Phòng thí nghiệm An toàn Thông tin
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật Web và Ứng dụng

Kỳ báo cáo: Buổi 01 (Session 01)

Tên chủ đề: Tổng quan các lỗ hổng bảo mật web thường gặp

GVHD: Ngô Đức Hoàng Sơn

Ngày báo cáo: 20/03/2024

Nhóm: 09

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.O22.ATCL.2

STT	Họ và tên	MSSV	Email
1	Hồ Ngọc Thiện	21522620	21522620@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Kịch bản 01	100%
2	Kịch bản 02	100%
3	Kịch bản 03	100%
4	Kịch bản 04	90%
5	Kịch bản 05	60%

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. Kịch bản 01

Tiêu đề: Broken Access Control. Tài sản bị ảnh hưởng: thông tin, dữ liệu

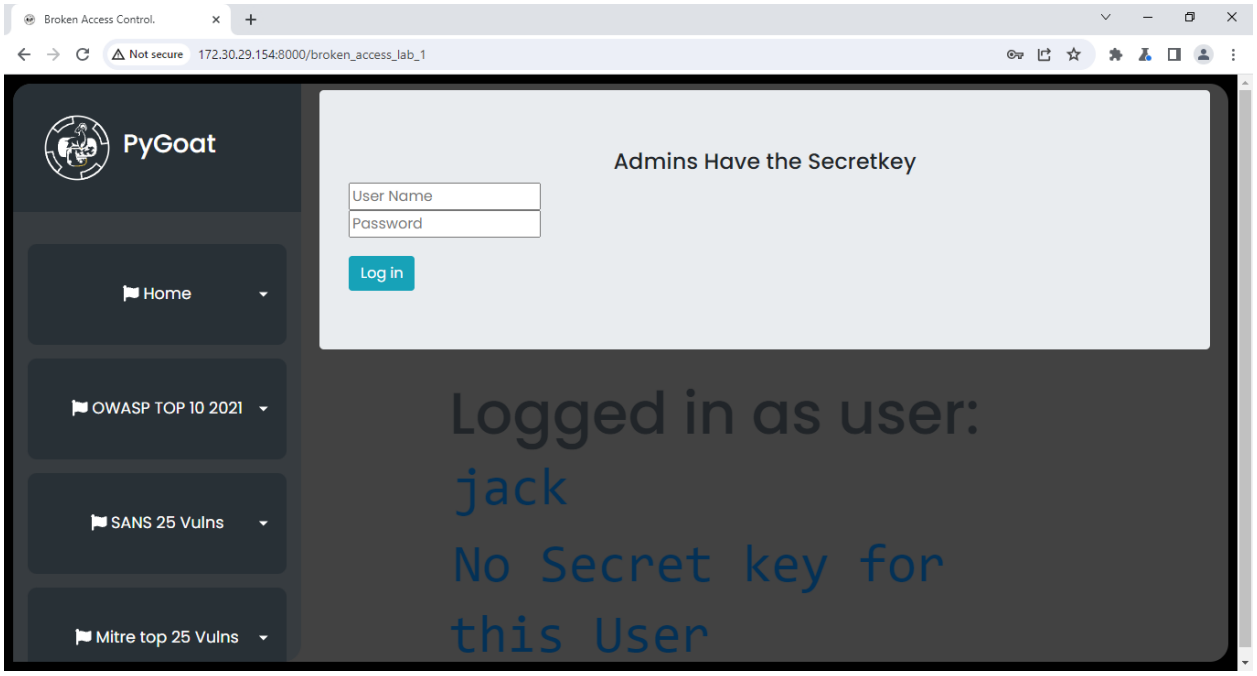
Mô tả lỗ hổng:

Khi dùng repeater để gửi thông tin login lên trang web, attacker có thể sửa đổi các yêu cầu gửi thông tin login bằng cách thay đổi các tham số, điều này có thể bao gồm việc thay đổi các giá trị của các trường người dùng và mật khẩu trong yêu cầu. Điều này có thể cho phép attacker truy cập vào hệ thống mà không cần có thông tin đăng nhập chính xác, hoặc thậm chí chiếm quyền truy cập vào các tài khoản có đặc quyền mà họ không được phép truy cập.

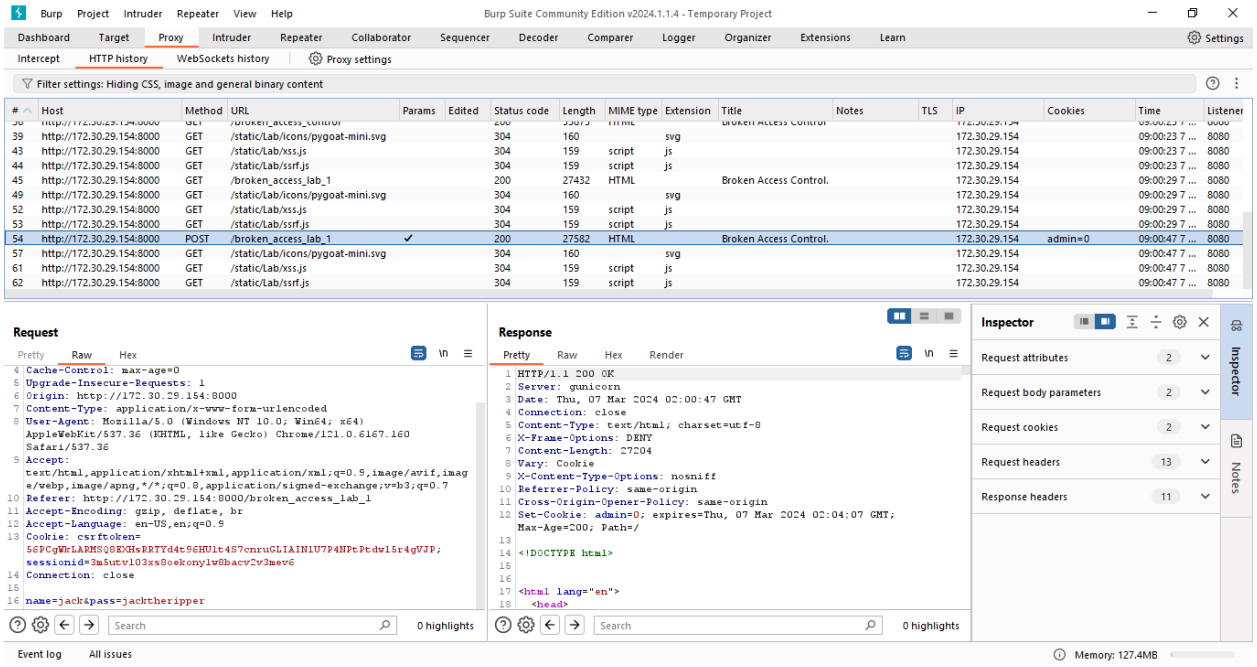
Các bước thực hiện:

Bước 1: Truy cập bài thực hành tại http://localhost:8000 => OSWAP TOP 10 2021 => A1: Broken Access Control => Lab 1 Details

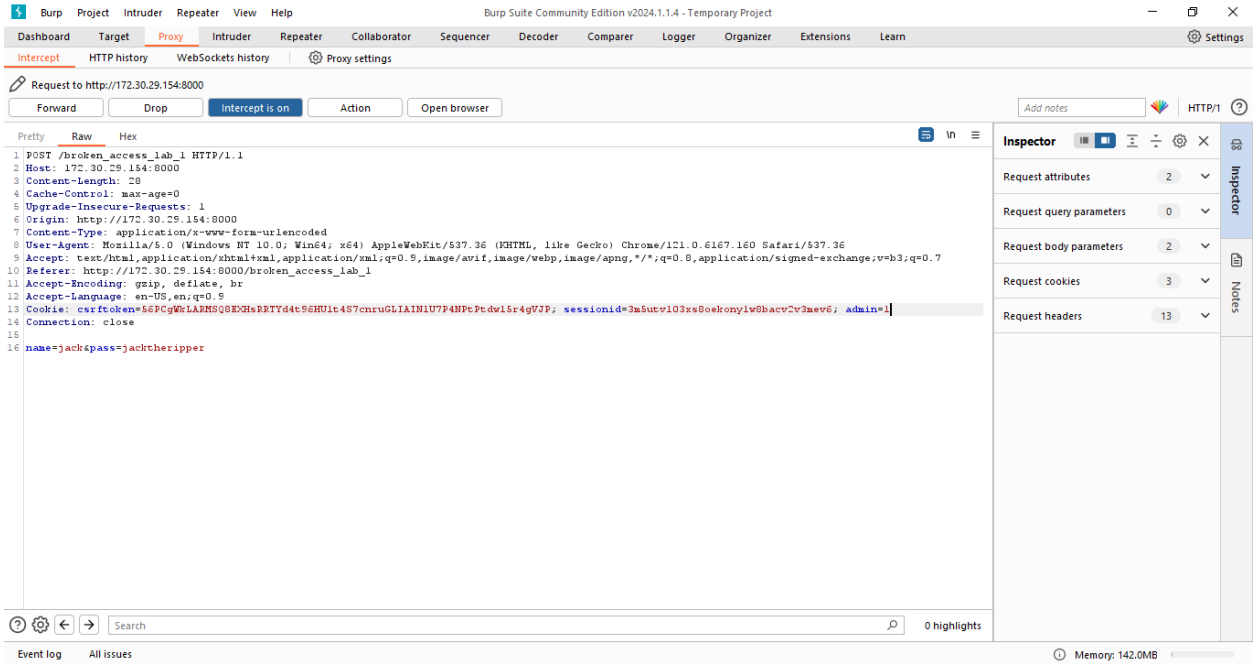
Bước 2: Đăng nhập vào trang web với tài khoản và mật khẩu được cung cấp của user Jack

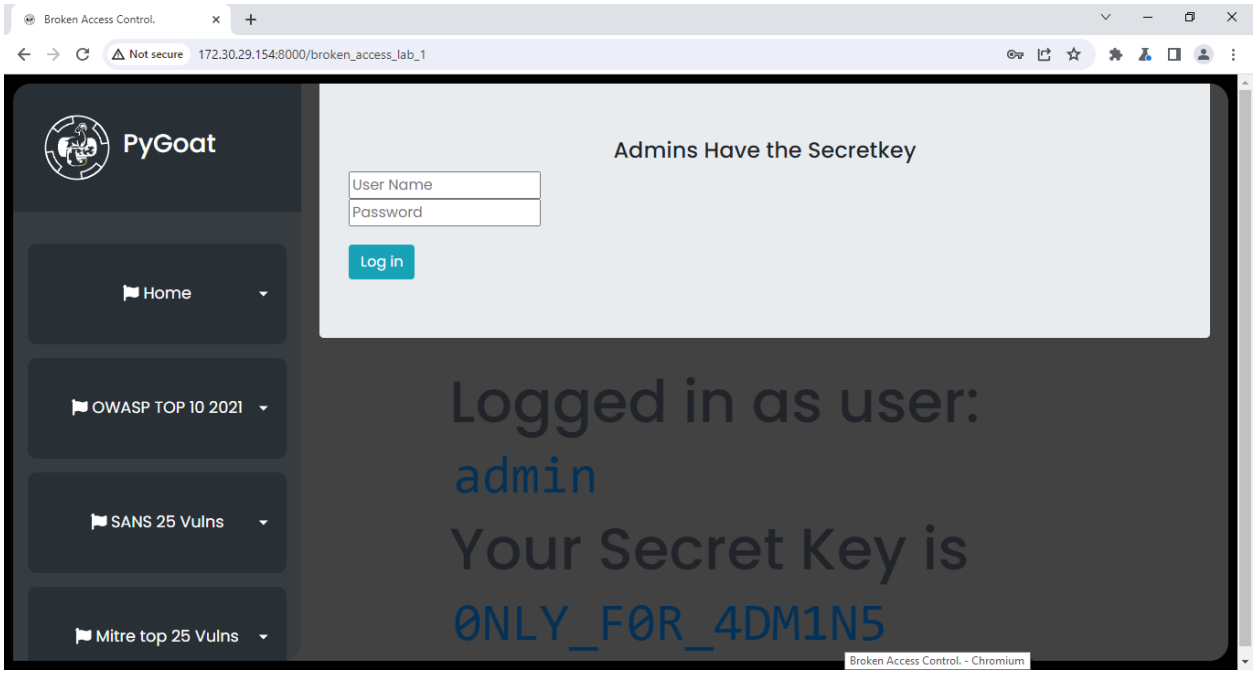


Bước 3: Trở lại giao diện HTTP history của Burpsuite để kiểm tra lịch sử câu truy vấn để hiểu rõ logic của ứng dụng.



Sau đó thực hiện chuyển đến repeater và thay đổi bằng thêm trường admin=1 vào phần cookie vào gửi lên server lại.





