

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật Web và ứng dụng

Lab 1: Tổng quan các lỗi hỏng bảo mật web thường gặp

GVHD: Ngô Đức Hoàng Sơn

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT132.012.ATCL.2- Nhóm 3

STT	Họ và tên	MSSV	Email
1	Đỗ Thị Yến Ly	21520337	21520337@gm.uit.edu.vn
2	Lê Hoàng Oanh	21521253	21521253@gm.uit.edu.vn
3	Nguyễn Đại Bảo Duy	21520772	21520772@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1	100%
2	Yêu cầu 2	100%
3	Yêu cầu 3	100%
4	Yêu cầu 4	100%
5	Yêu cầu 5	100%
6	Yêu cầu 6	100%
7	Yêu cầu 7	100%
8	Yêu cầu 8	100%

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

BÁO CÁO CHI TIẾT

1. Câu truy vấn tại đây đang làm gì?

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 POST /broken_access_lab_1 HTTP/1.1				1 HTTP/1.1 200 OK			
2 Host: localhost:8000				2 Server: gunicorn			
3 Content-Length: 28				3 Date: Thu, 14 Mar 2024 01:17:16 GMT			
4 Cache-Control: max-age=0				4 Connection: close			
5 sec-ch-ua:				5 Content-Type: text/html; charset=utf-8			
6 sec-ch-ua-mobile: ?0				6 X-Frame-Options: DENY			
7 sec-ch-ua-platform: ""				7 Content-Length: 27204			
8 Upgrade-Insecure-Requests: 1				8 Vary: Cookie			
9 Origin: http://localhost:8000				9 X-Content-Type-Options: nosniff			
10 Content-Type: application/x-www-form-urlencoded				10 Referrer-Policy: same-origin			
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36				11 Cross-Origin-Opener-Policy: same-origin			
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7				12 Set-Cookie: admin=0; expires=Thu, 14 Mar 2024 01:20:36 GMT; Max-Age=200; Path=/"			
13 Sec-Fetch-Site: same-origin				13			
				14 <!DOCTYPE html>			
				15			
				16			

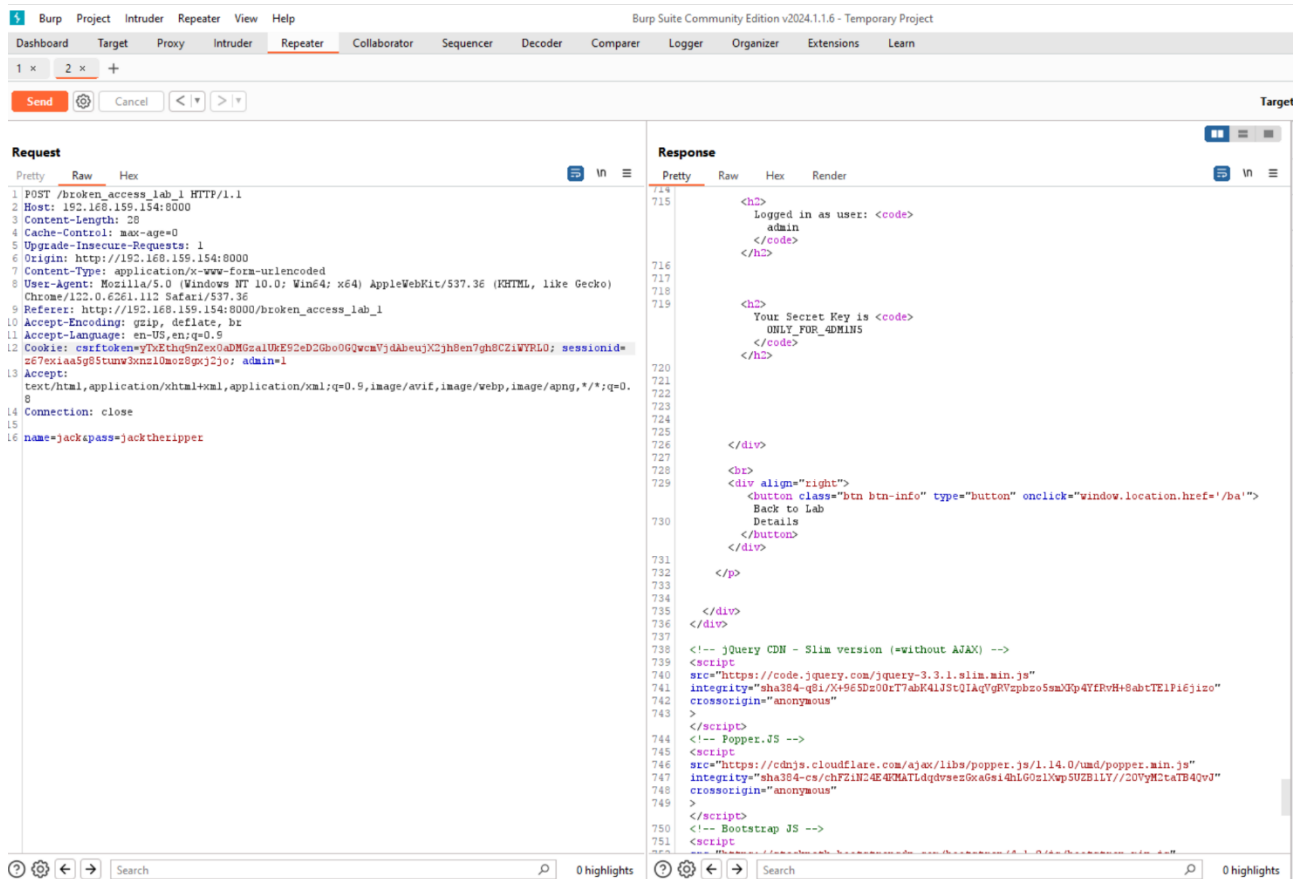
Câu truy vấn này là một phản hồi HTTP, cụ thể là một header "Set-Cookie" được gửi từ máy chủ đến trình duyệt web của bạn khi bạn thực hiện một loạt các hoạt động trên trang web. Trong trường hợp này, header "Set-Cookie" đang cố gắng đặt một cookie có tên là "admin" với giá trị là "0".

