* Broken access controll lab 2

Ảnh có chứa văn bản

Mô tả được tạo tự động

* 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

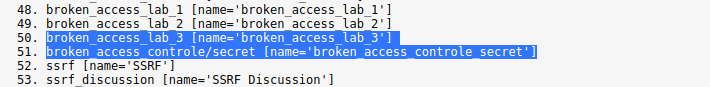
Mô tả được tạo tự động

* 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
* Broken cryptographic failure lab 3

Ảnh có chứa văn bản

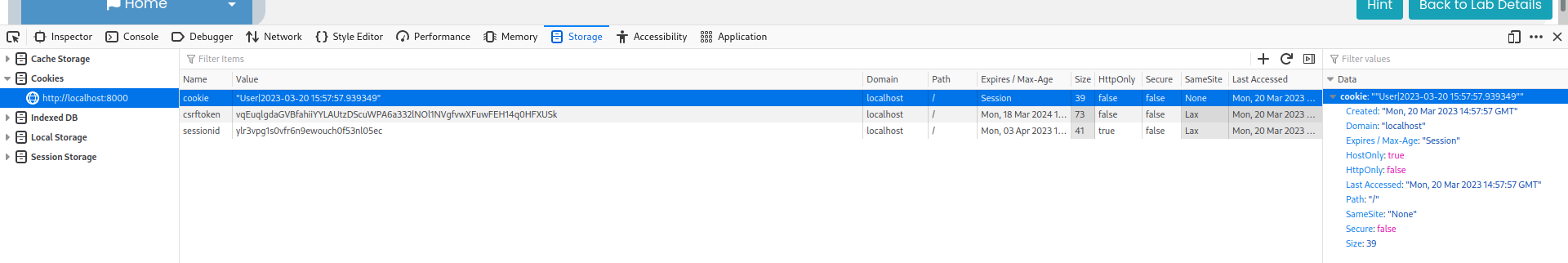
Mô tả được tạo tự động

* Khi truy cập vào challenge ta được 1 tài khoản của user bình thường

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sử dụng để truy cập và thấy không có gì



* Khi ta inspect thử trang web và xem phần storage có thể thấy phần cookie của ta được lưu dưới dạng username|time stamp
* Ta có thể thử đổi username thành admin

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta đã vào được với admin cookie
* Broken cryptographic failure lab 2

Ảnh có chứa văn bản

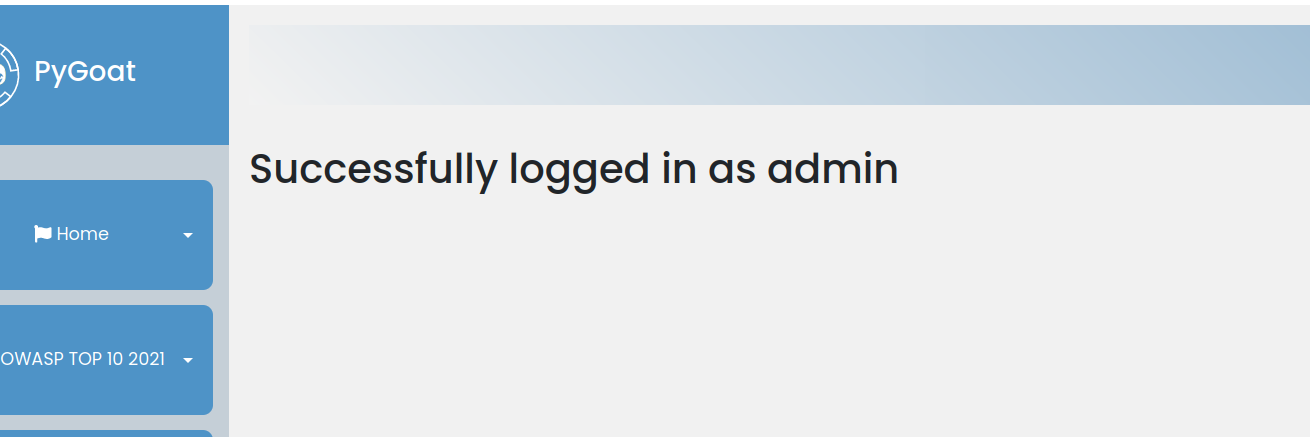
Mô tả được tạo tự động

* Ta được cung cấp username là admin và pass là 1 mã hash dài 64 ký tựẢnh có chứa văn bản

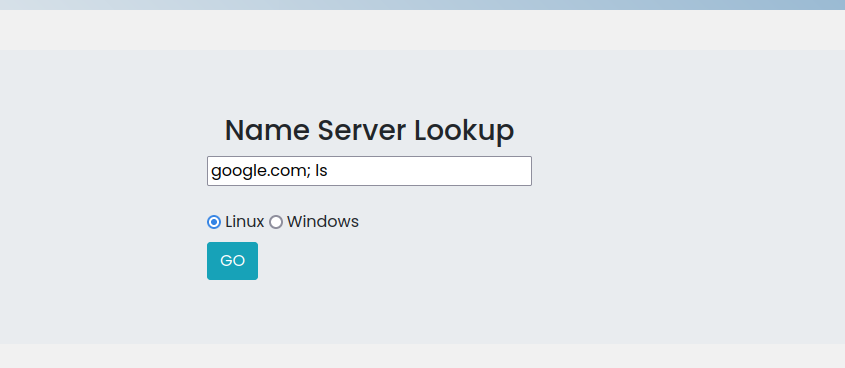
  Mô tả được tạo tự động
* Dùng hash indentifier thì ta biết nó là SHA256



* Sau khi đảo ngược hàm văm admin và tìm trong các từ điển hash trực tuyến thì ta thấy được nó là mã hash của “pasword777”



* CMD\_Lab



* Ở challenge này ta sẽ được cho 1 ô để nhập để tra cứu tên miền đã cho
* Ta sẽ nhập 1 tên miền và máy chủ sẽ thực hiện nslookup và trả lại kết quả cho ta
* Ta có thể chọn hệ điều hành đang chạy là linux hoặc windown
* Ở đây có 1 lỗ hổng là không giới hạn và xác thực đầu vào
* Ta sẽ thêm thử 1 câu lệnh là “ls” sau khi thực hiện tra cứu tên miền

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Kết quả trả về vừa là kết quả của câu lệnh nslookup mà còn là câu lệnh “ls” mà ta đã thêm vào
* Ở đây ta có thể thêm các câu lệnh khác để có thể reverse shell