

Báo Cáo Thực Hành Môn Bảo Mật Web Và Ứng Dụng

Lab 01: OWASP Top 10 Part 1

GVHD: Nghi Hoàng Khoa

Nhóm: 4

Thông tin thành viên

STT	Họ và tên	MSSV
1	Võ Sỹ Minh	21521146

Mức độ hoàn thành

Yêu cầu	Mức độ hoàn thành
Bài tập 1	100%
Bài tập 2	100%
Bài tập 3	100%
Bài tập 4	100%
Bài tập 5	100%
Bài tập 6	100%

1. Lỗ hổng A01-2021

Tiêu đề: Broken Access Control.

Tài sản bị ảnh hưởng: hoạt động của server/ doanh nghiệp, dữ liệu.

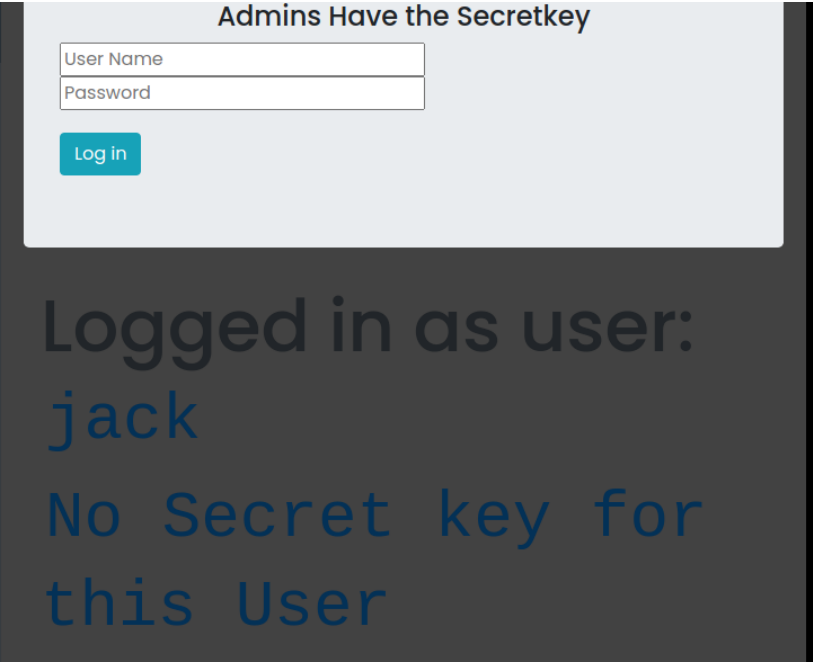
Mô tả lỗ hổng: Khi dùng repeater để gửi thông tin login lên trang web, attacker có thể sửa đổi các yêu cầu gửi thông tin login bằng cách thay đổi các tham số, điều này có thể bao gồm việc thay đổi các giá trị của các trường người dùng và mật khẩu trong yêu cầu. Điều này có thể cho phép attacker truy 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.

Chậm lại và suy nghĩ 1: Câu truy vấn ở đây là cung cấp cho server cặp username và password để yêu cầu xác thực. Trong đó có trường 'admin = 0' có nghĩa tài khoản này không phải admin.