Cụ thể, đoạn mã "Set-Cookie: admin=0; expires=Thu, 14 Mar 2024 01:20:36 GMT; Max-Age=200; Path=/" nói rằng:

- Tên của cookie là "admin".
- Giá trị của cookie là "0".
- Thời gian hết hạn của cookie là "Thu, 14 Mar 2024 01:20:36 GMT".
- Độ tuổi tối đa của cookie là 200 giây (tức là sau 200 giây kể từ khi nó được thiết lập, cookie sẽ không còn hiệu lực).
- Đường dẫn của cookie được đặt là "/".

Tóm lại, câu truy vấn này đang thiết lập một cookie có tên "admin" với giá trị "0" và sẽ hết hạn vào ngày 14 tháng 3 năm 2024 vào lúc 01:20:36 GMT. Cookie này chỉ có hiệu lực trong vòng 200 giây kể từ khi nó được thiết lập và áp dụng cho mọi đường dẫn trên trang web (/).

2. Sử dụng repeater để thực hành bài tập



3. Báo cáo lỗ hổng đang được thực hành.

- Tiêu đề: Broken Access Control – truy cập hoặc chỉnh sửa tài khoản người dùng khác
- Mô tả lỗ hổng:

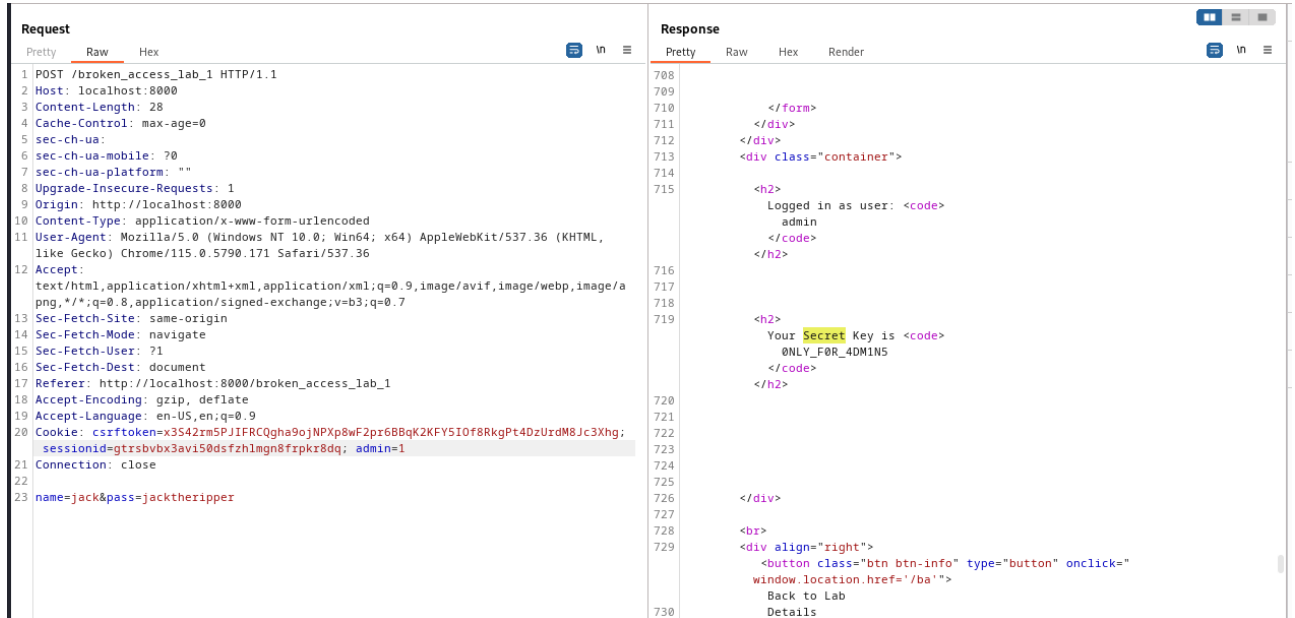
Broken Access Control:

- Kiểm soát truy cập thực hiện việc thực thi chính sách sao cho người dùng không thể thực hiện các hành động khác ngoài các quyền họ được dự định. Lỗi phân quyền sẽ dẫn đến một số hậu quả như việc tiết lộ thông tin trái phép, sửa đổi hoặc phá hủy tất cả dữ liệu hoặc chức năng kinh doanh ngoài giới hạn của người dùng đó được phép.
- Bỏ qua kiểm soát truy cập bằng cách sửa đổi URL, trạng thái nội bộ của ứng dụng, trang HTML hoặc sửa đổi các yêu cầu API.
- Truy cập API với không có kiểm soát truy cập nào dành cho các phương thức POST, PUT và DELETE

Tóm tắt: Các bước để thực hiện lại và bằng chứng:

1. bước 1: Truy cập bài thực hành tại <http://localhost:8000> => OSWAP TOP 10 2021 => A1: Broken Access Control => Lab 1 Details và đăng nhập vào trang web với tài khoản và mật khẩu được cung cấp.

2. bước 2: Trở lại giao diện HTTP history của Burpsuite để kiểm tra lịch sử câu truy vấn để hiểu rõ logic của ứng dụng.
3. bước 3: Lấy gói GET có được sau khi đăng nhập gửi đến Repeater, vô tab Repeater sửa quyền admin=1, rồi send.



- Mức độ ảnh hưởng của lỗ hổng:

Nâng cao đặc quyền. Ví dụ như khi không đăng nhập ứng dụng nhưng hành động như người dùng bình thường.

- Khuyến cáo khắc phục:

Xác thực và ủy quyền mạnh mẽ: Thực hiện các biện pháp xác thực mạnh mẽ để xác định danh tính của người dùng. Sử dụng các phương pháp xác thực như JWT (JSON Web Tokens), OAuth, hoặc các phiên bản cải tiến của Cookie để đảm bảo rằng người dùng đã được xác thực trước khi truy cập vào các tài nguyên quan trọng.

4. Đoạn chuỗi ký tự trên là gì?

Can U login as Admin ? Some hacker previously performed a sql injection attack and managed to get the database dump for user table.

```
alex,9d6edee6ce9312981084bd98eb3751ee
admin,c93ccd78b2076528346216b3b2f701e6
rupak,5ee3547adb4481902349bdd0f2ffba93
```

Đoạn chuỗi ký tự trên là danh sách các tài khoản người dùng và mật khẩu của họ trong một hệ thống, trong đó có tên người dùng và mật khẩu của họ được mã hóa hàm băm MD5.

5. Báo cáo lỗ hổng đang được thực hành

- Tiêu đề: Cryptographic Failures
- Mô tả lỗ hổng:

Cryptographic Failures:

- Điều đầu tiên phải xác định nhu cầu bảo vệ dữ liệu khi ở trạng thái truyền và trạng thái nghỉ. Ví dụ như mật khẩu, thông tin số thẻ tín dụng, bản ghi sức khỏe, thông tin cá nhân và bí mật doanh nghiệp cần được bảo vệ.
- Lỗi mật mã là nguyên nhân chính dẫn đến lỗi Tiết lộ thông tin dữ liệu nhạy cảm. Các CWE có thể tham khảo như CWE-259: Sử dụng mật khẩu mã hoá cứng, CWE-327: Thuật toán mã hoá bị hỏng hoặc rủi ro, CWE-331...


