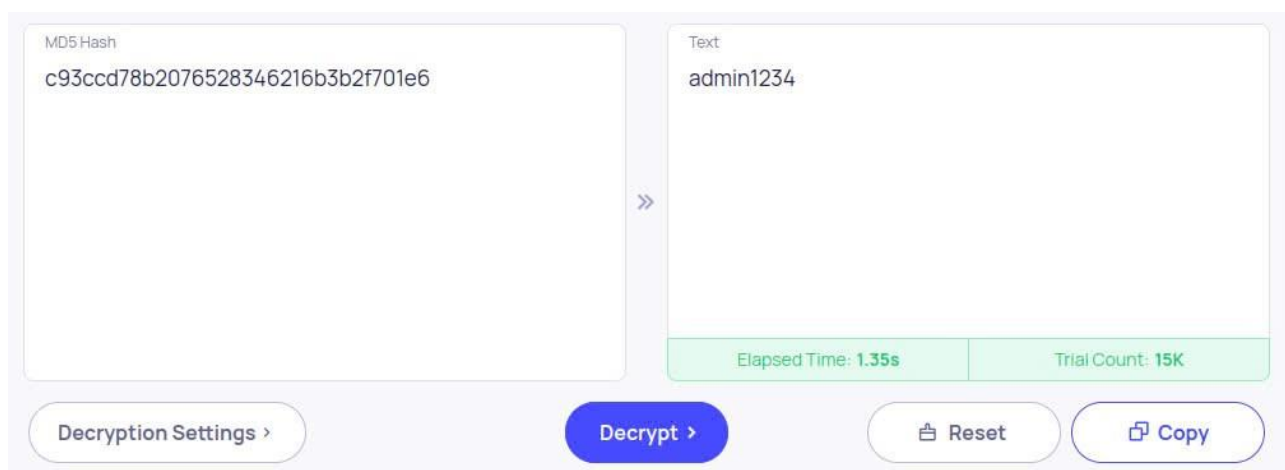
**### Tóm tắt:** Lỗ hổng **Cryptographic Failures** xuất hiện khi các tổ chức hoặc ứng dụng không sử dụng mã hóa hoặc áp dụng mã hóa yếu kém cho dữ liệu nhạy cảm (ví dụ như mật khẩu, thông tin thẻ tín dụng). Ngoài ra, quản lý không đúng cách các khóa mã hóa cũng có thể dẫn đến việc khóa bị lộ hoặc dễ bị tấn công.