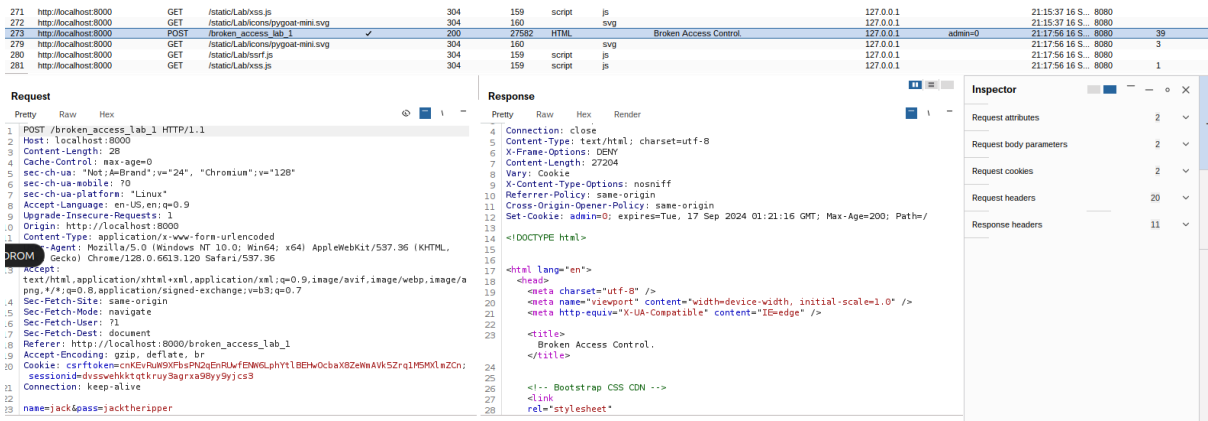
Các bước thực hiện:

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

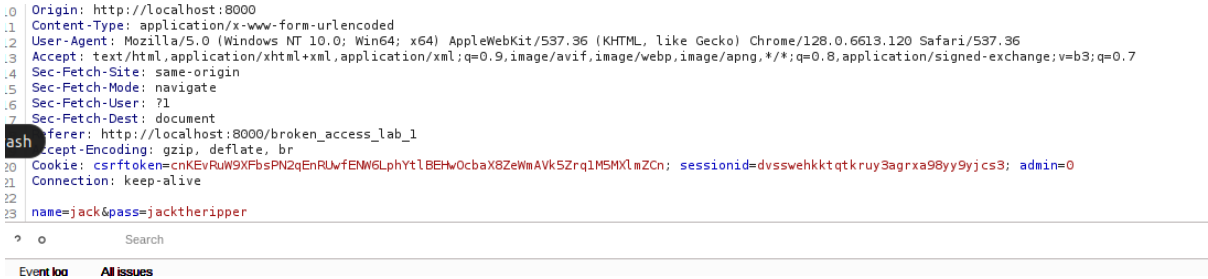
Bước 2: Đăng nhập vào trang web với tài khoản và mật khẩu được cung cấp của user Jack



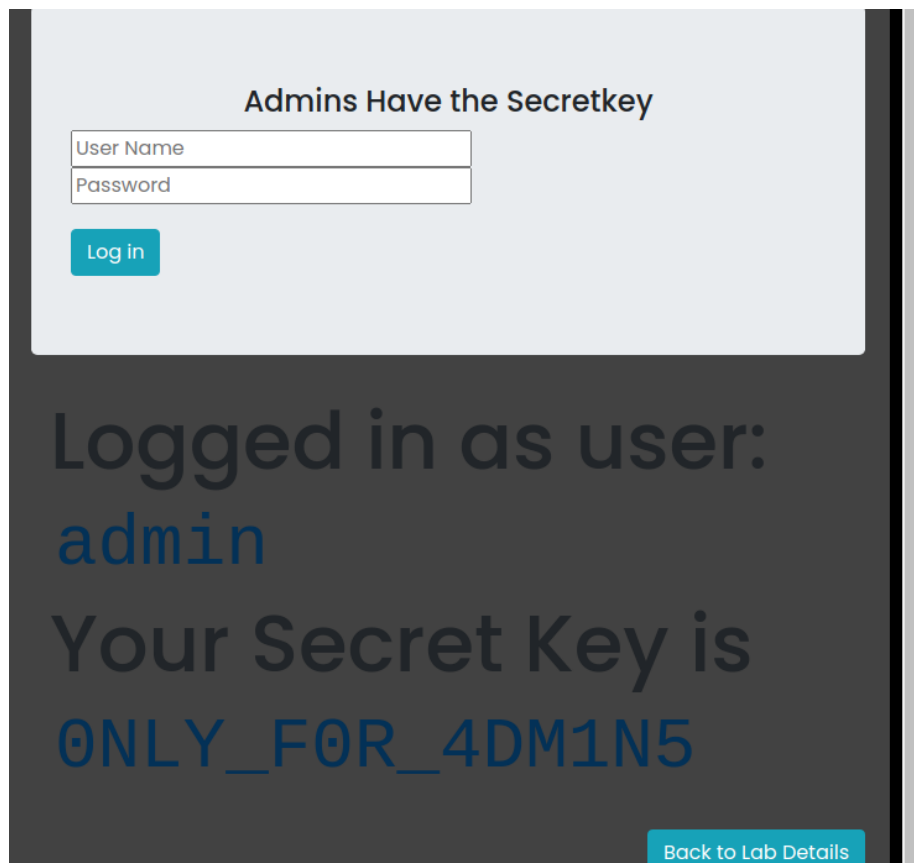
Bước 3: Trở lại giao diện HTTP history của Burpsuite để kiểm tra lịch sử câu truy vấn để tìm hiểu



