Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta sử dụng burpsite mở trình duyệt và mở chế độ intercept on
* Sau đó sử dụng tài khoản đã được cấp để đăng nhập

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sau đó ta click chuội trái và Send to Repeater

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sau đó ta sửa đổi cookie của admin= thành admin=1 sau đó ấn send để gửi cho server

Ảnh có chứa văn bản

Mô tả được tạo tự động

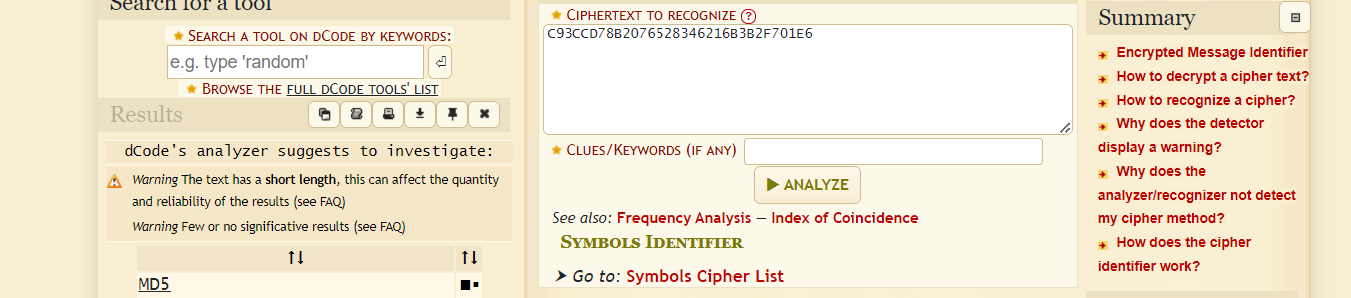
* Sau khi nhận được Response và ta kiểm tra thì thấy ta đã ở quyền admin và có được Secret key

b) A02:2021 – Cryptographic Failures

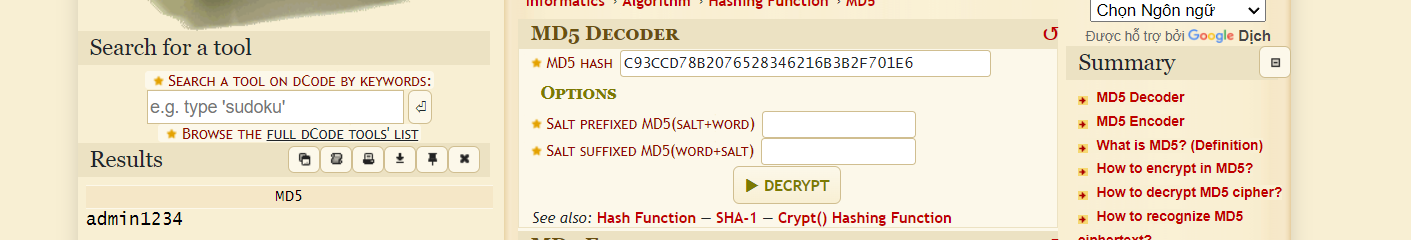
Ảnh có chứa văn bản

Mô tả được tạo tự động

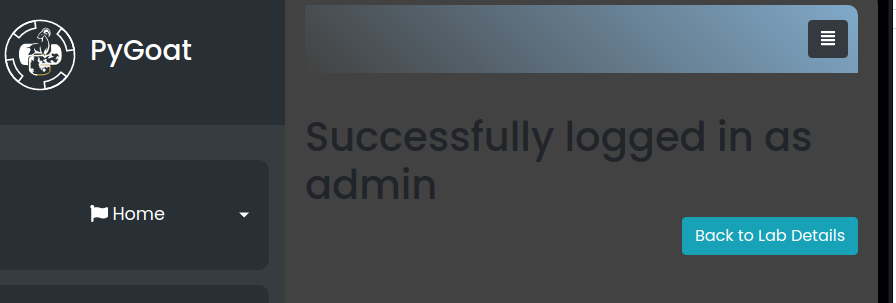
* Theo em nghĩ thì những đoạn mã dài ở trên sẽ là mật khẩu người dùng khi được gửi lên server thì sẽ được 1 thuật toán nào đó để mã hóa