Tóm tắt: Các bước để thực hiện lại và bằng chứng:

1. bước 1: Truy cập http://localhost:8000/cryptographic_failure/lab

2. bước 2: Giải mã mật khẩu qua trang <https://www.md5online.org/md5-decrypt.html>

Enter your MD5 hash below and cross your fingers :

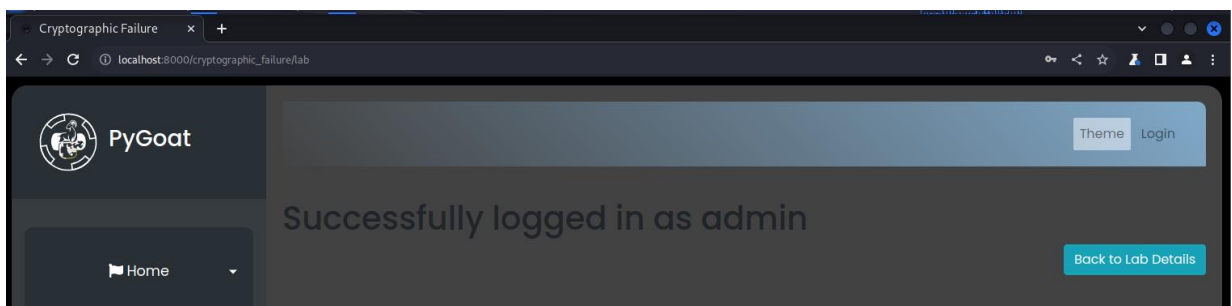
c93ccd78b2076528346216b3b2f701e6

☒ Quick search (free) ☐ In-depth search (1 credit) 

Loading...

Found : admin1234
(hash = c93ccd78b2076528346216b3b2f701e6)

3. bước 3: Dùng mật khẩu tìm được tiến hành đăng nhập vào bài tập thực hành để kiểm tra.



- Mức độ ảnh hưởng của lỗ hổng: Tác động bảo mật nào mà kẻ tấn công có thể đạt được?

Lỗ hổng Cryptographic Failures có thể dẫn đến lộ thông tin, tấn công MITM, phá mã, tấn công Brute Force, đe dọa tính toàn vẹn dữ liệu, và tổn thất uy tín/hậu quả pháp lý.

- Khuyến cáo khắc phục: Làm thế nào để vá lỗ hổng này?

Đảm bảo áp dụng các thuật toán, giao thức và khóa tiêu chuẩn mạnh mẽ và cập nhật; sử dụng quản lý khóa thích hợp.

Lưu trữ mật khẩu bằng cách sử dụng các hàm băm thích ứng và băm mạnh với hệ số công việc (hệ số độ trễ), chẳng hạn như Argon2, scrypt, bcrypt hoặc PBKDF2.

6. Nếu trang web thực hành bị lỗi tiêm SQL thì khai thác như thế nào?

Ta có username là admin và password ta chỉ cần nhập đoạn sau: ' OR '1' ='1

Truy vấn này có nghĩa là select username = admin trong đó mật khẩu là bất kỳ thứ gì HOẶC '1'='1' . '1'='1' sẽ luôn cho kết quả TRUE và truy vấn tìm nạp người dùng có tên quản trị viên và mật khẩu=TRUE. Do đó cho phép đăng nhập với tư cách quản trị viên.

7. Báo cáo lỗ hổng đang được thực hành.

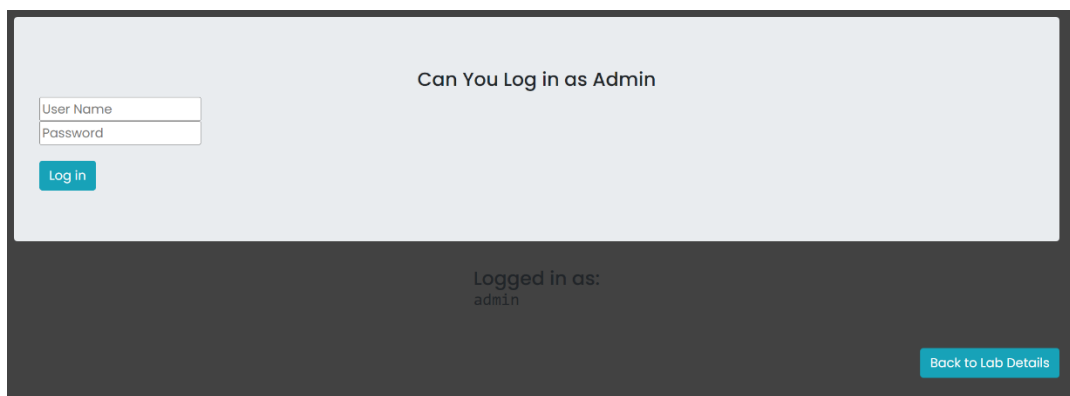
- Tiêu đề: SQL Injection
- Mô tả lỗ hổng:

SQL Injection:

- Một ứng dụng có khả năng bị tấn công tiêm khi dữ liệu người dùng cung cấp không được xác thực hoặc lọc bởi ứng dụng.
- Tùy theo kiểu tiêm thì mã tấn công có thể khác nhau và tùy chỉnh theo cấu trúc của ứng dụng muốn tấn công, một số kiểu tiêm phổ biến như SQL injection, NoSQL injection, OS command injection, Object Relational Mapping(ORM) injection, LDAP injection, và Expression Language (EL) injection hoặc Object Graph Navigation Library (OGNL) injection.