Bước 4: Sử dụng intercept để leo thang quyền bằng cách đổi giá trị của biến 'admin' từ 0 thành 1



Vậy là đã leo thang quyền thành công và có key



Mức độ ảnh hưởng của lỗ hổng: high

Khuyến cáo khắc phục:

- Mã hóa dữ liệu truyền: Sử dụng SSL để bảo vệ dữ liệu truyền qua mạng.
- Kiểm tra tính hợp lệ của dữ liệu nhập
- Xác thực nhiều yếu tố.
- 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.

Tài liệu tham khảo: https://owasp.org/Top10/A01_2021-Broken_Access_Control/#example-attack-scenarios

2. Lỗi hỏng A02-2021

Tên tiêu đề: Cryptographic Failures

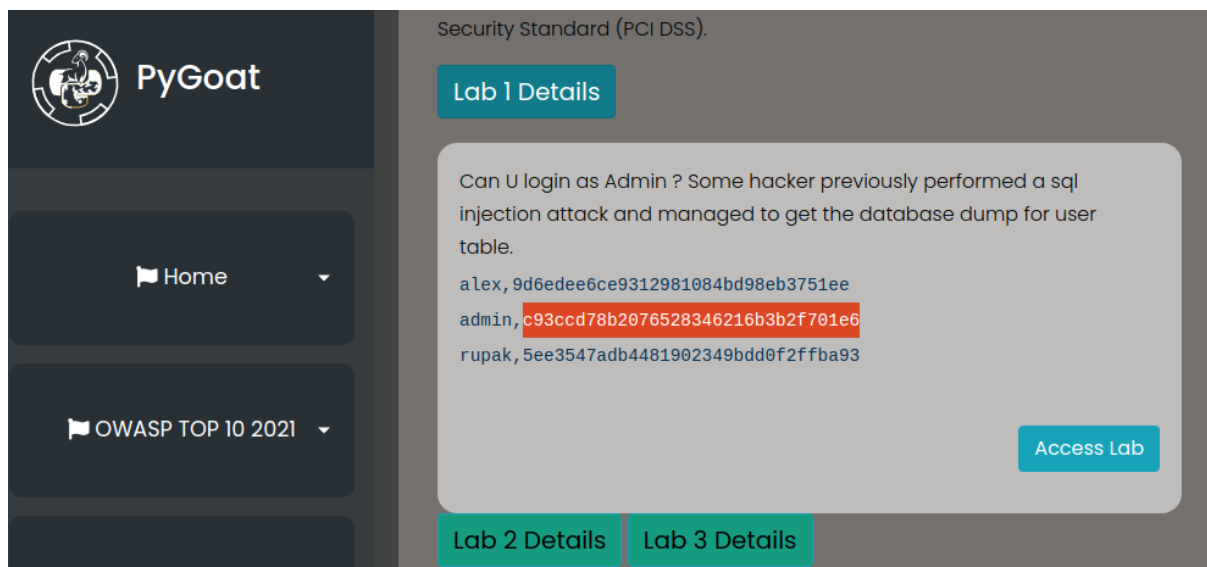
Tài sản bị ảnh hưởng: thông tin, dữ liệu

Mô tả lỗi hỏng: Sử dụng hàm MD5 một hash cũ có thể sử dụng các công cụ trên internet để decrypt password.