### ### Các bước để thực hiện lại và bằng chứng:

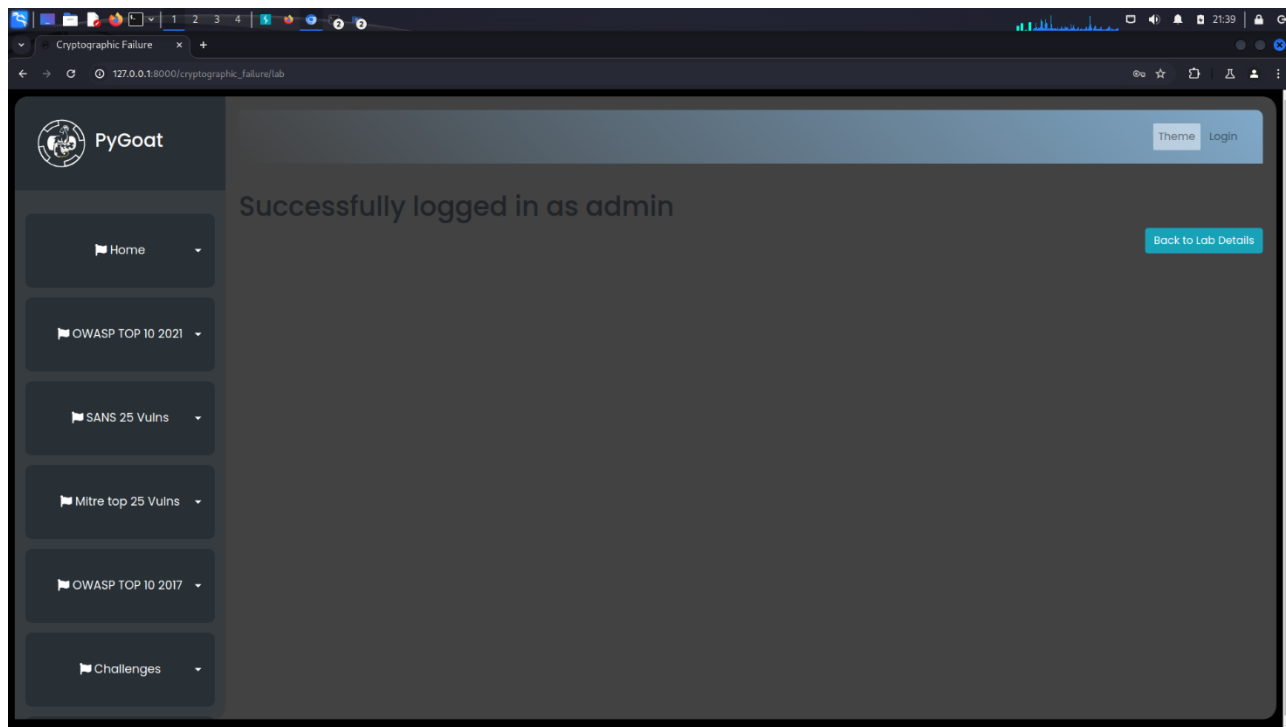
- **Bước 1:** Thông tin **admin** thu thập được từ database:



- **Bước 2:** Tiến hành **decrypt** mã thu được:



- **Bước 3:** Đăng nhập vào tài khoản admin với password: **admin1234** :



**#Mức độ ảnh hưởng:** Lỗ hổng **Cryptographic Failures** có thể dẫn đến việc lộ thông tin nhạy cảm như mật khẩu, thông tin thanh toán hoặc các dữ liệu cá nhân. Nếu không được mã hóa hoặc mã hóa không đủ mạnh, các dữ liệu này dễ dàng bị kẻ tấn công đánh cắp và sử dụng cho các mục đích xấu, gây ra những thiệt hại nghiêm trọng cho cá nhân hoặc tổ chức.

### **#Khuyến cáo khắc phục:**

1. Áp dụng mã hóa mạnh mẽ (như AES-256) cho tất cả các dữ liệu nhạy cảm, cả khi lưu trữ lẫn khi truyền tải.
2. Sử dụng các phương pháp quản lý khóa an toàn, tránh lưu trữ khóa mã hóa cùng vị trí với dữ liệu được mã hóa.

## d) A03:2021 – Injection

**Bài tập 4:** Báo cáo lỗ hổng đang được thực hành.

### #Tiêu đề: **Lỗ hổng Injection - Tấn công qua chèn mã độc**

**#Mô tả lỗ hổng:** Lỗ hổng **Injection** xuất hiện khi một ứng dụng không xử lý đúng các đầu vào từ người dùng, dẫn đến việc kẻ tấn công có thể chèn và thực thi các lệnh hoặc mã độc. Các loại tấn công chèn mã phổ biến bao gồm SQL Injection, Command Injection, và Cross-Site Scripting (XSS). Điều này cho phép kẻ tấn công truy cập trái phép vào cơ sở dữ liệu, sửa đổi hoặc xóa dữ liệu, và thực hiện các hành động độc hại khác.

**### Tóm tắt:** Lỗ hổng **Injection** xảy ra khi đầu vào từ người dùng không được xác thực hoặc xử lý đúng cách, dẫn đến việc chèn mã độc vào các câu lệnh hoặc hệ thống. Ví dụ, SQL Injection cho phép kẻ tấn công thực thi các câu lệnh SQL trái phép trên cơ sở dữ liệu của ứng dụng.