* Khi sử dụng cipher indentifier thì em biết đây là 1 mã hash MD5
* Em nghĩ khi đưa lên SQL server thì mật khẩu người dùng sẽ được hash ra để có thể dễ dàng truy xuất hơn

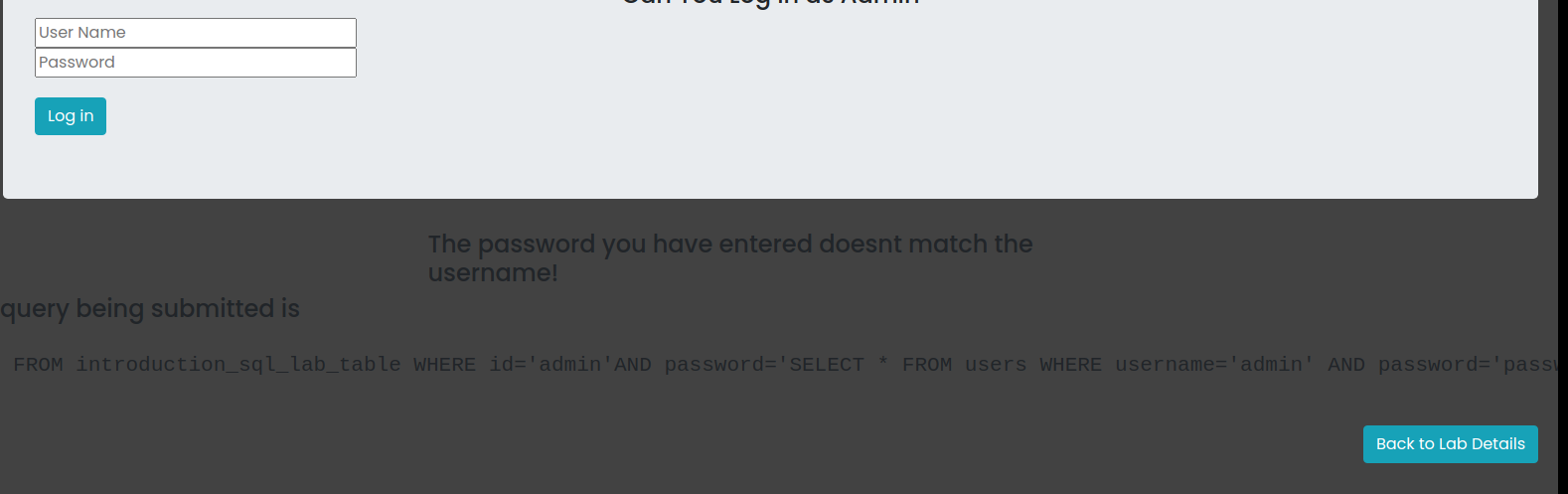


* Và khi tính ngược lại thì ta có được pass của user admin

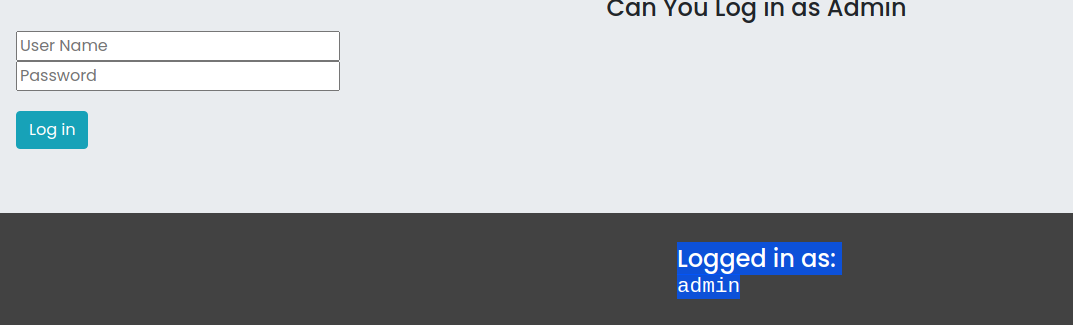


* Sau khi sử dụng username là “admin” và pass “admin1234” mà ta đã tính được ở trên thì ta thành công đăng nhập vào user admin