Tóm tắt: Các bước để thực hiện lại và bằng chứng:

1. bước 1: truy cập trang http://localhost:8000/injection_sql_lab
2. bước 2: ta đăng nhập bằng user admin và nhập ' OR '1' ='1 vào phần password và coi kết quả.



- Mức độ ảnh hưởng của lỗ hổng:

Lỗ hổng SQL Injection có thể dẫn đến việc truy cập, sửa đổi, hoặc xóa dữ liệu trong cơ sở dữ liệu của một ứng dụng web. Kẻ tấn công có thể đạt được sự kiểm soát hoặc gây ra hậu quả nghiêm trọng đối với bảo mật hệ thống, bao gồm truy cập vào thông tin nhạy cảm, thực thi mã độc hại, và phá vỡ tính toàn vẹn dữ liệu.

- Khuyến cáo khắc phục:

Sử dụng LIMIT và các điều khiển SQL khác trong truy vấn để ngăn chặn việc tiết lộ hàng loạt bản ghi trong trường hợp chèn SQL.

8. Lỗi thiết kế không an toàn nằm ở đâu? Chú ý là web được tạo nhiều tài khoản.

Lỗi thiết kế không an toàn là khi hết vé vẫn lấy được.

9. Báo cáo lỗ hổng đang được thực hành.

- Tiêu đề: Insecure Design
- Mô tả lỗ hổng:
Là một vấn đề không an toàn khi một hệ thống cho phép người dùng tạo một số lượng không giới hạn các tài khoản mà không có các biện pháp kiểm soát hợp lệ. Để tái tạo lỗ hổng thì chúng ta tạo một ứng dụng mà không có các biện pháp bảo vệ chặt chẽ để kiểm soát việc tạo tài khoản, đảm bảo rằng người dùng có thể tạo bất kỳ số lượng tài khoản nào mà họ muốn mà không gặp phải bất kỳ rào cản nào.
- Tóm tắt: Các bước để thực hiện lại và bằng chứng:
 1. bước 1: Tạo thử account và lấy vé, được thông báo là còn 50 vé nữa
 2. bước 2: Tạo thêm nhiều account khác để lấy vé đến khi hết vé (12 accounts)
 3. bước 3: Tạo thêm account thứ 13 vẫn lấy được và xem phim