### ### Các bước để thực hiện lại và bằng chứng:

- **Bước 1:** Ta biết được trang web kiểm tra mật khẩu theo cú pháp trong hình:

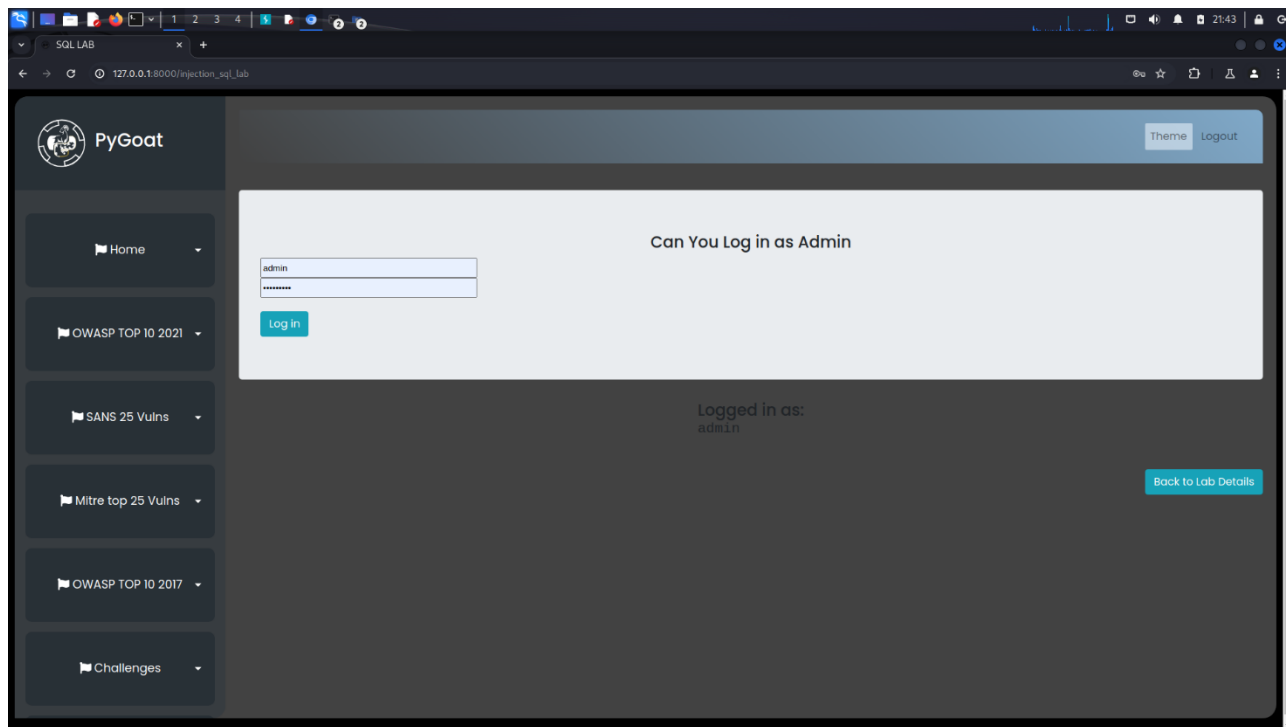
```
When we inserted a ' in the input it threw an error , this is because the sql query was not balanced and it threw an error.  
SELECT * FROM introduction_login WHERE user='admin' AND password=''  
The query quotes in the password field are unbalanced, this can be balanced by adding another quote to it.
```

- **Bước 2:** Sử dụng user name là admin, sử dụng dấu ' để thoát khỏi dòng **password = ''** và sau đó chèn thêm lệnh **or '1 = 1** để kết quả luôn trả về đúng:

```
1 username: admin  
2 password: 1' or '1=1|  
3
```