c) A03:2021 – Injection

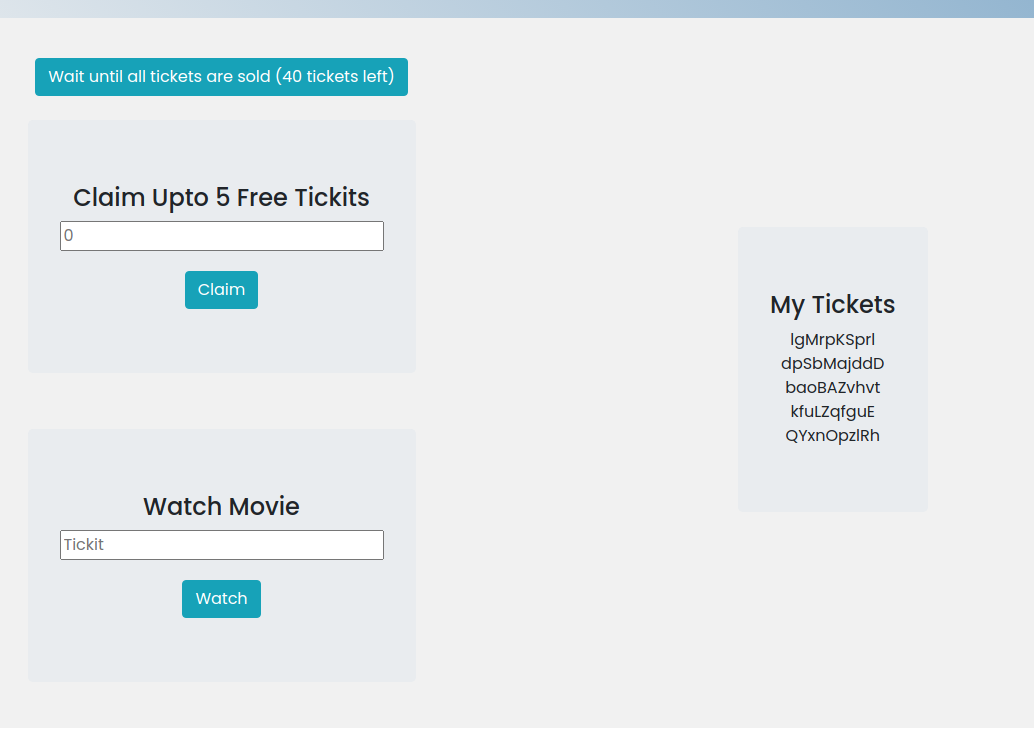


* Khi em thử đăng nhập với username là “admin” và password là 1 câu truy vấn thì em thấy trang web trả về 1 câu truy vấn SELECT trong SQL
* Vậy trang web này có thể khai thác SLQ Injection
* Khi tìm hiểu thì em biết ở đây câu lệnh sẽ truy vấn username=”admin” và password là gì đó
* Ở đây để khai thác SQL Injection ta cần chèn 1 câu lệnh SQL sao đó điều kiện kiểm tra password luôn đúng
* Ở đây em sử dụng câu lệnh: "' 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