Chậm lại và suy nghĩ 2: Đoạn chuỗi trên là hash của password ứng với username đã cho

Các bước thực hiện:

Bước 1: Xem các thông tin được biết trước trong đó có username là admin cùng hash được cho là password.

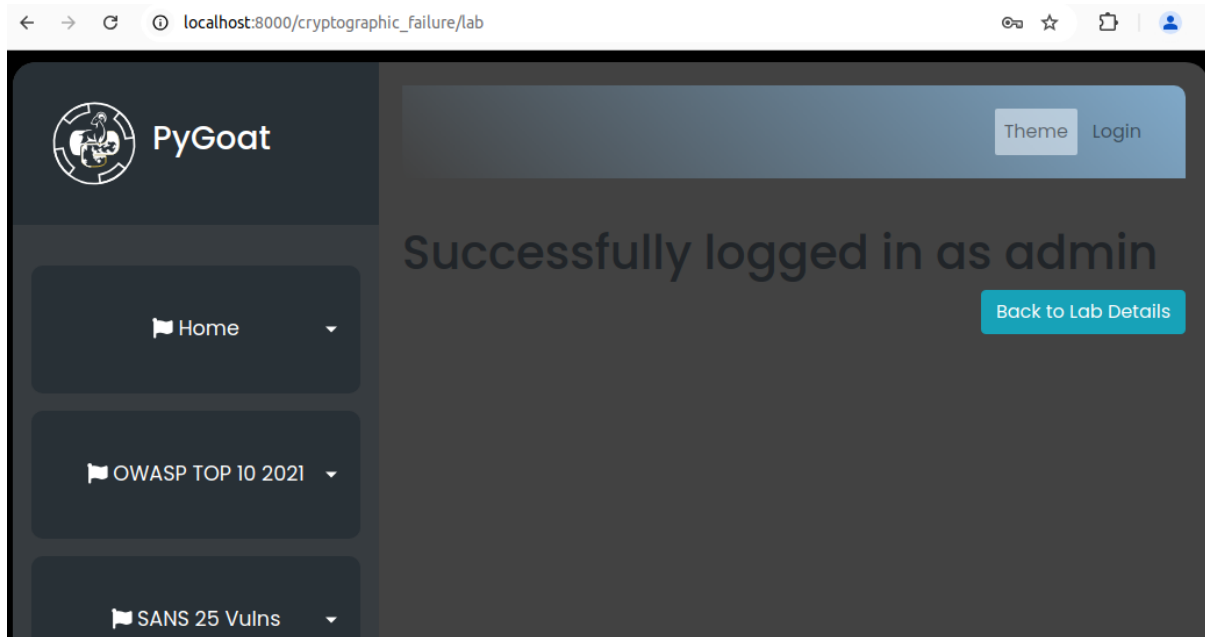


Bước 2: sử dụng <https://www.md5online.org/md5-decrypt.html> để xem plain text của mã hash md5 trên

Found : admin1234

(hash = c93ccd78b2076528346216b3b2f701e6)

Bước 3: Đăng nhập với cặp username, password có được



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

3. Lỗi hổng A03-2021

Tên tiêu đề: SQL Injection.