Key: 0NLY_F0R_4DM1N5

Mức độ ảnh hưởng của lỗ hổng: high

Khuyến cáo khắc phục:

- Mã hóa dữ liệu: Mã hóa thông tin đăng nhập trước khi gửi đi để đảm bảo rằng người dùng và mật khẩu không thể dễ dàng bị đoán biết hoặc sửa đổi bởi attacker. Sử dụng giao thức HTTPS để bảo vệ dữ liệu truyền qua mạng.

- Kiểm tra tính hợp lệ của dữ liệu nhập

- Dùng Captcha: Sử dụng cơ chế captcha hoặc reCaptcha để xác nhận rằng người dùng là người thật và không phải là bot. Điều này giúp ngăn chặn việc tự động gửi yêu cầu thông qua repeater.

- Xác thực 2 yếu tố

Tài liệu tham khảo:

https://owasp.org/Top10/A01_2021-Broken_Access_Control/#example-attack-scenarios

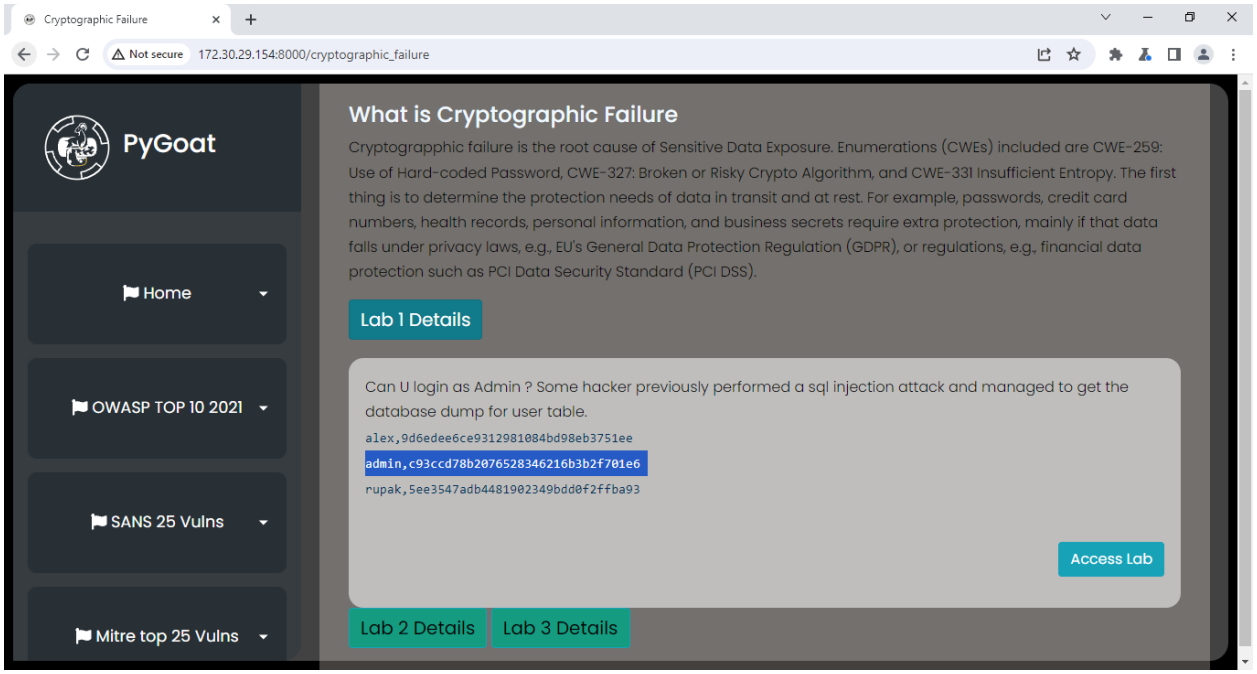
2. Kịch bản 02

Cryptographic Failures. Tài sản bị ảnh hưởng: thông tin, dữ liệu

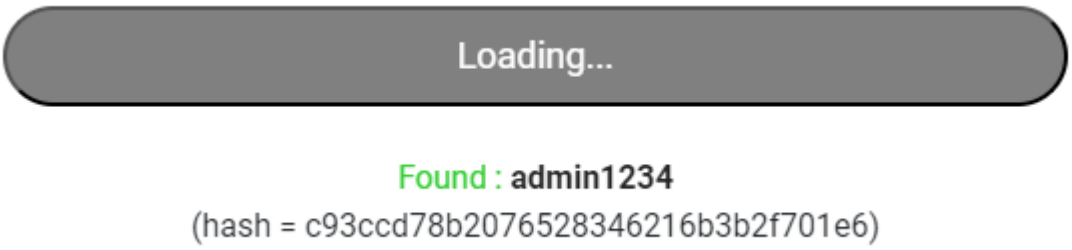
Mô tả lỗ hổng:

Sử dùng hàm MD5 một hash cũ có thể sử dụng các công cụ trên internet để decrypt password.

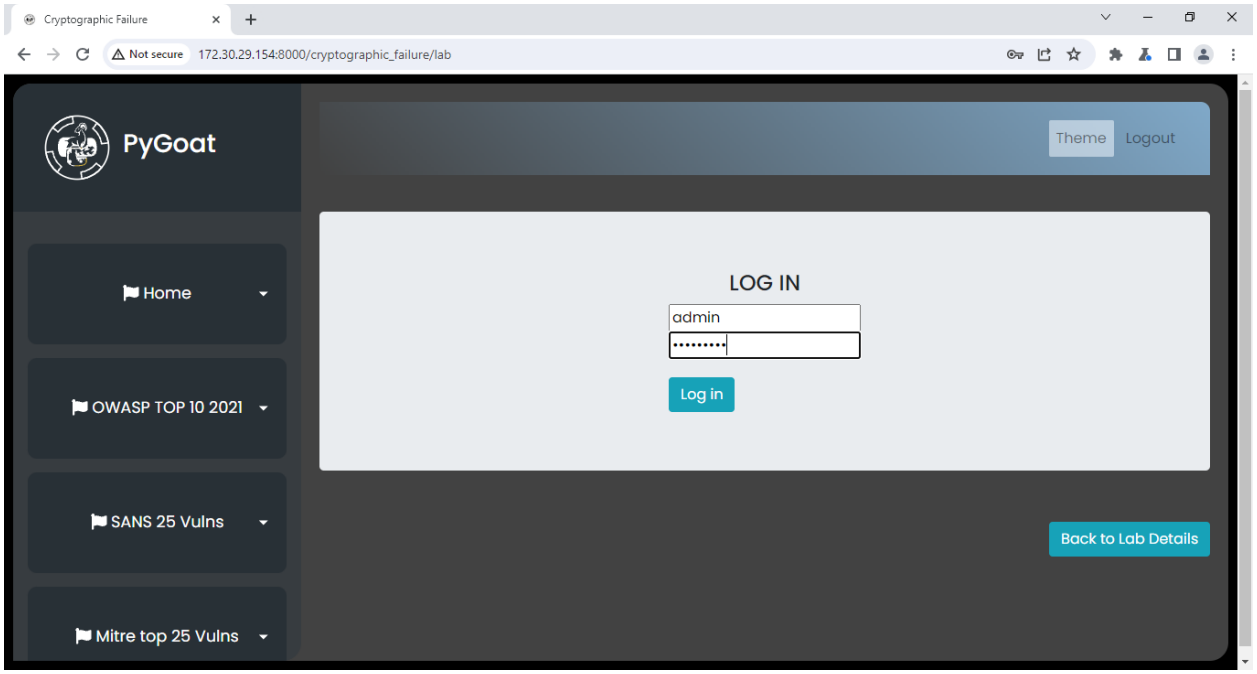
Các bước thực hiện:

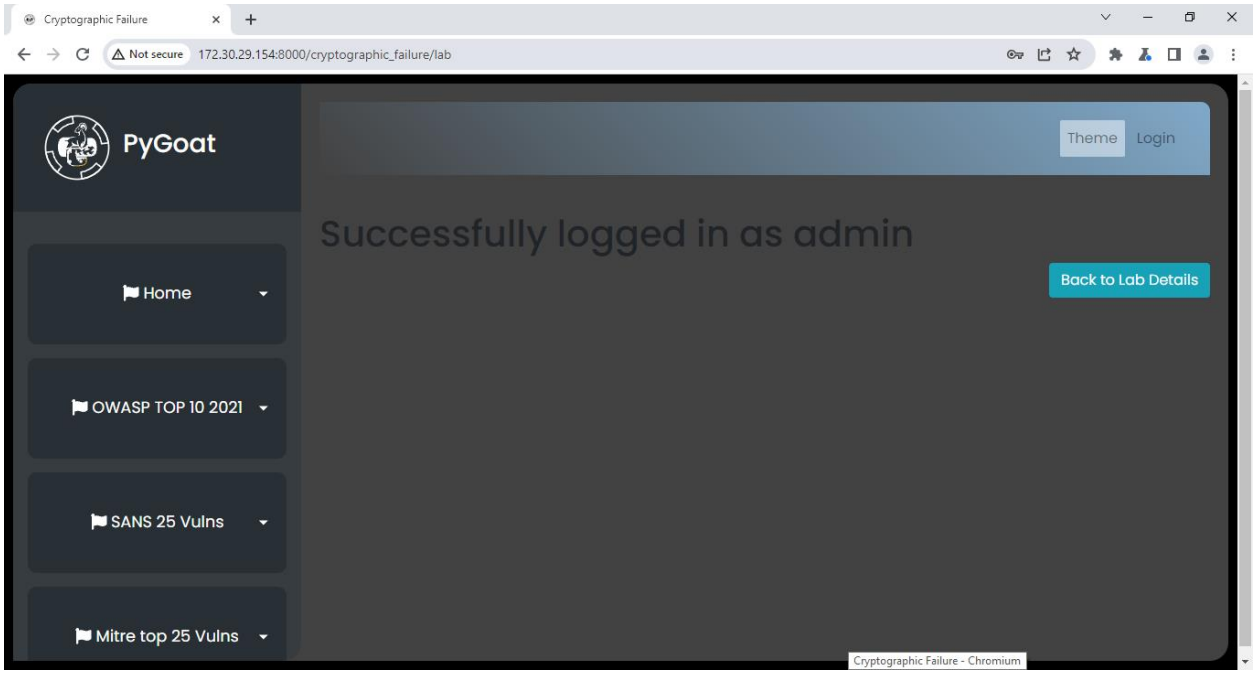


Các password được cung cấp dưới dạng MD5. Hàm hash MD5 đã bị bruteforce và dễ dàng tìm kiếm thông qua các trang web online trên mạng. Ở đây chúng ta sẽ thử trang https://www.md5online.org/md5-decrypt.html



Sử dụng username đã được cung cấp và password đã được giải để login.





Mức độ ảnh hưởng: high

Khuyến cáo khắc phục:

- Dùng các thuật toán hash mạnh hơn như SHA-256 hoặc SHA3 thay vì MD5.
- Sử dụng salt.

Tài liệu tham khảo:

https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

3. Kịch bản 03

Injection. Tài sản bị ảnh hưởng: thông tin

Mô tả lỗ hổng:

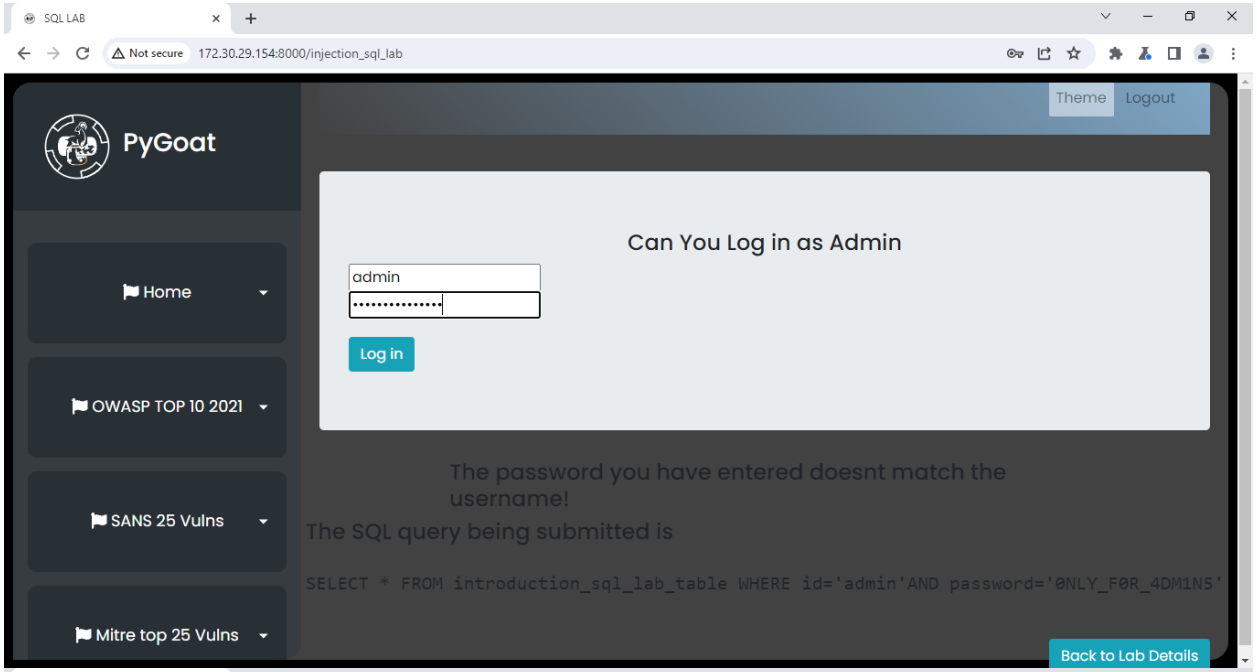
Sử dụng việc thiếu xác thực đầu vào, truyền trực tiếp đầu vào vào câu truy vấn để lấy quyền truy cập.

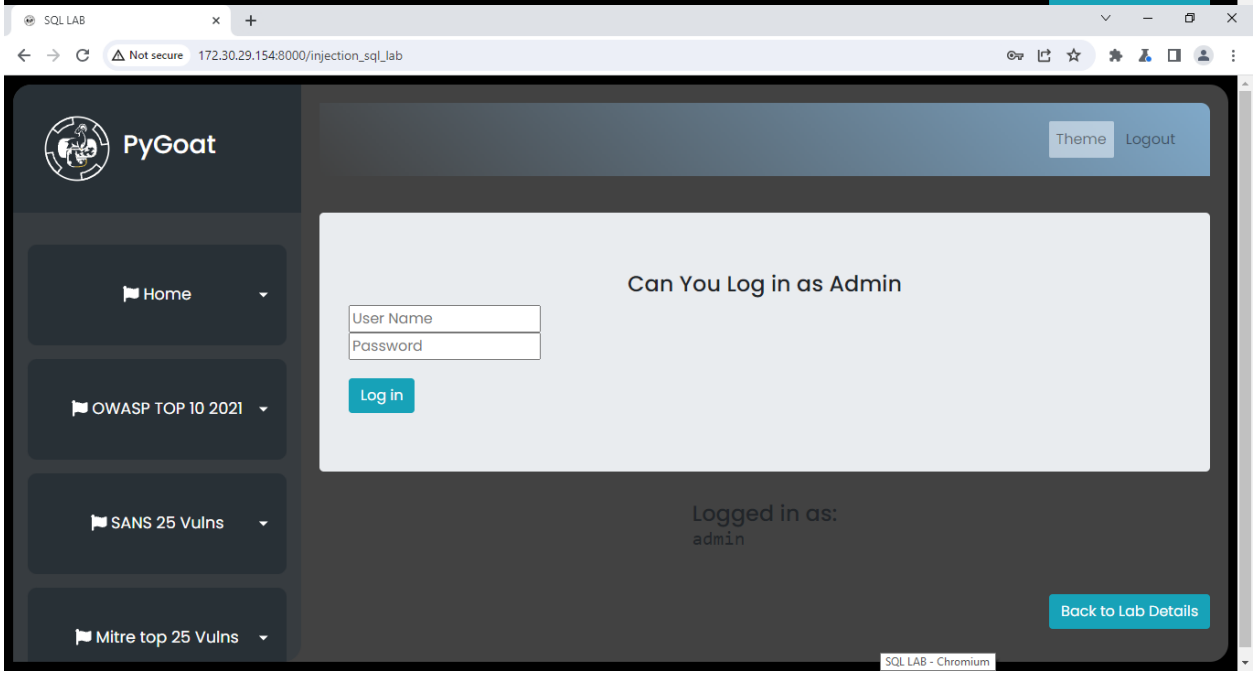
Các bước thực hiện:

Đầu tiên truy cập vào trang web: http://localhost:8000/injection_sql_lab

Ở đây ta đã biết được username là admin, tiến hành truy cập thử với ' or 1=1—

Ý nghĩa của câu lệnh là luôn đúng và ký tự -- đằng sau để có thể loại bỏ hết các điều kiện phía sau của câu truy vấn





Ta đã truy cập được vào admin.

Mức độ ảnh hưởng: high

Khuyến cáo khắc phục:

- Không bao giờ được tin tưởng những input người dùng nhập vào: Dữ liệu luôn phải được xác thực trước khi sử dụng trong các câu lệnh SQL.

- Giới hạn quyền truy cập của người dùng đối với cơ sở dữ liệu: Chỉ những tài khoản có quyền truy cập theo yêu cầu mới được kết nối với cơ sở dữ liệu. Điều này có thể giúp giảm thiểu những lệnh SQL được thực thi tự động trên server.

- Các lệnh được chuẩn bị sẵn: Điều này bao gồm việc tạo truy vấn SQL như hành động đầu tiên và sau đó xử lý toàn bộ dữ liệu được gửi như những tham số.

- Hãy loại bỏ các kí tự meta như '"/\; và các kí tự extend như NULL, CR, LF, ... trong các string nhận được từ:

+ input do người dùng đệ trình

+ các tham số từ URL

+ các giá trị từ cookie

Tài liệu tham khảo:

SQL Injection là gì? Cách phòng chống tấn công SQL Injection (quantrimang.com)

4. Kịch bản 04

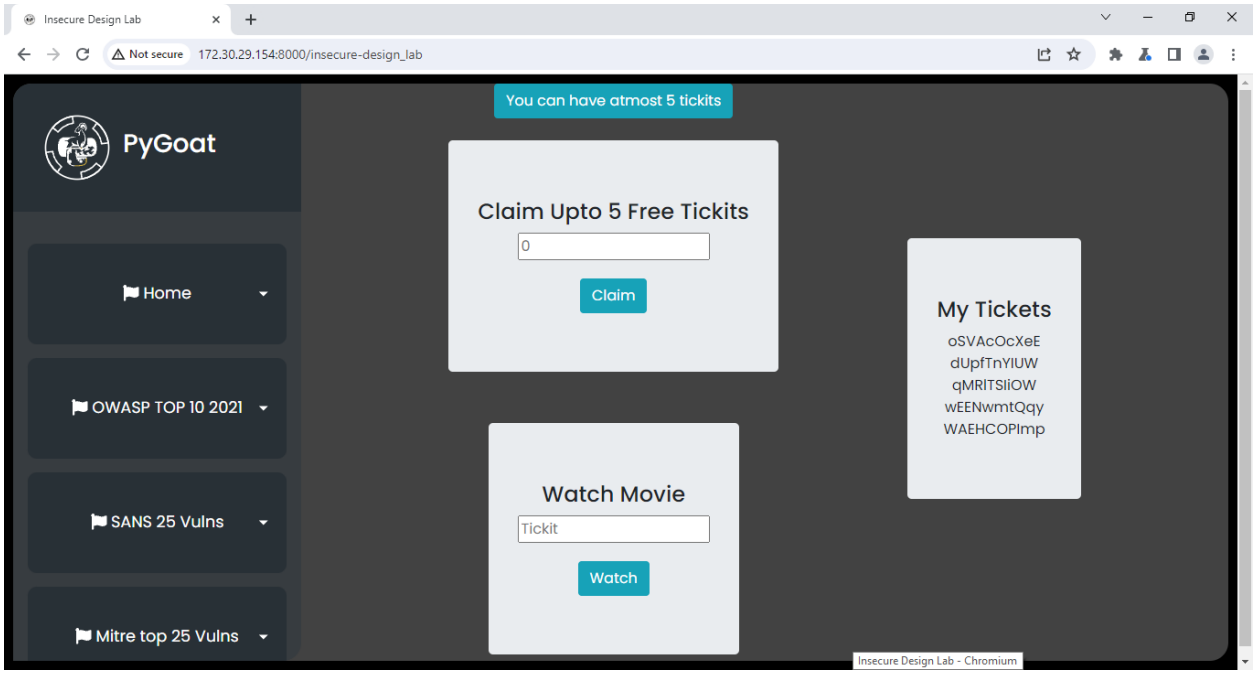
Insecure Design. Tài sản bị ảnh hưởng: lợi nhuận

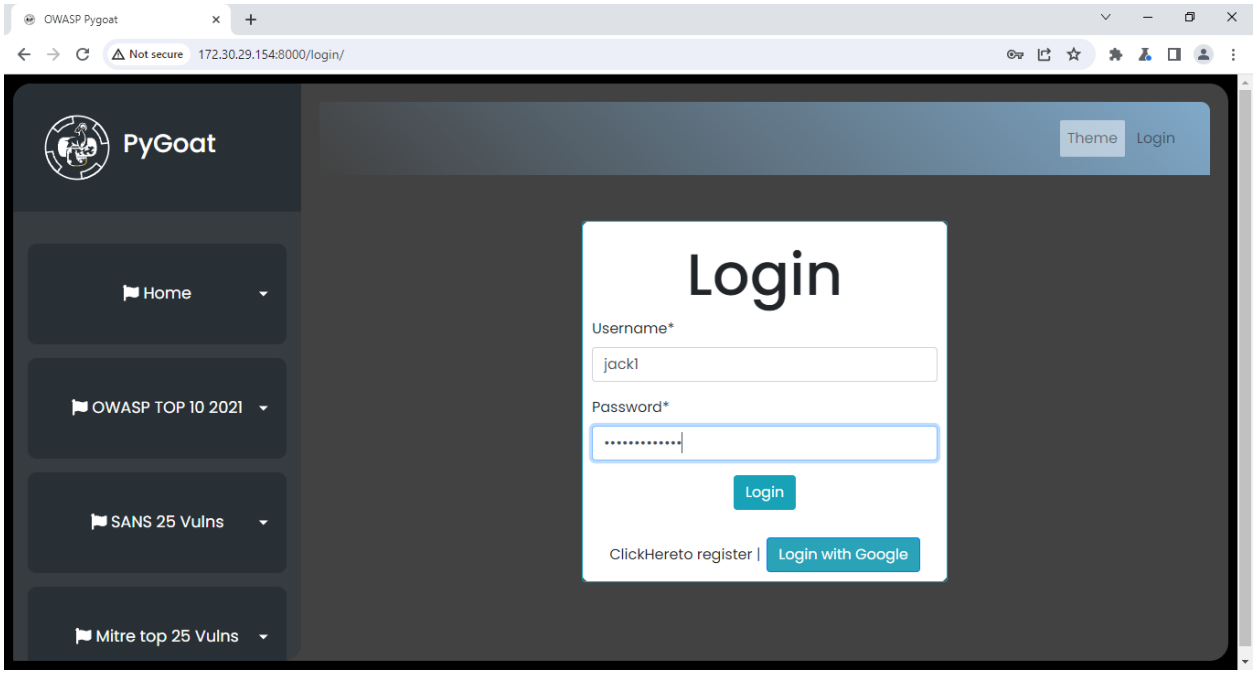
Mô tả lỗ hổng:

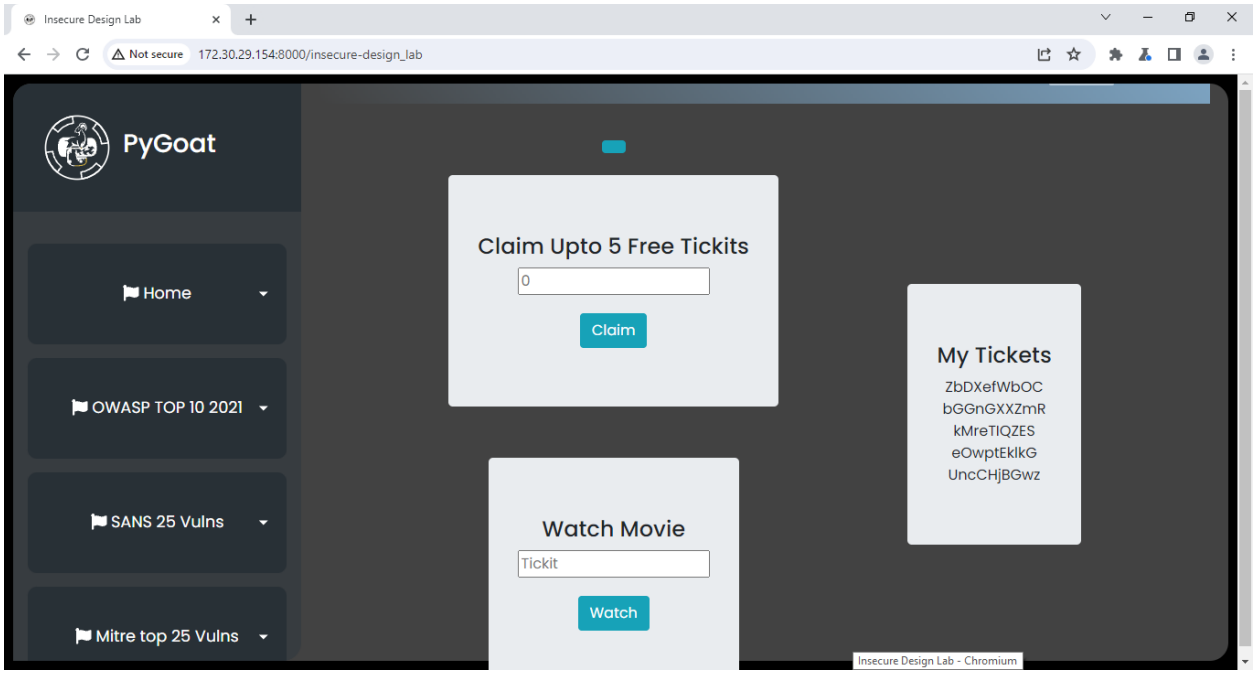
Tận dụng lỗi thiết kế không an toàn để lấy toàn bộ vé xem phim.

Các bước thực hiện:

Đầu tiên truy cập http://localhost:8000/insecure-design_lab để mua vé.


Insecure Design Lab
Not secure
172.30.29.154:8000/insecure-design_lab
PyGoat
You can have atmost 5 tickits
Claim Upto 5 Free Tickits
0
Claim
My Tickets
oSVAcOcXeE
dUpfTnYIUW
qMRITSliOW
wEENwmtQqy
WAEHCOPlmp
Watch Movie
Tickit
Watch
Home
OWASP TOP 10 2021
SANS 25 Vulns
Mitre top 25 Vulns
Insecure Design Lab - Chromium


OWASP Pygoat
Not secure
172.30.29.154:8000/login/
PyGoat
Theme
Login
Login
Username*
jack1
Password*
Login
ClickHereto register |
Login with Google
Home
OWASP TOP 10 2021
SANS 25 Vulns
Mitre top 25 Vulns



Ta có thể có thể thấy trang web này không có kiểm tra việc 1 người dùng có thể tạo nhiều tài khoản để lấy vé. Do đó ta chỉ cần tạo 12 tài khoản để lấy hết vé.

Mức độ ảnh hưởng: high

Khuyến cáo khắc phục:

- Xây dựng và sử dùng vòng đời phát triển an toàn.

- Xây dựng và sử dụng thư viện các mẫu thiết kế an toàn.

- Áp dụng mô hình đe dọa cho các lĩnh vực quan trọng như xác thực, kiểm soát truy cập, logic kinh doanh và các luồng chính của ứng dụng.

- Tích hợp ngôn ngữ bảo mật và điều khiển vào user story

- Tách biệt các tầng ứng dụng và tầng mạng dựa trên mức độ phơi bày và nhu cầu bảo vệ

- Hạn chế việc tiêu thụ tài nguyên bởi người dùng hoặc dịch vụ để ngăn chặn các cuộc tấn công từ chối dịch vụ và đảm bảo phân bổ tài nguyên công bằng.

Tài liệu tham khảo:

https://owasp.org/Top10/A04_2021-Insecure_Design/

5. Kịch bản 05

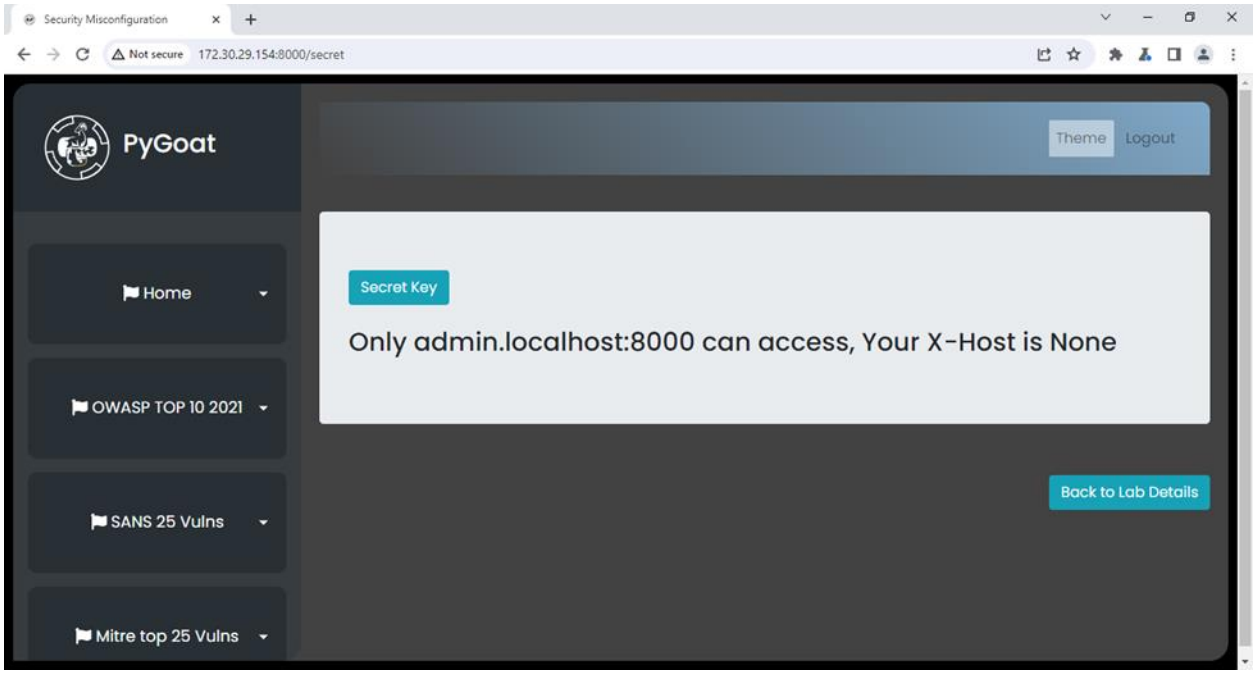
Security Misconfiguration. Tài sản bị ảnh hưởng: thông tin, dữ liệu

Mô tả lỗ hổng:

Thêm trường X-Host: admin.localhost:8000 vào và forward gói tin để có thể truy cập vào quyền admin

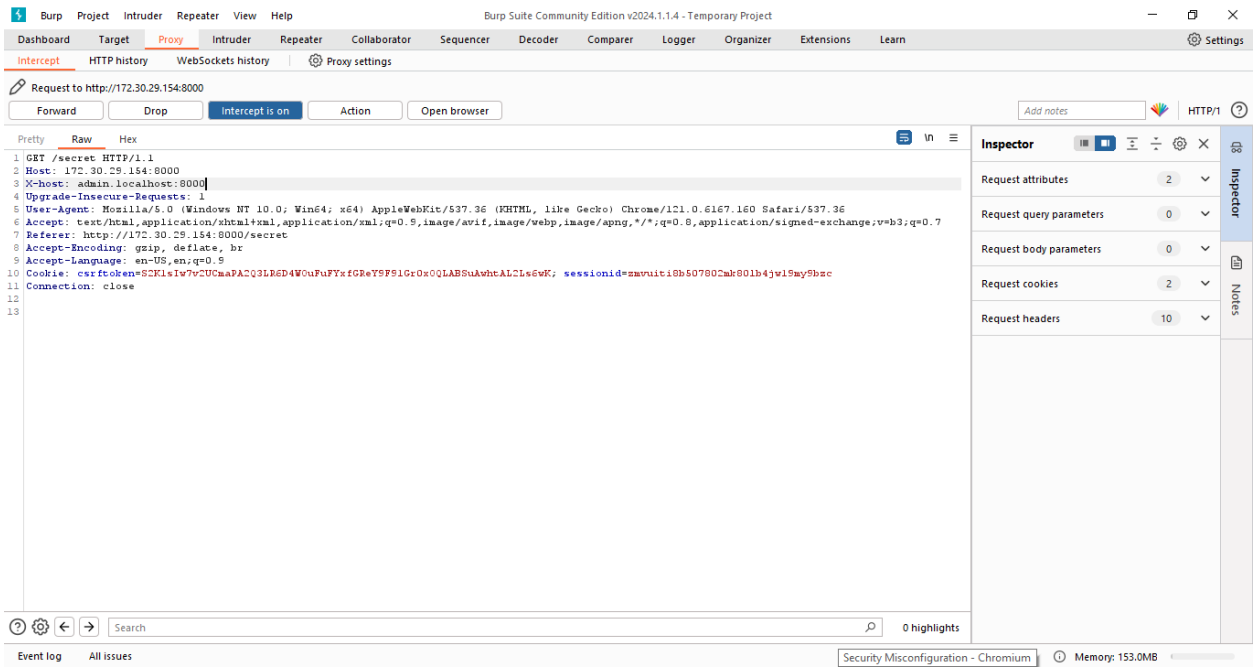
Các bước thực hiện:

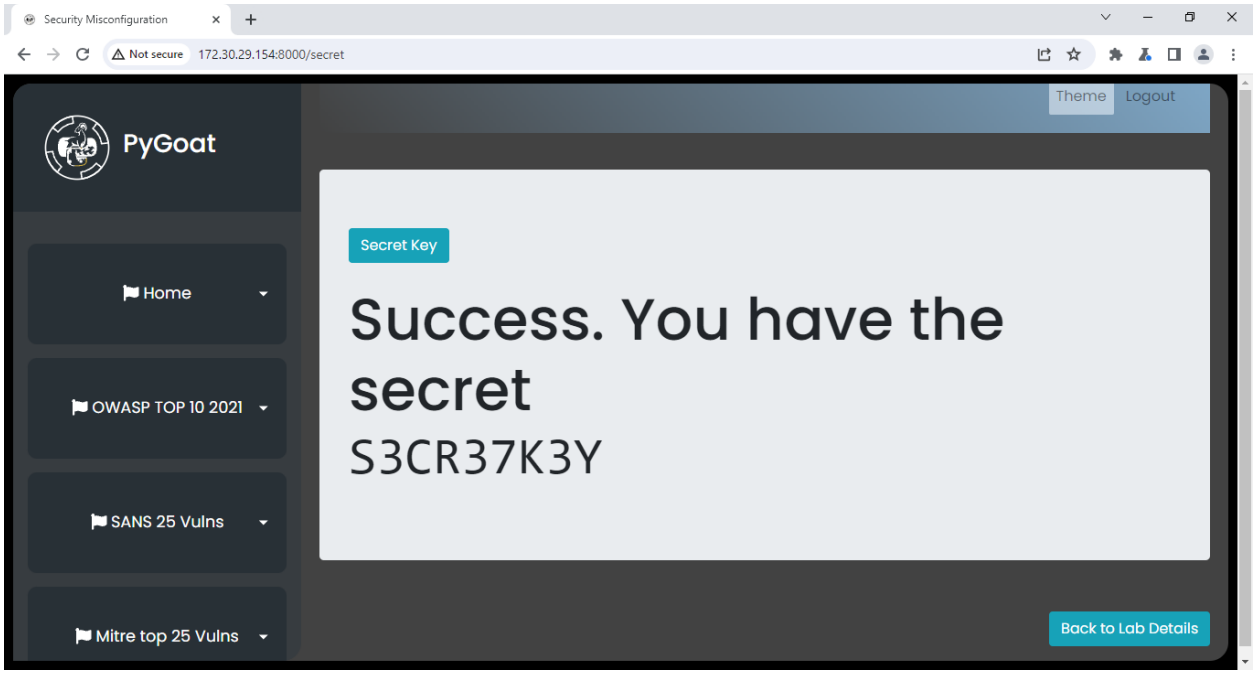
Đầu tiên khi nhấn lấy khoá bí mật, thông báo hiện ra là chỉ có trang admin.localhost:8000 mới có thể truy cập vào chức năng này. Và thông báo X-Host lúc này là None



Ở đây X-Host là 1 HTTP Header được sử dụng để xác định tên miền hoặc địa chỉ IP của máy chủ chứa tài nguyên trên mạng. X-Host được sử dụng trong các trường hợp cần định danh chỉ định máy chủ để có thể truy cập tài nguyên trên mạng.

Ta sẽ thử chặn gói tin và thêm trường X-Host: admin.localhost:8000





Sau khi forward thì ta có thể lấy được secret key

Mức độ ảnh hưởng: high

Khuyến cáo khắc phục:

- Quá trình tăng cường lặp lại giúp triển khai môi trường mới nhanh chóng và dễ dàng, đảm bảo môi trường đó được khóa chặt chẽ. Môi trường phát triển, kiểm thử và sản xuất nên được cấu hình giống nhau, với các thông tin đăng nhập khác nhau.

- Nền tảng tối giản không chứa bất kỳ tính năng, thành phần, tài liệu và ví dụ không cần thiết. Loại bỏ hoặc không cài đặt các tính năng và framework không sử dụng.

- Xem xét và cập nhật cấu hình phù hợp với tất cả các ghi chú, cập nhật và bản vá bảo mật.

- Tự động hóa quá trình xác minh hiệu quả của cấu hình và thiết lập trong tất cả các môi trường.

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

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo 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]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

  *Ví dụ: [*NT101.K11.ATCL*]-Session1_Group3.*
- 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 Lab.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

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

HẾT