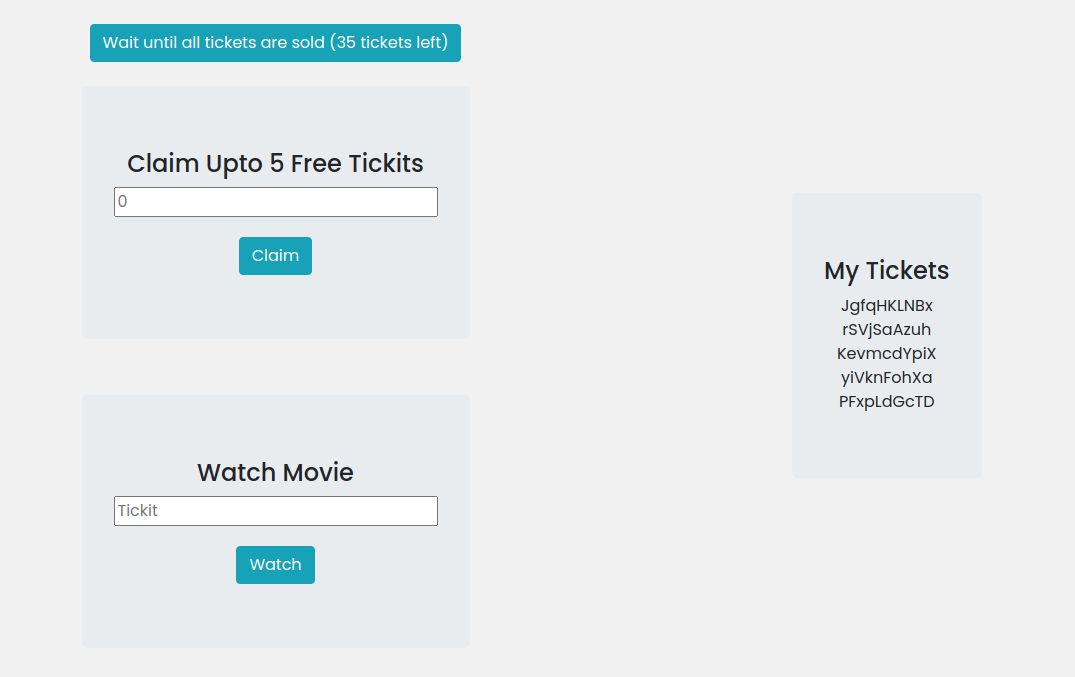


* Kết quả khi thực thi với username là admin và pass là 1 câu truy vấn như ở trên