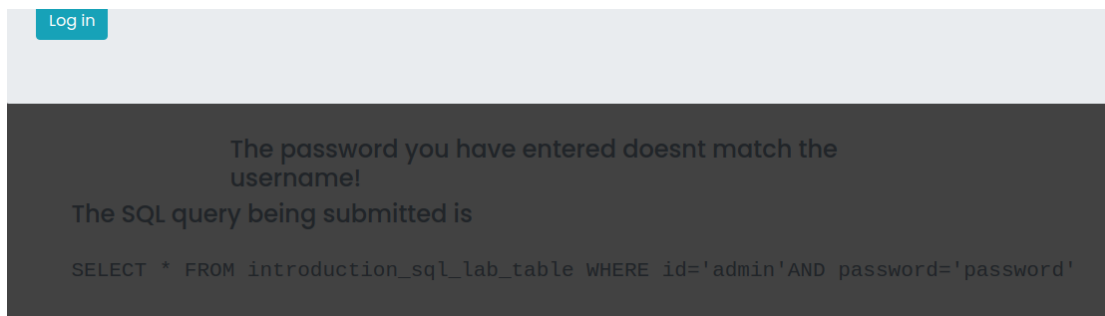
Tài sản bị ảnh hưởng: thông tin

Mô tả lỗi hổng: Sử dụng việc thiếu xác thực đầu vào, truyền trực tiếp đầu vào vào câu truy vấn để lấy quyền truy cập và thông tin quan trọng.

Chậm lại và suy nghĩ 3: Nếu một trang web có lỗi hổng SQL injection thì có thể khai thác bằng nhập vào các trường có thể nhập (như password,...) các loại điều kiện để việc truy vấn luôn đúng (như `or 1=1, ...`) hoặc nhằm lôi lên các dữ liệu quan trọng bằng các câu lệnh SQL.

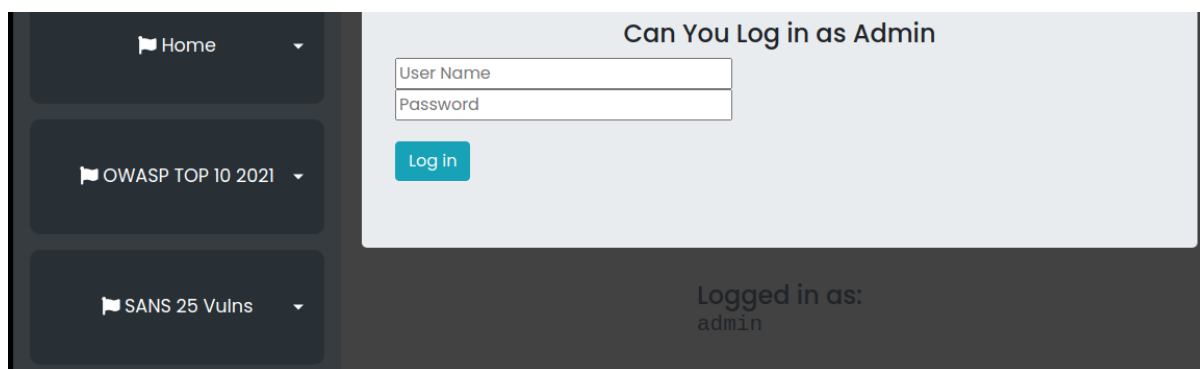
Các bước thực hiện:

Bước 1: Đăng nhập thử, được biết ở đây không có xác thực đầu vào nên có thể sử dụng SQL injection



Bước 2: username là admin như đã biết, tiến hành truy cập với password là: ' 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



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.

