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: Ngô Khánh Khoa

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.O21.ANTN

STT	Họ và tên	MSSV	Email
1	Hà Thị Thu Hiền	21522056	21522056@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

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.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. A1: Broken Access Control

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

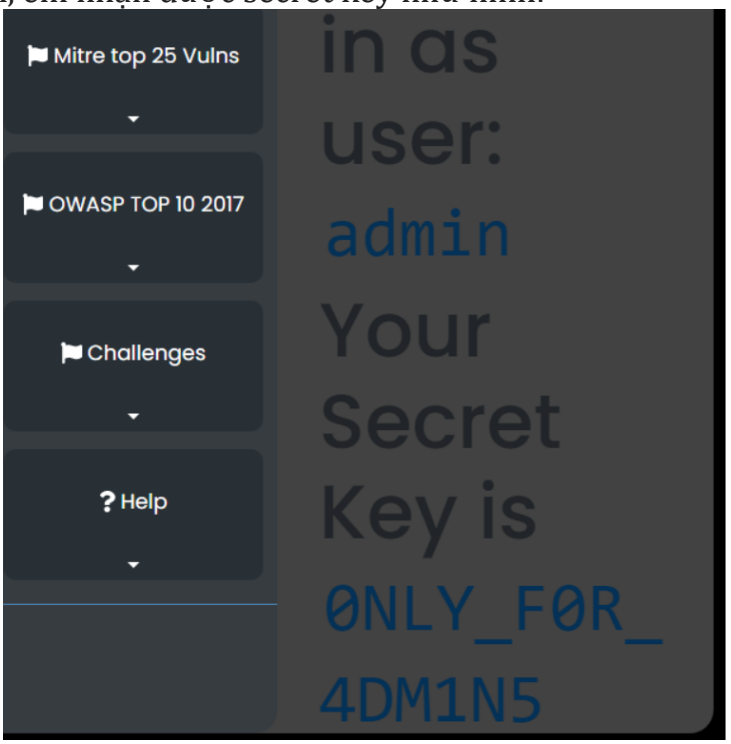
- Tại tab Repeater, em sẽ sửa giá trị thành "admin=1" trong cookie để gửi lên server với tư cách là admin:

Request

Pretty Raw Hex

```
1  POST /broken_access_lab_1 HTTP/1.1
2  Host: localhost:8000
3  Content-Length: 28
4  Cache-Control: max-age=0
5  sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
6  sec-ch-ua-mobile: ?0
7  sec-ch-ua-platform: "Windows"
8  Upgrade-Insecure-Requests: 1
9  Origin: http://localhost:8000
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
   Gecko) Chrome/110.0.5481.178 Safari/537.36
12 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
   g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:8000/broken_access_lab_1
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: csrftoken=e6YXxdEYTq8vNkMPuohadlpAx5yK6qYQTUWYqYKJ8phFlNobt2RJFtgeaFRlFxjf;
   sessionid=70yzvscohzbn5ubm7la3pykl3ey4z6af; admin=1
21 Connection: close
22
23 name=jack&pass=jacktheripper
```