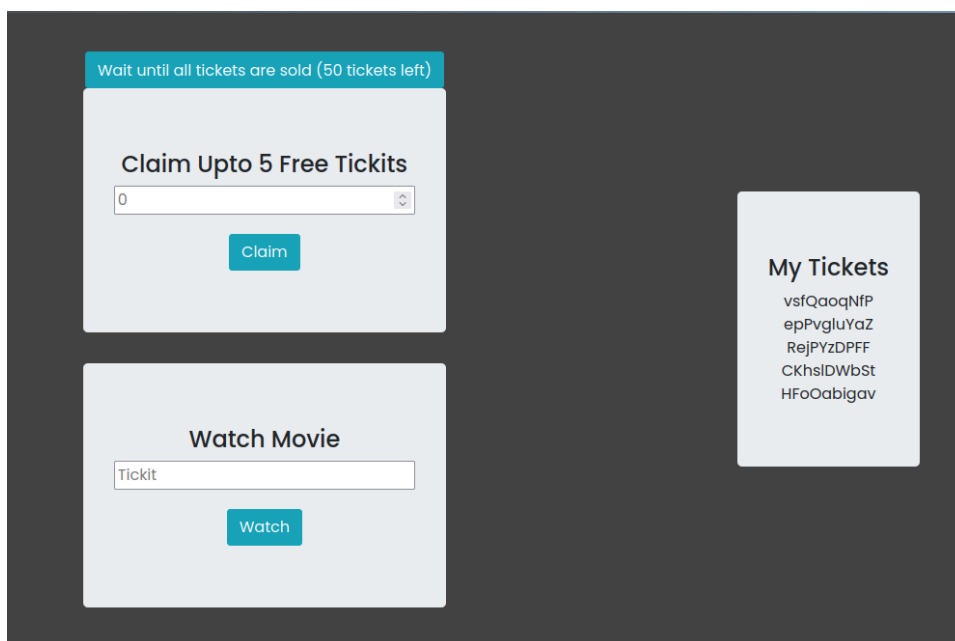


Figure 1: Account1

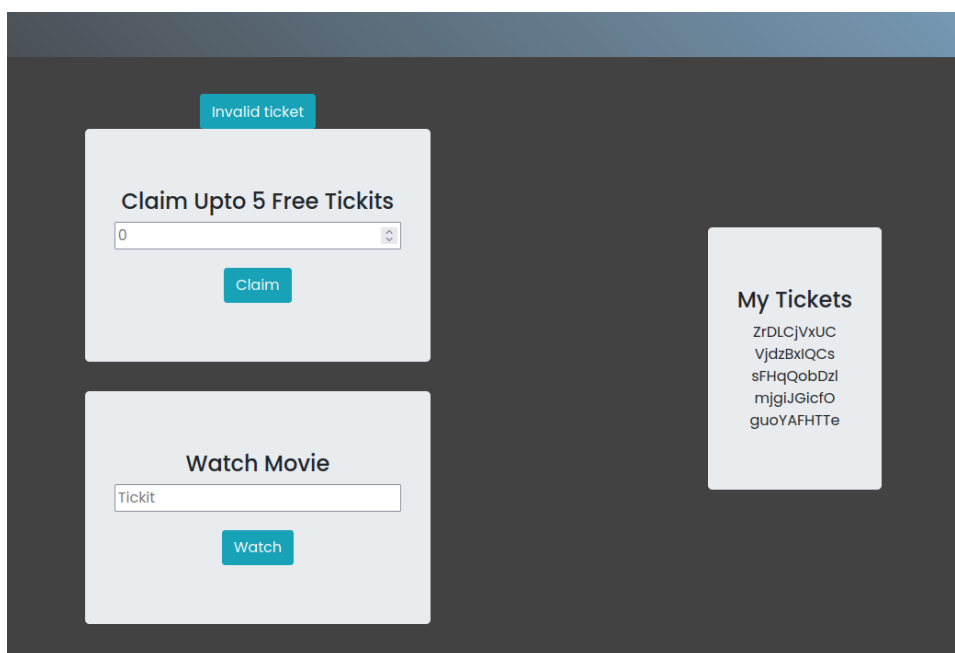


Figure 2: Account 12

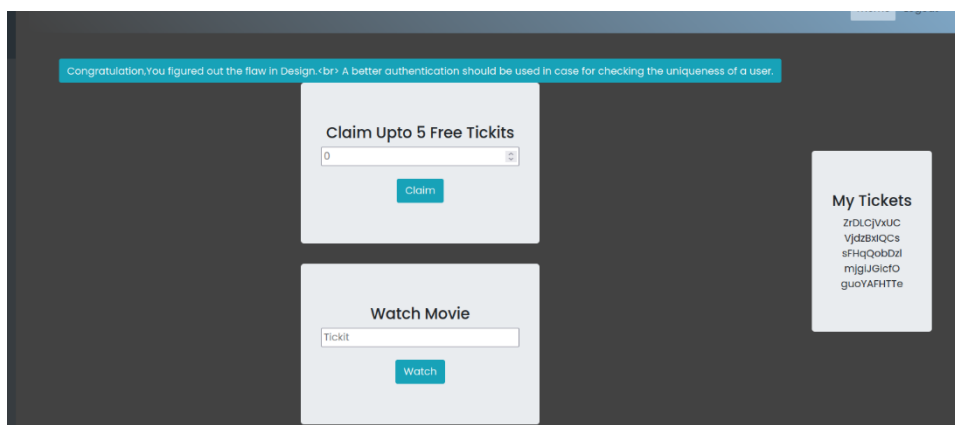


Figure 3: Account 12 xem phim thành công

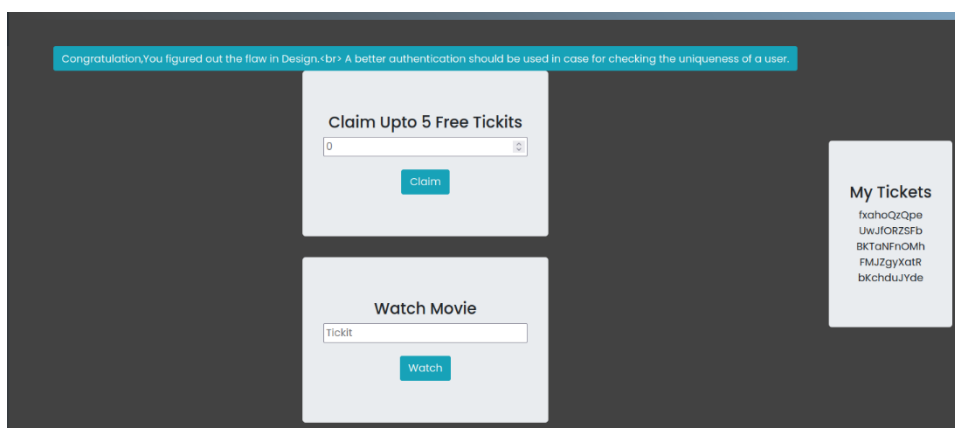


Figure 4: Account 13 vẫn lấy được 5 vé và xem phim thành công

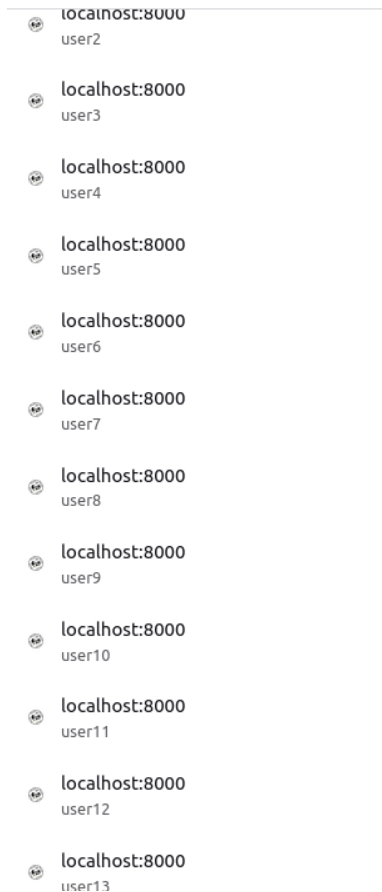


Figure 5: Các account được tạo

- Mức độ ảnh hưởng của lỗ hổng:
Lỗ hổng tạo nhiều tài khoản có thể dẫn đến xâm nhập thông tin cá nhân và đe dọa an ninh dữ liệu. Kẻ tấn công có thể lợi dụng để giả mạo và gây tổn hại cho danh tiếng người dùng và tổ chức. Điều này nhấn mạnh sự cần thiết của biện pháp an ninh mạnh mẽ để ngăn chặn các tác động tiềm ẩn này.
- Khuyến cáo khắc phục:
Để khắc phục lỗ hổng tạo nhiều tài khoản và ngăn chặn các rủi ro bảo mật, cần áp dụng mật khẩu mạnh, kích hoạt xác thực hai yếu tố, giám sát hoạt động tài khoản, giới hạn số lượng tài khoản, tăng cường giáo dục người dùng, và thực hiện kiểm tra và nâng cấp thường xuyên. Điều này sẽ giúp cải thiện bảo mật thông tin cá nhân và giảm thiểu nguy cơ xâm nhập.

10. X-Host is None là gì? Có kiểm soát được X-Host không.