Tài liệu: https://quantrimang.com/cong-nghe/tan-cong-kieu-sql-injection-va-cac-phong-chong-trong-asp-net-34905#mcetoc_1cptf5bu20

4. Lỗ hổng A04-2021

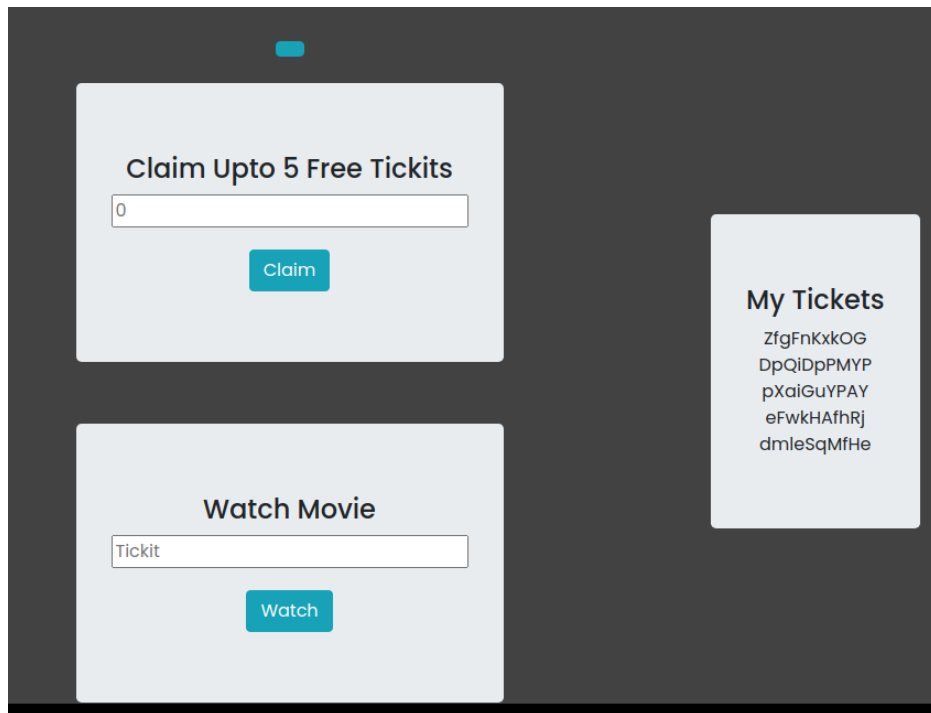
Tiêu đề: Insecure Design

Tài sản bị ảnh hưởng: tài sản.

Mô tả lỗ hổng: Việc xây dựng ứng dụng thiếu các bước xác thực cụ thể để hạn chế spam account có thể gây thiệt hại về tài sản hoặc các chiến lược kinh doanh.

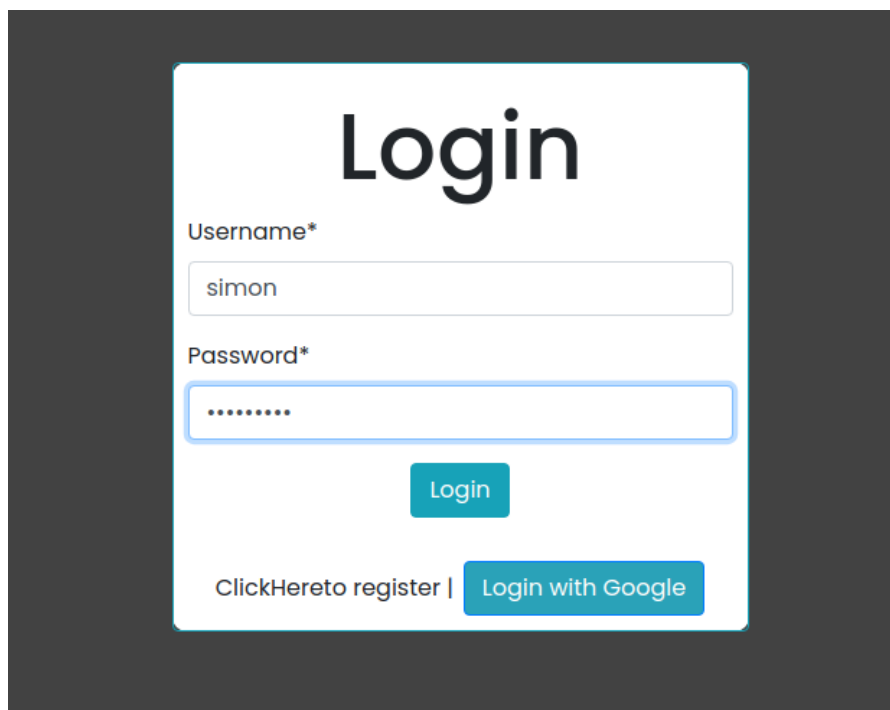
Các bước thực hiện:

Bước 1: nhập 5 vé để nhận vé.



The screenshot shows a dark-themed web interface. On the left, there are two light gray boxes. The top box is titled "Claim Upto 5 Free Tickits" and contains a text input field with the number "0" and a teal "Claim" button below it. The bottom box is titled "Watch Movie" and contains a text input field with the word "Tickit" and a teal "Watch" button below it. On the right side, there is a light gray box titled "My Tickets" which lists five alphanumeric strings: "ZfgFnKxkOG", "DpQiDpPMYP", "pXaiGuYPAY", "eFwkHArHj", and "dmleSqMfHe".

Bước 2: Đăng nhập tài khoản mới để tiếp tục



The screenshot shows a dark-themed web interface with a central white login form. The form has the title "Login" in large black font. Below the title, there are two labels: "Username*" and "Password*". The "Username*" label is followed by a text input field containing the text "simon". The "Password*" label is followed by a password input field with a blue border and a blue outline, containing a series of dots. Below the password field is a teal "Login" button. At the bottom of the form, there is a link "ClickHereto register |" followed by a teal button labeled "Login with Google".

Bước 3: Tiếp tục nhận vé

The screenshot shows a web application interface with a dark background. At the top, a teal banner reads "You can have atmost 5 tickits". Below this, there are two main sections on the left and a "My Tickets" section on the right.

Claim Upto 5 Free Tickits

0

Claim

Watch Movie

Tickit

Watch

My Tickets

AjFwxYcRXT
OJpZiKavMg
GVNzbzjcEv
GVvUcRVbAf
yOvacAQTmn

Mức độ ảnh hưởng: high

Khuyến cáo khắc phục:

- Xây dựng và sử dụng vòng đời phát triển an toàn.
- Xây dựng và sử dụng thư viện các mẫu thiết kế an toàn.
- Áp dụng threat model cho các lĩnh vực quan trọng như xác thực, kiểm soát truy cập, logic kinh doanh và các luồng chính của ứng dụng.

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

5. Lỗi hổng A05-2021

Tiêu đề: Security Misconfiguration.

Tài sản bị ảnh hưởng: thông tin, dữ liệu

Mô tả lỗi hổng: Nút secret key được thêm vào dễ dàng truy cập và không có cơ chế tốt để kiểm tra quyền admin.

Các bước thực hiện:

Bước 1: 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

Secret Key

Only admin.localhost:8000 can access, Your X-Host is 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.

Bước 2: Với gợi ý, cần thêm trường X-host với url như trên.

```
1 GET /secret HTTP/1.1
2 Host: localhost:8000
3 X-host: admin.localhost:8000
4 sec-ch-ua: "Not;A=Brand";v="24", "Chromium";v="128"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Linux"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Sa
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: http://localhost:8000/secret
16 Accept-Encoding: gzip, deflate, br
17 Cookie: csrftoken=KqcvLK0BW4Fbk80wVm2MN550GsxCDD5S4UvWvb0zsfal3ClilH5JBGsZLfskG7TS; sessionId=xg67tneov9knxnm12qlt5m
18 Connection: keep-alive
```

Bước 3: Sau khi forward thì truy cập thành công và lấy được key.

Secret Key

Success. You have the secret
S3CR37K3Y

Mức độ ảnh hưởng: high

Khuyến cáo khắc phục:

- Hệ thống 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.