- **Bước 3:** Sử dụng use name và password đã tạo đăng nhập và thu được kết quả như hình bên dưới:





**#Mức độ ảnh hưởng:** Lỗ hổng **Injection** rất nghiêm trọng vì nó cho phép kẻ tấn công chiếm quyền kiểm soát hoàn toàn cơ sở dữ liệu hoặc hệ thống. Hậu quả có thể bao gồm rò rỉ thông tin nhạy cảm, thay đổi dữ liệu, và gây ra gián đoạn dịch vụ. Với SQL Injection, kẻ tấn công có thể truy cập, chỉnh sửa, hoặc xóa bất kỳ dữ liệu nào trong hệ thống.

### #Khuyến cáo khắc phục:

1. Sử dụng các câu lệnh đã chuẩn bị sẵn (prepared statements) với các tham số truy vấn để tránh việc chèn mã độc.
2. Xác thực và làm sạch đầu vào: Kiểm tra và lọc đầu vào từ người dùng trước khi đưa vào câu lệnh hoặc hệ thống.

### e) A04:2021 – Insecure Design

**Bài tập 5:** Báo cáo lỗ hổng đang được thực hành.

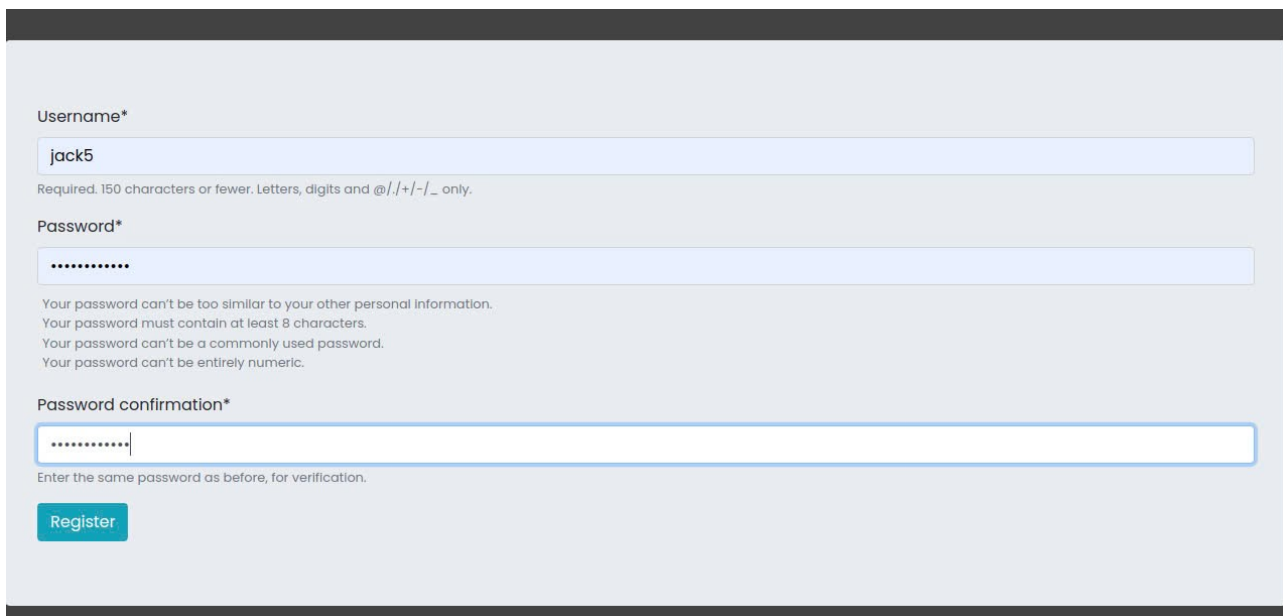
## #Tiêu đề: **Lỗ hổng Insecure Design - Thiết kế không an toàn**

**#Mô tả lỗ hổng:** Lỗ hổng **Insecure Design** xảy ra khi một hệ thống hoặc ứng dụng được thiết kế mà không tính đến các khía cạnh bảo mật hoặc không có các biện pháp phòng ngừa đối với các nguy cơ bảo mật tiềm ẩn. Lỗ hổng này thường là kết quả của việc thiếu kiểm tra bảo mật trong quá trình phát triển hoặc thiết kế hệ thống không có các biện pháp bảo mật cơ bản.