Trong giao thức HTTP, trường Header Host được sử dụng để chỉ định tên miền (domain name) của máy chủ web được đang được truy cập hoặc đang trả về nội dung. Host header được sử dụng trong các yêu cầu HTTP cho phép máy chủ web nhận biết tên miền được yêu cầu và phục vụ nội dung phù hợp.

Điều này cho biết header X-Host không được đặt trong yêu cầu HTTP. Nếu hệ thống của bạn yêu cầu một giá trị cụ thể của header "X-Host" để kiểm soát truy cập và giá trị này được thiết lập thành None (không xác định), điều này có thể tạo ra một lỗ hổng bảo mật hoặc trở ngại trong quá trình xác thực và ủy quyền truy cập.

Về việc kiểm soát được giá trị của "X-Host", điều này phụ thuộc vào cách ứng dụng của bạn được cấu hình và xử lý các yêu cầu HTTP. Bạn có thể kiểm soát giá trị của "X-Host" thông qua mã nguồn của ứng dụng và các cấu hình máy chủ. Điều này có thể bao gồm việc xác thực, kiểm tra và xử lý các giá trị tiêu đề "X-Host" được gửi trong yêu cầu HTTP để quyết định liệu yêu cầu được chấp nhận hay từ chối.

11. Báo cáo lỗ hổng đang được thực hành.

- Tiêu đề: Security Misconfiguration
- Mô tả lỗ hổng:

Security Misconfiguration: Ứng dụng có thể gặp phải vấn đề cấu hình bảo mật sai trong một số trường hợp như:

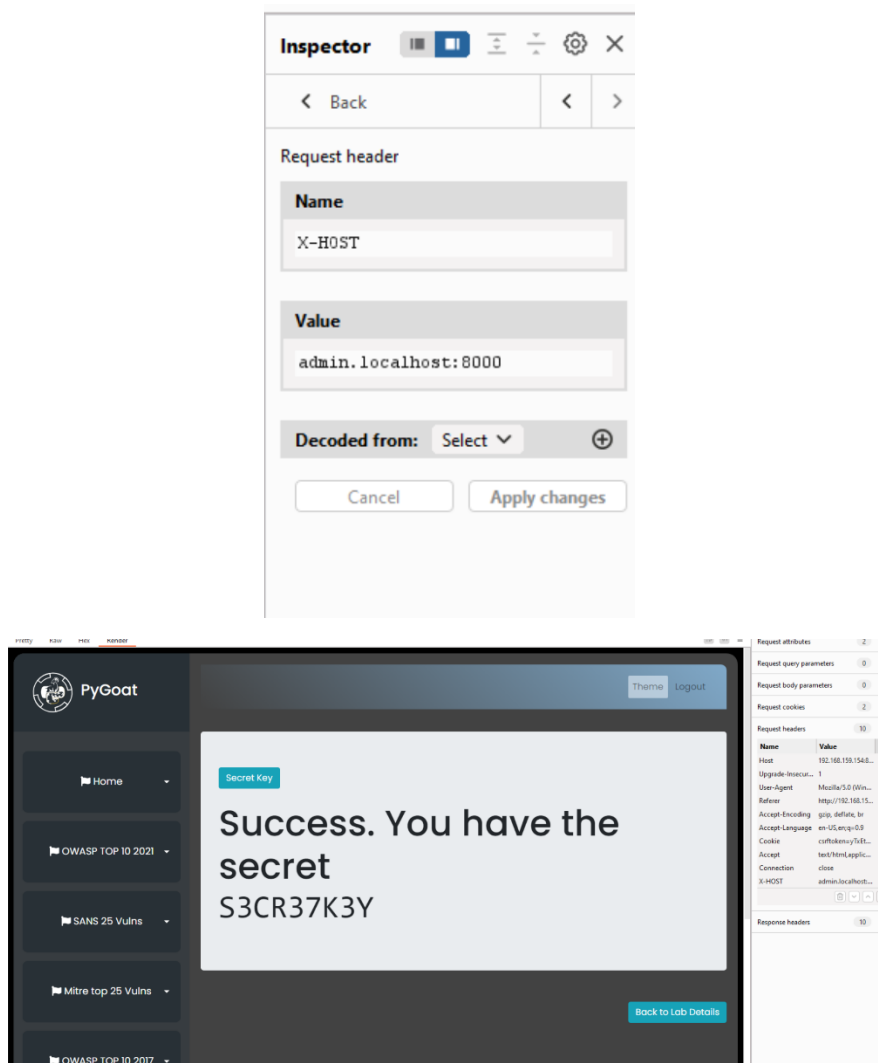
- Các tính năng không cần thiết được bật hoặc cài đặt (ví dụ như các cổng, dịch vụ, trang, tài khoản, hoặc quyền không cần thiết)
- Tài khoản mặc định và mật khẩu được bật và không thay đổi.
- Xử lý thông báo lỗi quá mức cho người dùng
- Đối với các hệ thống được nâng cấp, tính năng bảo mật mới nhất bị vô hiệu hoá hoặc không được cấu hình an toàn.
- Phần mềm bị lỗi thời hoặc có lỗ hổng (xem thêm A06:2021-Vulnerable and Outdated Components)

Tóm tắt: Các bước để thực hiện lại và bằng chứng:

1. bước 1: Truy cập bài tập tại: http://localhost:8000/sec_mis_lab

2. bước 2: Kết quả 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

3. bước 3: Cho X-Host giá trị là admin.localhost:8000 thì ta sẽ thấy khóa bí mật



- Mức độ ảnh hưởng của lỗ hổng:

Lỗ hổng Security Misconfiguration có thể dẫn đến việc truy cập trái phép, lộ thông tin nhạy cảm, chiếm quyền kiểm soát, tấn công DoS, hỏng hóc ứng dụng, và vi phạm quy định bảo mật. Điều này tạo ra nguy cơ nghiêm trọng cho tính bảo mật và ổn định của hệ thống thông tin.

- Khuyến cáo khắc phục:

Kiểm tra Cấu hình: Thực hiện một kiểm tra cấu hình đầy đủ và chi tiết trên tất cả các thành phần của hệ thống, bao gồm máy chủ, cơ sở dữ liệu, ứng dụng và tất cả các thành phần mạng.

Loại bỏ Cài đặt Mặc định: Đảm bảo rằng tất cả các cài đặt mặc định không an toàn đã được thay đổi và cập nhật thành cấu hình an toàn và phù hợp.

Kiểm tra Tổ chức Thư mục và Tập: Đảm bảo rằng tất cả các thư mục và tập được bảo vệ đúng cách và không thể truy cập trái phép.