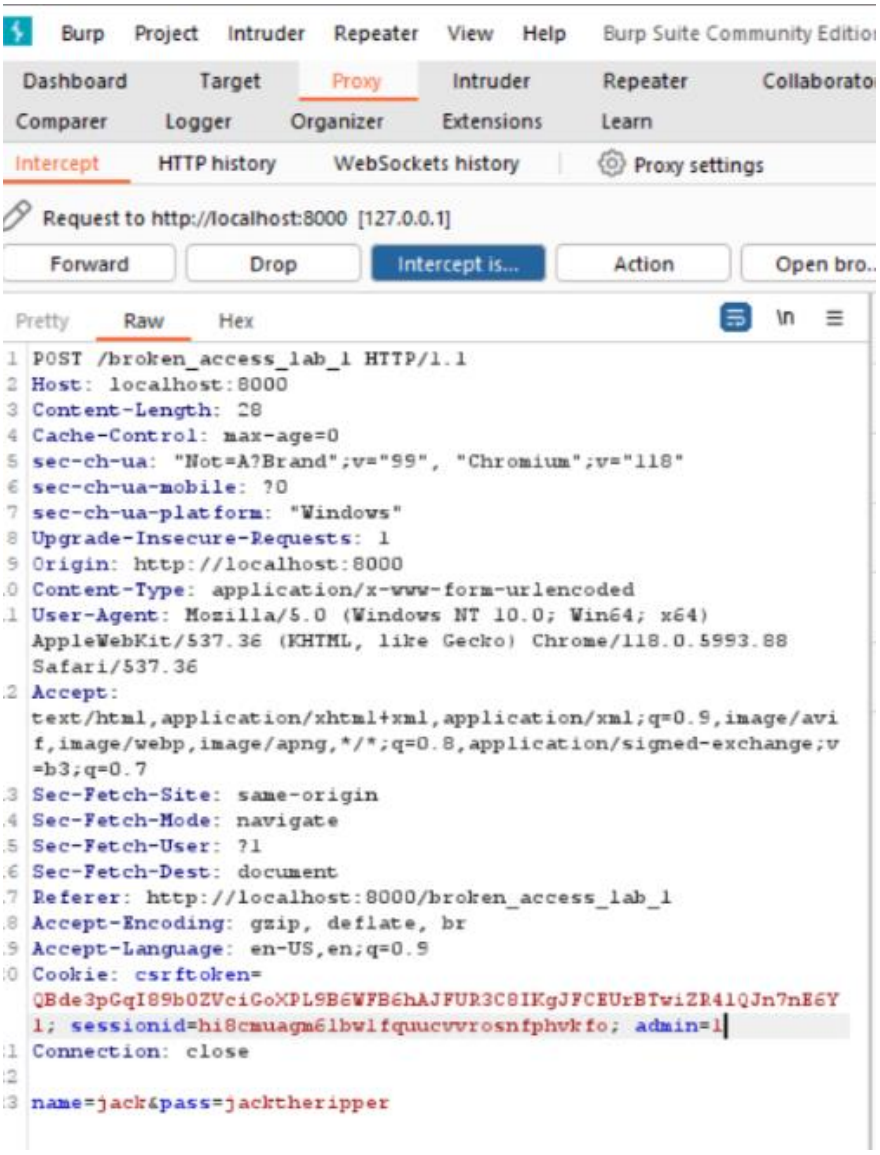
- Gửi gói tin đi, em nhận được secret key như hình:



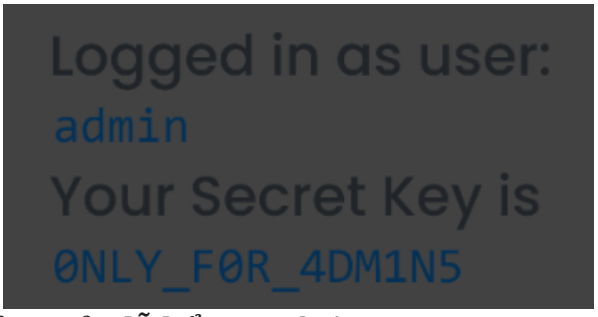
Bài tập 2: Báo cáo lỗ hổng đang được thực hành. Có thể sử dụng format theo mẫu sau:

- **Tiêu đề:** Lỗ hổng Broken Access Control tiết lộ thông tin nhạy cảm.
- **Mô tả lỗ hổng:** Đây là lỗ hổng phân quyền, cho phép người dùng bình thường có thể đăng nhập, có quyền hạn như một quản trị viên.
- **Các bước thực hiện khai thác :**
  Thay đổi giá trị admin từ 0 thành 1 để chiếm quyền quản trị viên.

  Bước 1: Bật Intercep để chặn gói tin và thay đổi giá trị **admin=0** thành **admin=1**.



Bước 2: Send request:



- **Mức độ ảnh hưởng của lỗ hổng:** Nghiêm trọng
- **Khuyến cáo khắc phục:**
  1. Lưu role của account ở database, sao cho khi user đăng nhập, sẽ dựa vào account đó tham chiếu vào database mà xác định role tướng ứng của user là normal user hay admin.
  2. Tạo ra một chuỗi random. Có sử dụng kỹ thuật băm để lưu trữ dữ liệu.
  3. JWT tokens nên vô hiệu hóa trên server khi đăng xuất.
  4. Nên cài đặt các rule ở Model để quản lý các thao tác với database.