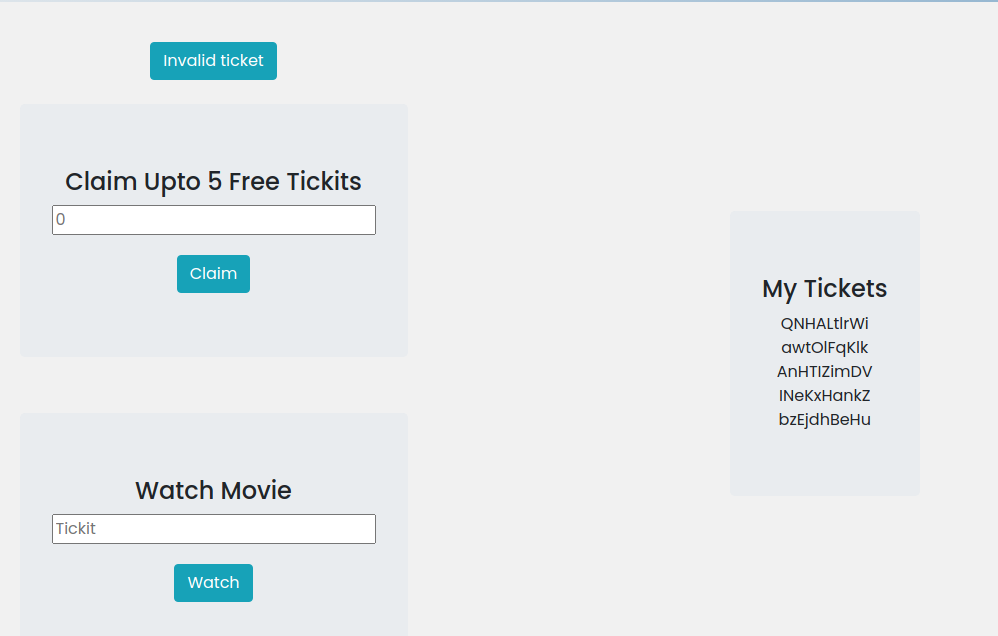
d) A04:2021 – Insecure Design



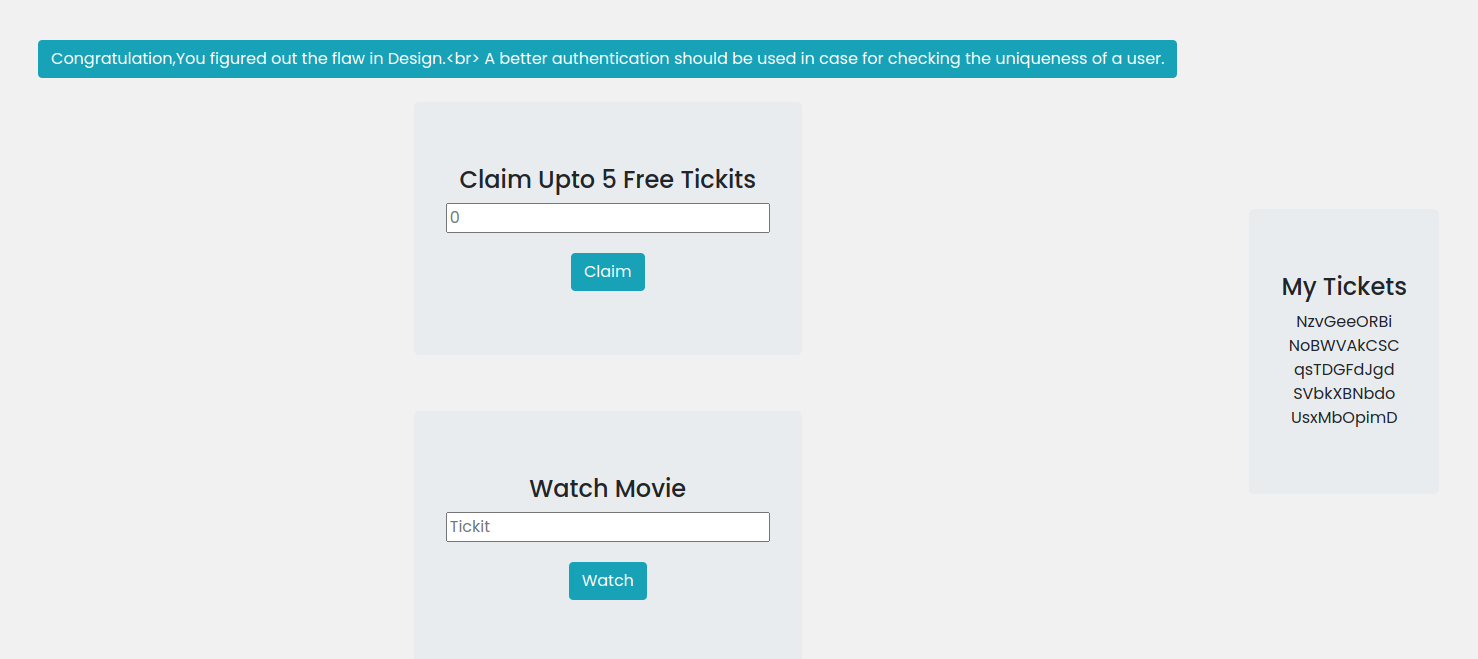
* Ta được 1 trang web để mua vé và mỗi tài khoản có thể có tối đa 5 vé
* Nhưng ta có thể tạo nhiều tài khoản và mỗi tài khoản đều có thể có tối đa 5 vé
* Nên ta cần tạo 12 tài khoản để lấy hết 60 vé để có thể xem phim



* Ta có thể thấy khi dùng 1 tài khoản khác đăng nhập thì số vé vẫn tiếp tục giảm xuống và My Ticket cũng không giống nhau