**### Tóm tắt:** Lỗ hổng **Insecure Design** không chỉ do lập trình sai mà còn liên quan đến các quyết định không an toàn trong quá trình thiết kế kiến trúc hệ thống. Ví dụ, hệ thống không có các quy trình xác thực chặt chẽ, không phân quyền rõ ràng, hoặc không xây dựng theo các tiêu chuẩn an toàn bảo mật.

### ### Các bước để thực hiện lại và bằng chứng:

**- Bước 1:** Tạo 12 tài khoản để đăng nhập vào lấy 60 ticket.

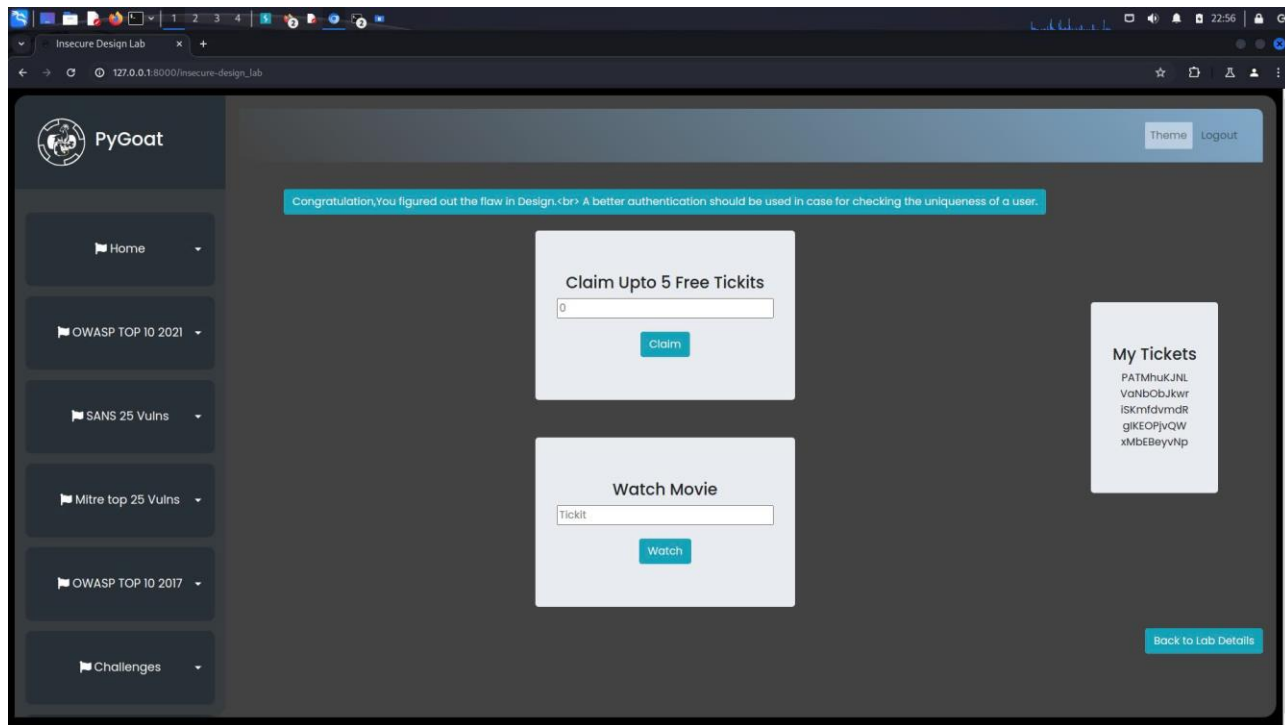


The screenshot shows a registration form with the following fields and labels:

- Username\***: Input field containing "jack5". Below it, a note reads: "Required. 150 characters or fewer. Letters, digits and @/./+/-/\_ only."
- Password\***: Input field with masked characters. Below it, a note lists password requirements: "Your password can't be too similar to your other personal information. Your password must contain at least 8 characters. Your password can't be a commonly used password. Your password can't be entirely numeric."
- Password confirmation\***: Input field with masked characters. Below it, a note reads: "Enter the same password as before, for verification."
- Register**: A blue button at the bottom of the form.

**- Bước 2:** Sau khi thực hiện lấy hết ticket thì tiến hành xem phim, kết quả bên dưới :

## Lab 1: Tổng quan các lỗ hổng bảo mật web thường gặp



**#Mức độ ảnh hưởng của lỗ hổng:** Lỗ hổng **Insecure Design** có thể dẫn đến các vấn đề nghiêm trọng về bảo mật như lộ thông tin, truy cập trái phép hoặc thậm chí chiếm quyền điều khiển hệ thống. Các hệ thống thiếu thiết kế bảo mật dễ bị tấn công từ nhiều phương diện, bao gồm tấn công brute force, SQL injection, hay khai thác các chức năng không được bảo vệ đúng cách.

### #Khuyến cáo khắc phục:

1. Áp dụng các nguyên tắc thiết kế an toàn: Tích hợp bảo mật ngay từ giai đoạn thiết kế, bao gồm quy trình phân quyền, xác thực mạnh mẽ, và quản lý phiên làm việc an toàn.
2. Thực hiện kiểm tra thiết kế định kỳ: Đánh giá và kiểm tra lại các thành phần kiến trúc của hệ thống để phát hiện và loại bỏ các thiết kế không an toàn.

## f) A05:2021 – Security Misconfiguration

**Bài tập 6:** Báo cáo lỗ hổng đang được thực hành.

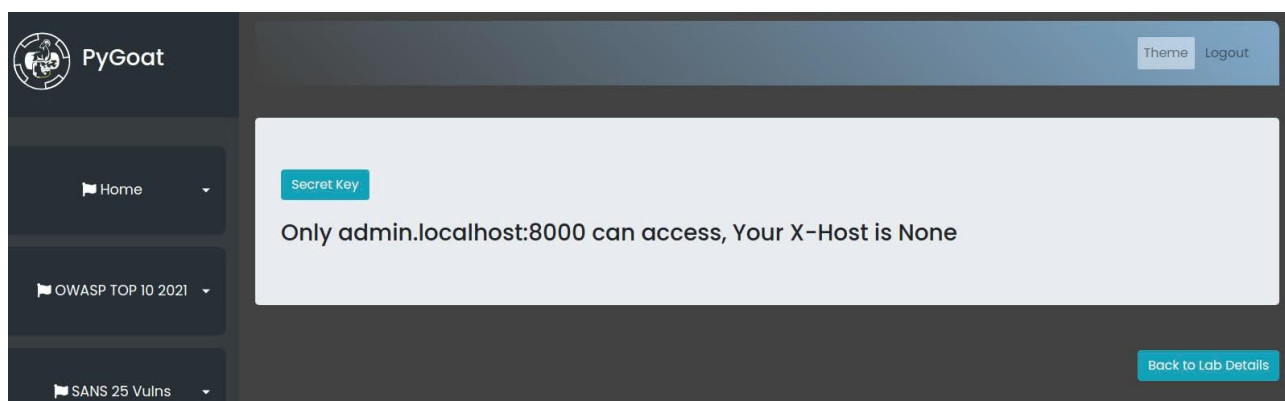
**#Tiêu đề:** Lỗ hổng Security Misconfiguration - Cấu hình bảo mật sai

**#Mô tả lỗ hổng:** Lỗ hổng **Security Misconfiguration** xảy ra khi hệ thống hoặc ứng dụng không được cấu hình bảo mật một cách chính xác, hoặc sử dụng các cấu hình mặc định, dễ bị tấn công. Lỗi này có thể phát sinh từ việc thiếu cập nhật phần mềm, sử dụng quyền truy cập không cần thiết, hoặc cấu hình dịch vụ mà không tuân theo các thực hành bảo mật tốt nhất.

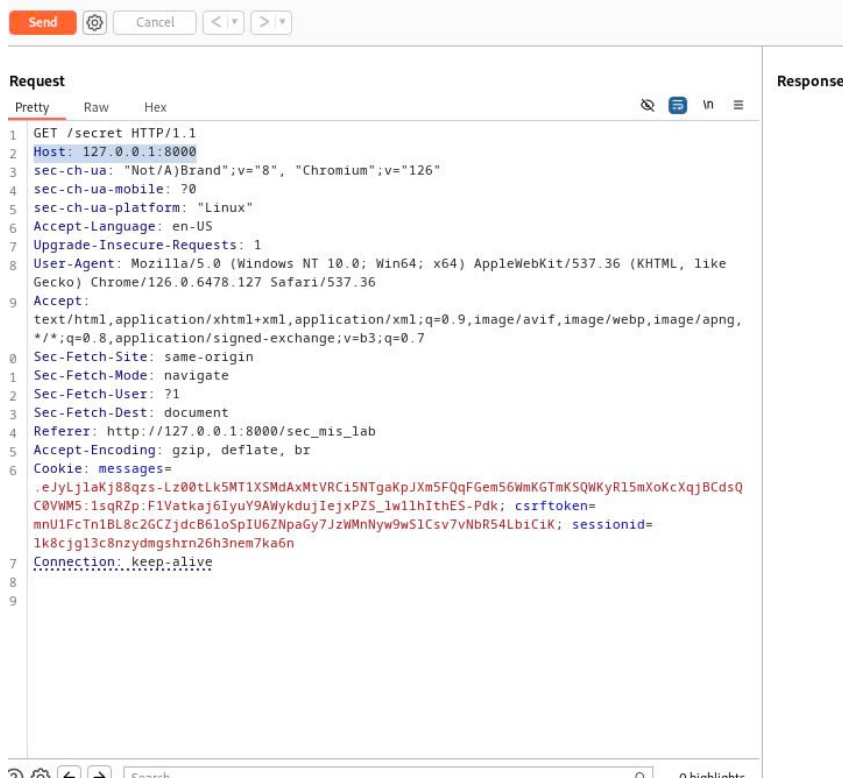
**### Tóm tắt:** Lỗ hổng **Security Misconfiguration** xuất hiện khi các quản trị viên hệ thống không thay đổi các thiết lập mặc định hoặc vô tình để lộ thông tin nhạy cảm như thông báo lỗi chi tiết. Một số ví dụ khác bao gồm vô hiệu hóa các tính năng hoặc quyền không cần thiết, để các cổng dịch vụ mở hoặc không đặt mật khẩu mạnh

### ### Các bước để thực hiện lại và bằng chứng:

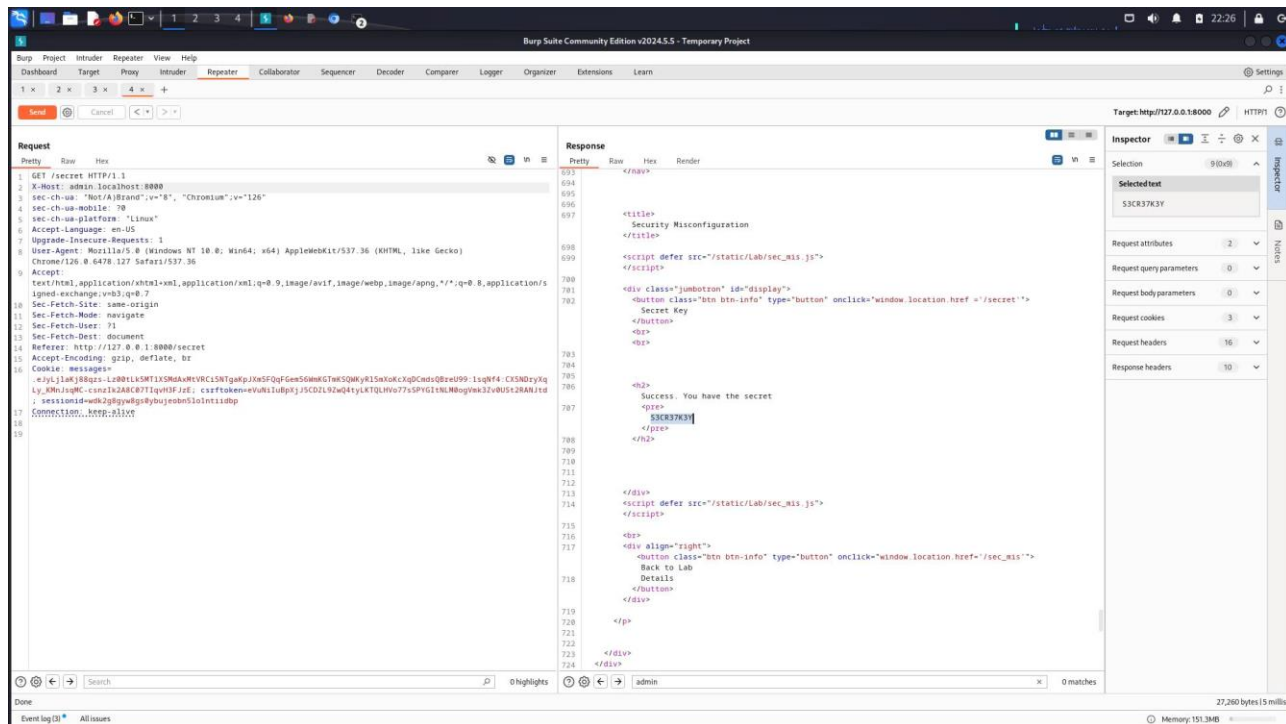
- **Bước 1:** Từ kết quả thu được ta nhận thấy rằng X-Host phải có giá trị là admin.localhost:8000 thì mới xem được khoá bí mật:



- **Bước 2:** Sử dụng công cụ Burp Suite để proxy, nhận thấy trường dữ liệu ta có là host: 127.0.0.1:8000, ta thay bằng X-Host: admin.localhost:8000 và gửi :



- **Bước 3:** Kết quả được hiển thị bên phần Response password: **S3CR37K3Y** :



**#Mức độ ảnh hưởng của lỗ hổng:** Lỗ hổng **Security Misconfiguration** cho phép kẻ tấn công khai thác các thiết lập không an toàn hoặc các cấu hình mặc định để truy cập trái phép vào hệ thống. Điều này có thể dẫn đến việc rò rỉ dữ liệu, xâm nhập trái phép, hoặc thực hiện các hành động phá hoại như thay đổi cấu hình hệ thống hoặc chiếm quyền kiểm soát toàn bộ hệ thống.

### **#Khuyến cáo khắc phục:**

1. Thực hiện các thực hành bảo mật tốt nhất: Cấu hình hệ thống và ứng dụng theo các khuyến nghị an toàn bảo mật, vô hiệu hóa các tính năng và dịch vụ không cần thiết.
2. Thay đổi tất cả các thiết lập mặc định: Đặt mật khẩu mạnh và thay đổi thông tin xác thực mặc định ngay sau khi triển khai hệ thống.

---

*Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này*

HẾT