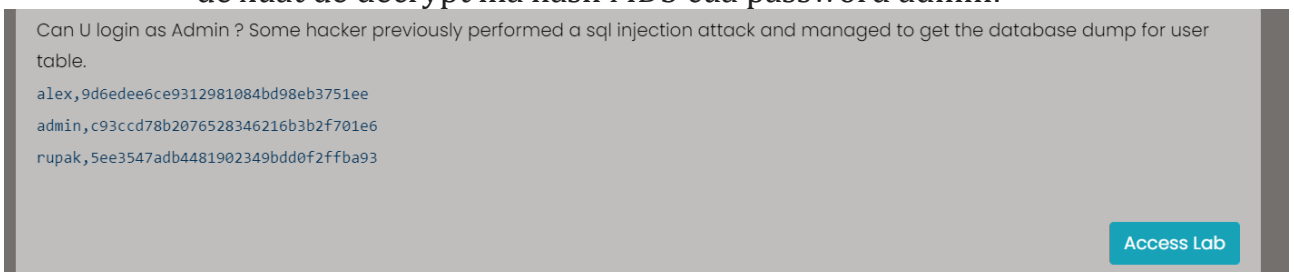
2. A02:2021 – Cryptographic Failures

Bài tập 3: Báo cáo lỗ hổng vừa được thực hành:

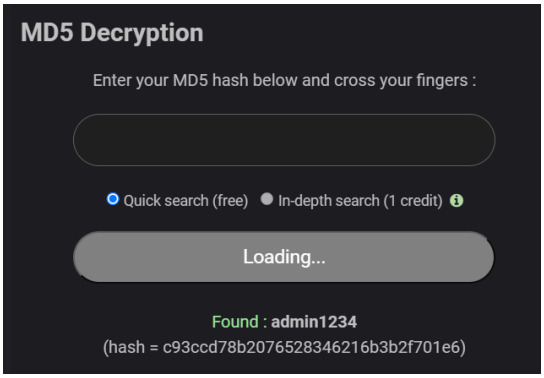
- **Tiêu đề:** Cryptographic Failures gây lộ dữ liệu ngay cả khi lưu trữ và truyền tải dữ liệu.
- **Mô tả lỗ hổng:** Đây là lổ hỏng bảo mật của việc mã hóa dữ liệu lưu trữ, dùng kỹ thuật hash đã lỗi thời, dễ bị decrypt.
- **Các bước thực hiện khai thác :**

Ta có được các thông tin mà đề bài cung cấp, nhận thấy đó là usernam và password đã được hash bằng MD5. Ta tiến hành như sau

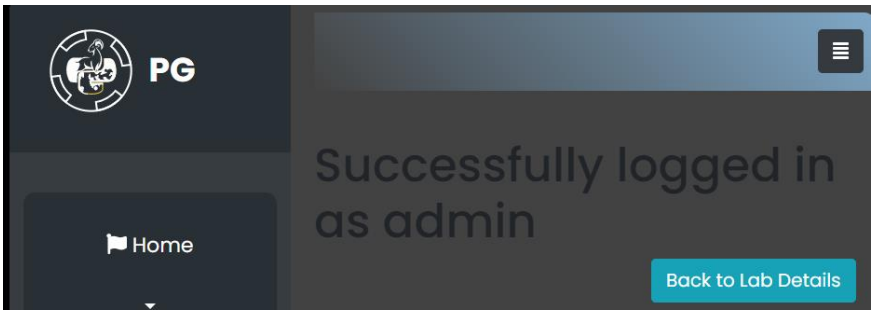
Bước 1: Dùng *https://www.md5online.org/md5-decrypt.html* là tool đề bài đề xuất để decrypt mã hash MD5 của password admin:



Bước 2: Sau khi giải mã:



Bước 3: Đăng nhập với user là **admin** và pass là **admin1234**:

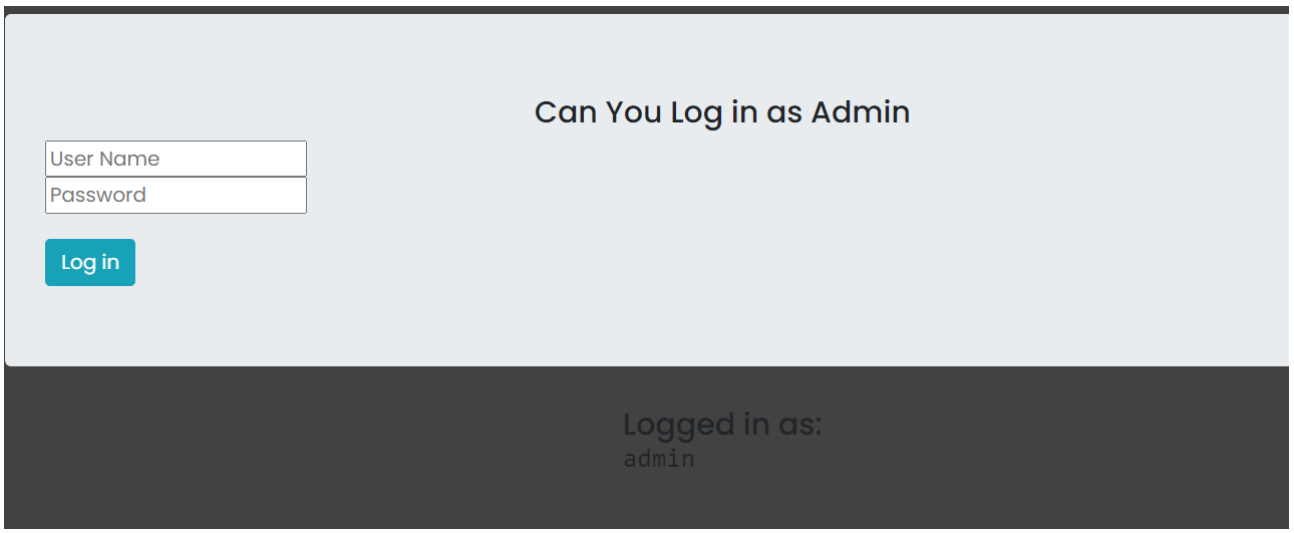


- **Mức độ ảnh hưởng của lỗ hổng:** Nghiêm trọng, đứng top 2
- **Khuyến cáo khắc phục:**
  Thường xuyên bảo trì, cập nhật code. Dùng kĩ thuật mã hóa an toàn như sha256, sha512 thay vì md5, tuân thủ quy trình phát triển an toàn. Mã hóa dữ liệu trên đường truyền bằng TLS, HTTPS.

3. A03:2021 – Injection

Bài tập 4: Báo cáo lỗ hổng vừa được thực hành:

- **Tiêu đề:** Injection – Sql Injection
- **Mô tả lỗ hổng:** Đây là lỗ hổng cho phép attacker có thể không cần biết thông tin account mà vẫn có thể đăng nhập được, vì lợi dụng sự không kiểm tra dữ liệu người dùng nhập vào, nên attacker có thể sử dụng câu truy vấn để "len lỏi" vào hệ thống.
- **Các bước thực hiện khai thác :**
  Bước 1: Đăng nhập với username là admin, password là **anything' OR '1' ='1** , nhận được thông báo như sau:



Bước 2: Password trên bypass được là vì có chứa '1'='1' là điều kiện luôn đúng, nên dù có nhập pass như thế nào, thì vẫn nhận được kết quả đăng nhập thành công với username là **admin.**

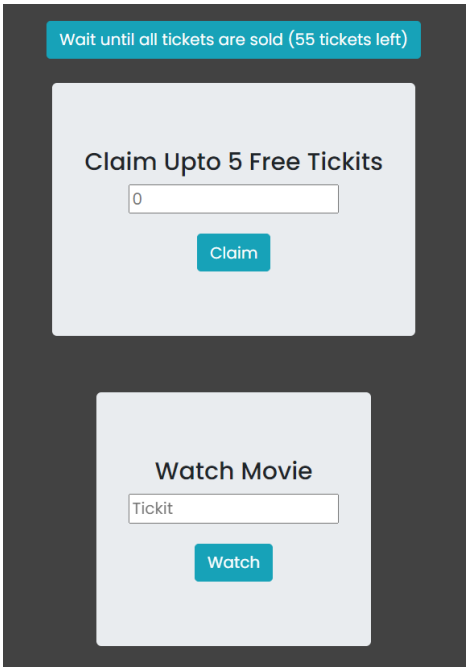
- **Mức độ ảnh hưởng của lỗ hổng:** Nghiêm trọng
- **Khuyến cáo khắc phục:**
  1. Dùng framework an toàn, được update thường xuyên.
  2. Lọc các kí tự đặc biệt thường dùng trong các cuộc tấn công SQL Injection.
  3. Thiết lập rule rõ ràng cho từng account.
  4. Sử dụng các công cụ quét lỗ hổng bảo mật.