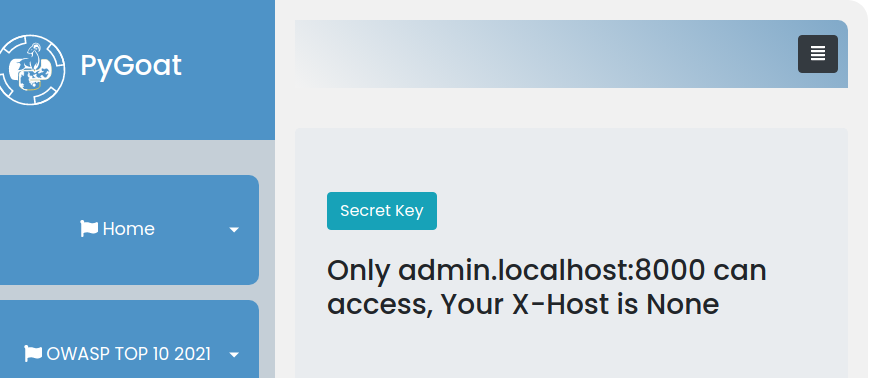


* Sau khi đã mua hết vé thì không thể lấy thêm được nữa

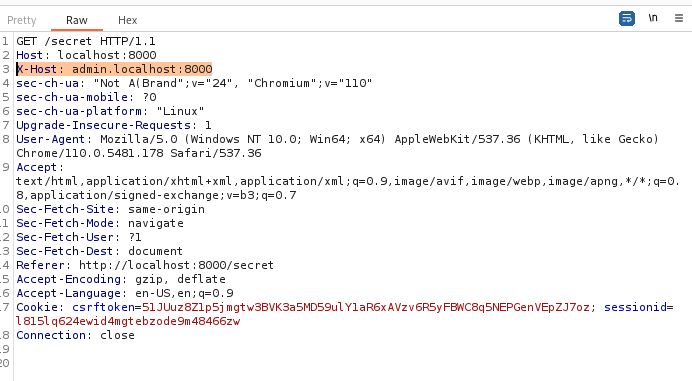


* Ta dùng vé của mình và có thể xem được phim

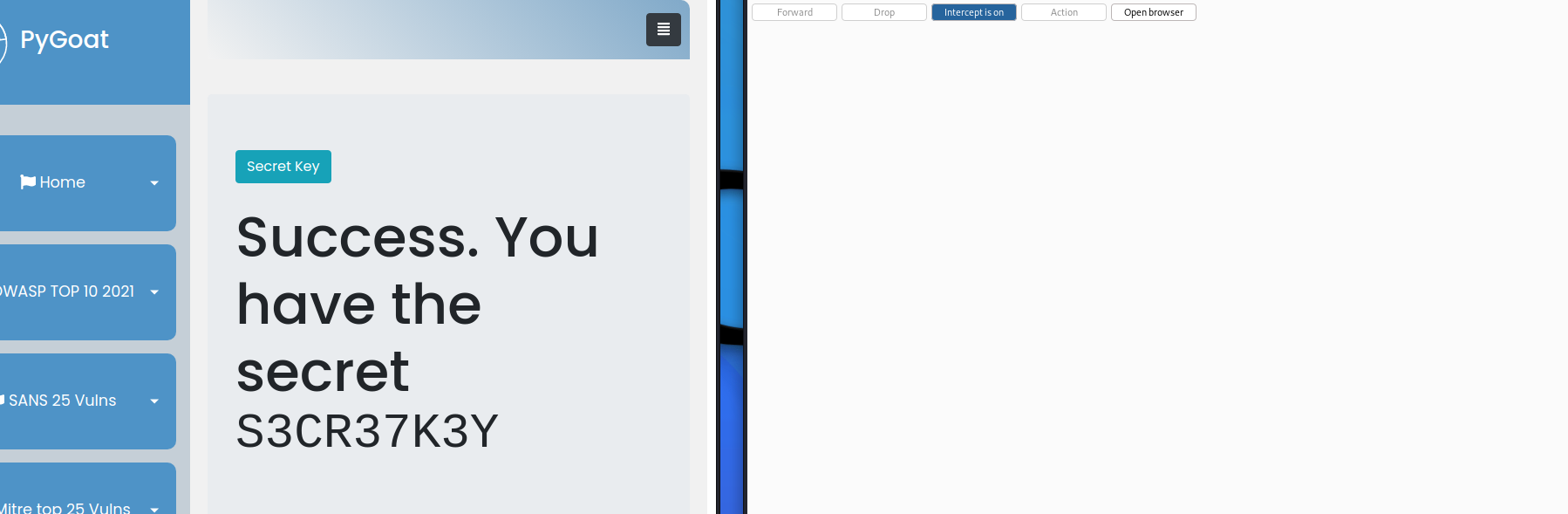
e) A05:2021 – Security Misconfiguration



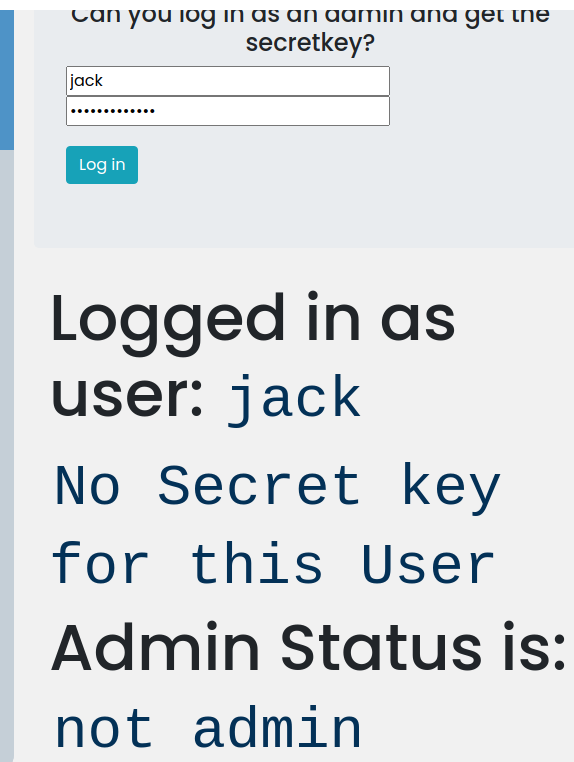
* Ta có được 1 trang web để có thể lấy secretkey
* Nhưng khi ấn thử thì hiện cho ta 1 thông báo đại khái lài chỉ có admin.localhost mới có thể truy cập và X-Host là chưa thiết lập
* Ở đây X-Host là 1 HTTP Header được sử dụng để xác định tên miền hoặc địa chỉ IP của máy chủ chứa tài nguyên trên mạng. 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
* Vậy ở đây ta cần định danh máy chủ là admin.localhost:8000 để có thể lấy được secret key



* Sử dụng burpsite để có thể intercept truy vấn
* Ta thêm trường X-Host và trong HTTP Header để có thể định danh máy chủ



* Sau khi forward thì ta có thể lấy được secret key
* Broken access controll lab 2



* Ta được 1 trang web đăng nhập và sử dụng tài khoản jack và password jacktheripper để có thể truy cập nhưng do không phải admin nên không lấy được secret key

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sau khi xem page source thì ta thấy 1 dòng bảo là admin không dùng các trình duyệt như là chrome hay firefox mà sử dụng pygoat
* Để có thể định danh các trình duyệt này ta cần sử dụng User-agent trong HTTP Header
* User-Agent: là một chuỗi ký tự định danh được sử dụng trong các giao thức mạng để xác định loại trình duyệt hoặc ứng dụng mà người dùng đang sử dụng để truy cập trang web hoặc tài nguyên mạng khác.

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sử dụng burpsite để intercept ta thấy user-agent ở đây là Chrome và Mozilla thì ta cần modified phần này thành pygoat\_admin để có truy cập

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sau đó forward gói tin

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta có thể đăng nhập và user admin và có được secret key
* Broken access control lab 3
* Ta được cấp tài khoản của admin và use John. Yêu cầu là ta phải vào được trang của admin bằng tài khoản của John hoặc không cần tài khoản

Ảnh có chứa Website

Mô tả được tạo tự động

* Đây là khi đăng nhập vào với user John

Ảnh có chứa văn bản

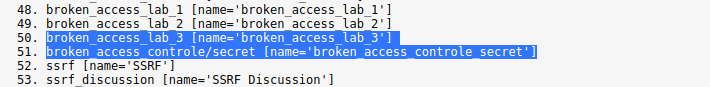
Mô tả được tạo tự động

* Đây là khi đăng nhập vào admin
* Khi nhìn vào URL của 2 trang thì ta thấy admin có 1 thêm 1 subdomain
* Ta thử bên John xem

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Nó hiển thị cho ta 1 trang là không khớp với bất kỳ cái nào trong danh sách



* Ta để ý thấy có 2 tên miền dành cho broken access control và có 1 cái là secret

Ảnh có chứa văn bản, Website

Mô tả được tạo tự động

* Ta đã truy cập được vào trang admin