4. A04:2021 – Insecure Design

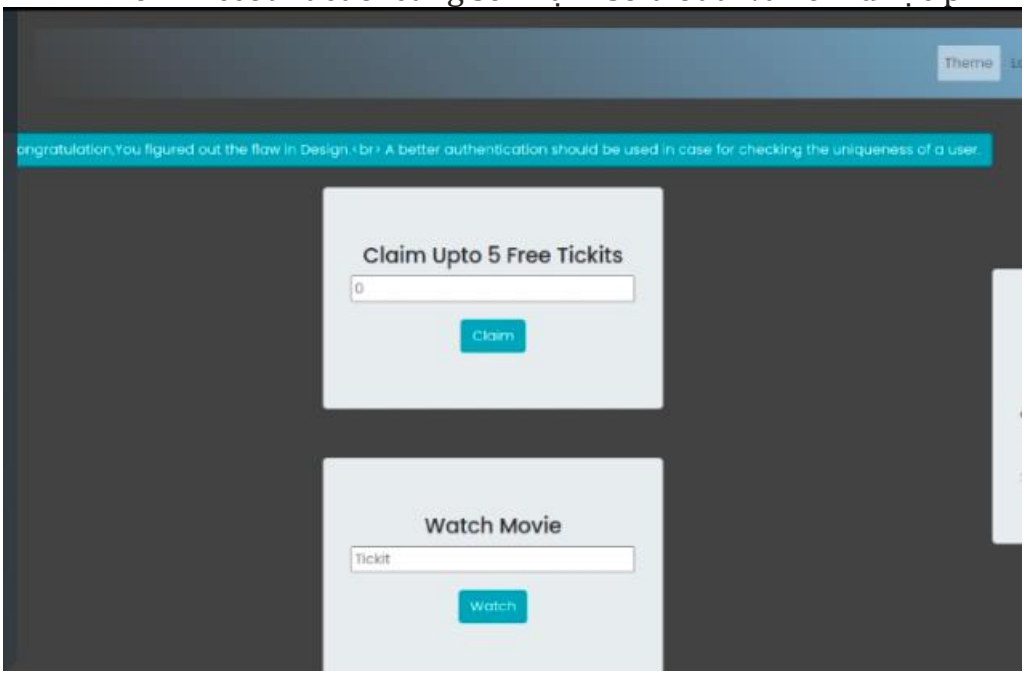
Bài tập 5: Báo cáo lỗ hổng vừa được thực hành:

- **Tiêu đề:** Insecure Design
- **Mô tả lỗ hổng:** Đây là lỗ hỏng vì nó không kiểm tra liệu một user có tạo nhiều account hay không. Nếu 1 người tạo nhiều acc và mỗi acc lấy 5 vé thì chắc chắn người đó sẽ xem được phim miễn phí, trong khi các vé được đặt chưa hẳn là người đó sẽ đến rạp để nhận và thanh toán phí mua vé.
- **Các bước thực hiện khai thác :**

  Bước 1: Tạo 12 accounts, mỗi account lấy 5 vé:



Bước 2: Account cuối cùng sẽ nhận "sold out" và xem được phim free:



- **Mức độ ảnh hưởng của lỗ hổng:** Nghiêm trọng.
- **Khuyến cáo khắc phục:**
  1. Khi đăng ký tài khoản cần xác thực thông tin đinh danh duy nhất như: dùng CCCD, CMND, vân tay, khuôn mặt,... để đảm bảo 1 user chỉ được đăng ký 1 account
  2. Block account ảo và thu hồi, vô hiệu hóa các tài nguyên mà account đó đã chiếm được. Hoặc giới hạn số lượng vé cho những tài khoản mới tạo, cần xác thực số điện thoại => 1 số điện thoại chỉ được tạo 1 account.

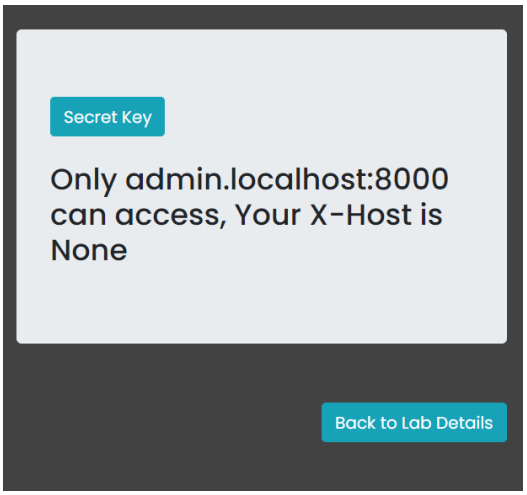
3. Kiểm tra lại tính login của chương trình, trình tự thực thi các bước từ đặt vé đến thanh toán đã hợp lý chưa, có sơ hở nào không?

5.A05:2021 – Security Misconfiguration

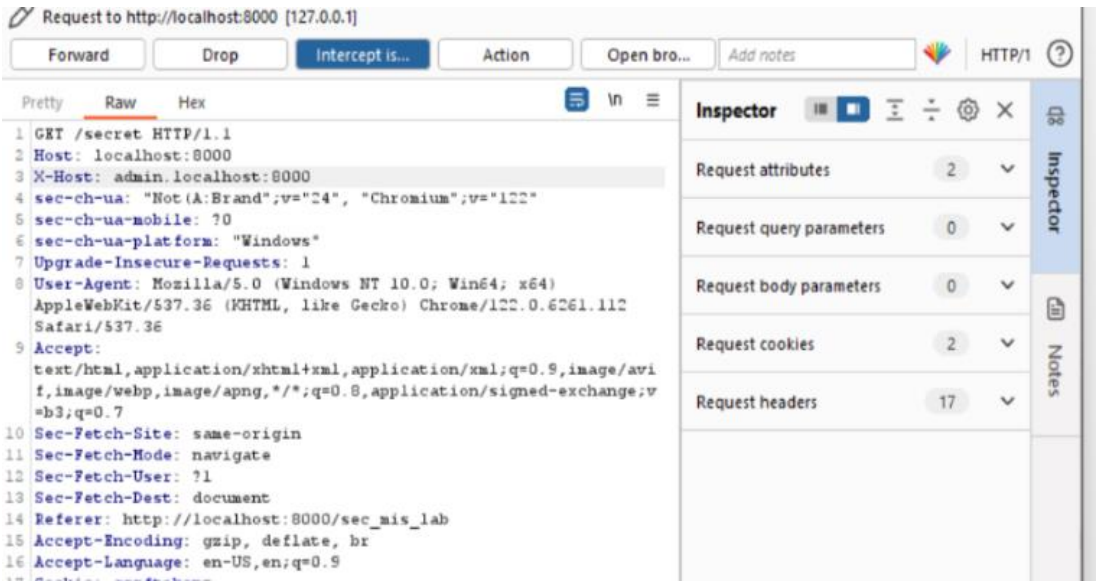
Bài tập 6: Báo cáo lỗ hổng vừa được thực hành:

- **Tiêu đề:** Security Misconfiguration
- **Mô tả lỗ hổng:** Đây là lỗ hổng về vấn đề thông báo lỗi nhưng kèm theo nhiều thông tin không cần thiết cho user thấy, từ đó user với mục đích xấu sẽ lợi dụng để khai thác chương trình.
- **Các bước thực hiện khai thác :**

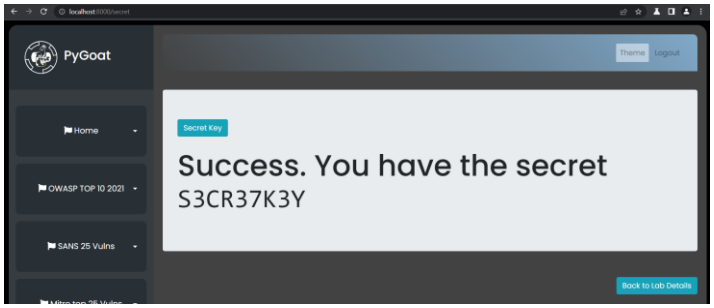
Bước 1: Access lab và nhận kết quả như hình:



Bước 2: Như thông báo hiển thị, đòi hỏi phải đăng nhập với tư cách admin. Thấy trường X-Host cũng được show ra luôn. Do đó em sẽ sử dụng Intercep để chặn gói tin, thay đổi nội dung và gửi lại lên server với X-Host là admin.localhost:8000 để được server chấp nhận**:**



Bước 3: Gửi lại request đã thêm header trên, ta có được secret key:



- **Mức độ ảnh hưởng của lỗ hổng:** nghiêm trọng.
- **Khuyến cáo khắc phục:**
  1. Loại bỏ những nội dung không cần thiết, kiểm soát nội dung sẽ hiển thị với user.
  2. Không dùng các trường header để xác định quyền của một request user.
  3. Thiết kế một cách an toàn và chặt chẽ

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

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

  *Ví dụ: [*NT101.K11.ANTT*]-Exe01_Group03.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT