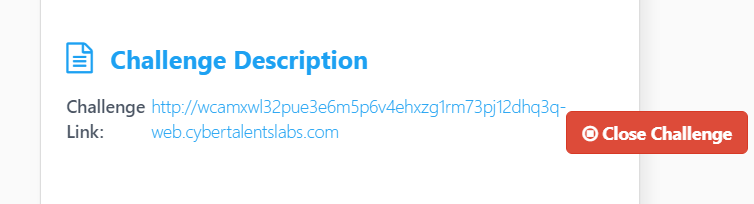
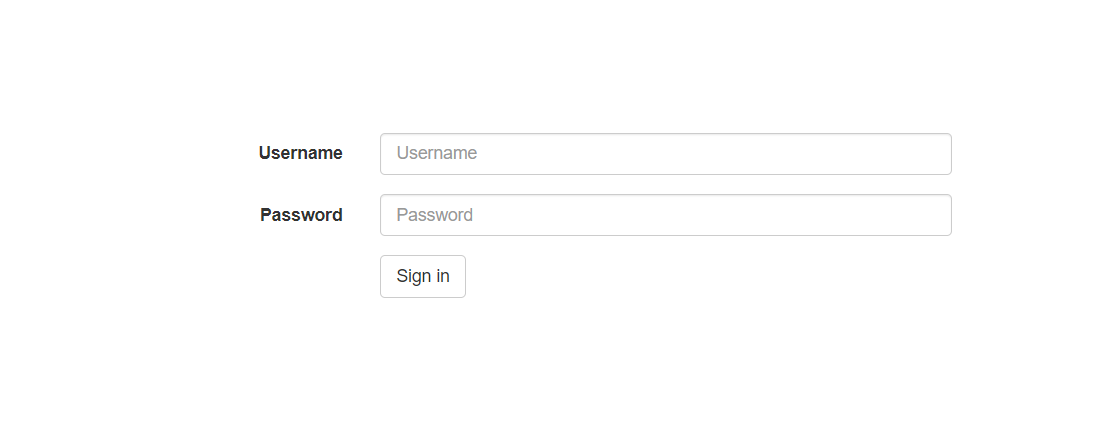
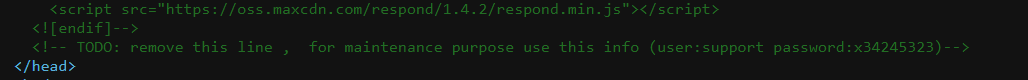
Challenge 1: Admin has the power



* Sau khi ta đăng ký tài khoản và truy cập vào challenge thì ta ấn start challenge
* Sau khi start thì chờ 1 khoảng thời gian trang web sẽ cho ta 1 link trang web



* Yêu cầu ta nhập usernam và password

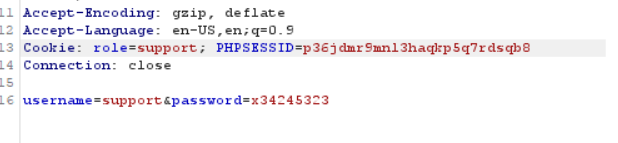


* Ta inspect thử trang web thì thấy có 1 dòng cung cấp ta user: support và password
* Ta dủng username và password để truy cập vào trang web

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Nó yêu cầu ta cần quyền cao hơn quyền support
* Tới đây ta không thể inspect được nữa
* Ta reload lại trang web và bắt lại bằng phần mềm burpsite

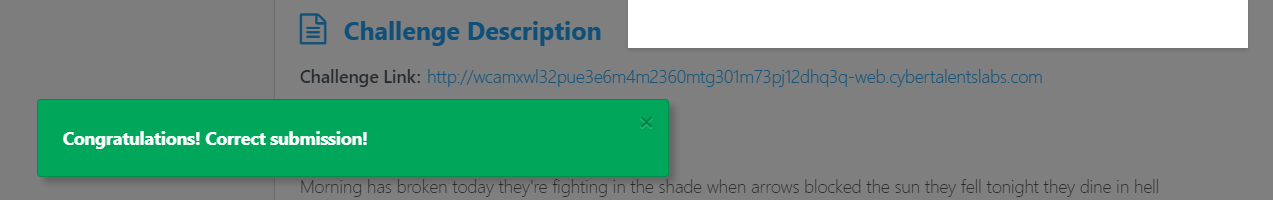


* Ta thấy có 1 dòng cooke có role là support. Ta thử thay đổi thành admin xem sao

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sau khi đổi thành admin và forward gói tin thì ta tới được trang admin và có được flag

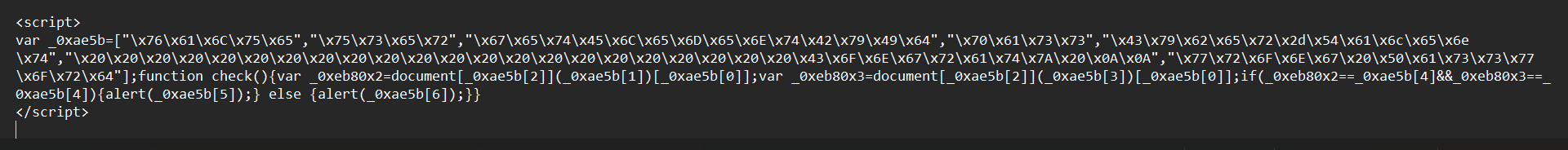


* Kết quả khi submit flag

Challenge 2: This is Sparta



* Sau khi vào link thì ta được 1 trang web đăng nhập



* Khi inspect vào trang web ta thấy có 1 đoạn JavaScript viết về 1 hàm check()
* Có biến var \_0xae5b là 1 chuỗi ký tự đã được mã hóa bằng unicode

Ảnh có chứa văn bản

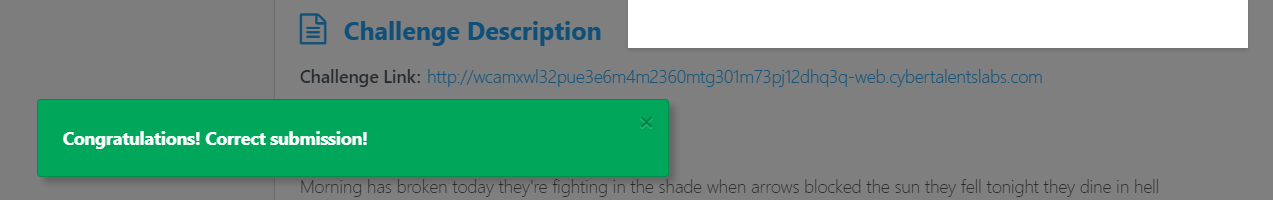
Mô tả được tạo tự động

* Ta thấy nếu value user, và pass đều là Cyber-Talent thì sẽ congratz

Ảnh có chứa văn bản

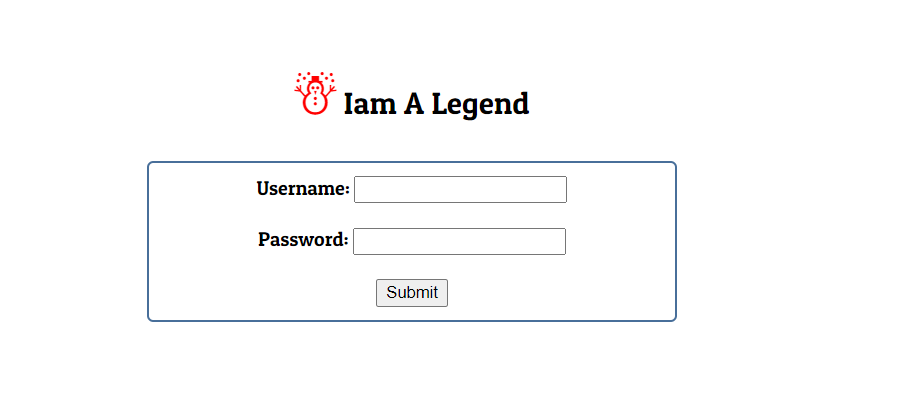
Mô tả được tạo tự động

* Sau khi nhập thì ta thấy xuất hiện flag



* Kết quả khi submit flag

Challenge 3: I am legend



* Khi truy cập vào link thì ta được 1 trang web đăng nhập

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Khi inspect thì ta thấy 1 đoạn script được mã hóa rất khó đọc
* Khi tìm hiểu thì đây là đoạn mã được viết bằng JSFuck
* Khi tìm kiếm 1 hồi các công cụ giải mã thì em tìm được 1 link

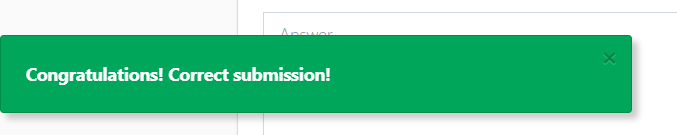
<https://lelinhtinh.github.io/de4js/>

* Khi giải mã thì ta được

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta có được flag



* Kết quả khi submit định dạng Flag đúng

Challenge 4: Cool Name effect

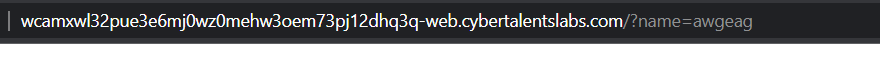
Ảnh có chứa văn bản

Mô tả được tạo tự động

* Khi truy cập vào link trang web ta được 1 trang có thể nhập bất cứ thứ gì

Ảnh có chứa văn bản

Mô tả được tạo tự động



* Khi nhìn lên thanh tìm kiếm thì ta thấy những gì ta nhập cũng được chèn vào trang web
* Khi tìm hiểu thì em biết đây là cách để có thể khai thác XSS để có thể bypass filter để ta có thể chèn vào 1 đoạn mã JavaScript để thực hiện ý đồ của mình

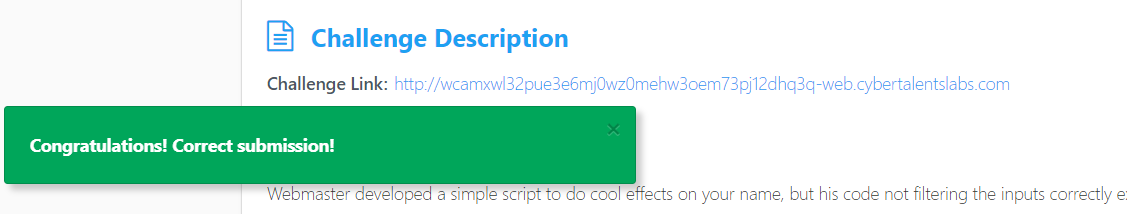
<https://nhattruong.blog/2016/11/08/mot-so-cach-bypass-xss-cua-zseano/>

* Em có tìm thấy 1 trang web để bypass filter và nó đã thành công

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sau khi nhập để bypass filter thì ta có được flag

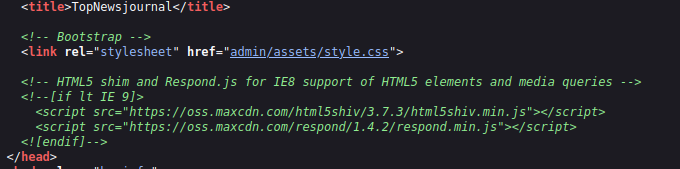


* Kết quả khi submit flag

Challenge 5: Encrypted Database



* Truy cập vào trang web được cấp thì ta thấy 1 trang bình thường
* Khi truy cập vào các tag cụng không có gì lạ
* Ta inspect thử trang web



* Ta thấy có 1 đường dẫn admin ta truy cập thử

Ảnh có chứa văn bản

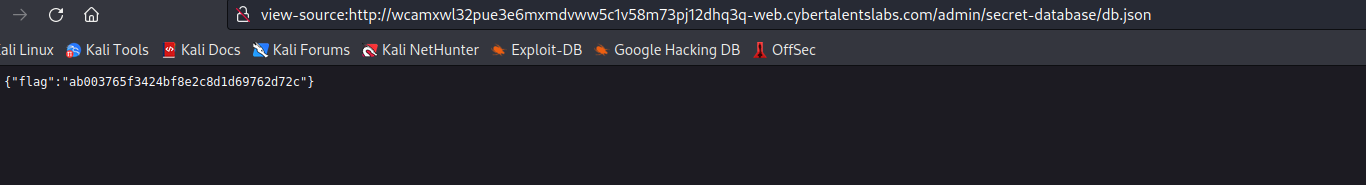
Mô tả được tạo tự động

* Không có gì hết

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Nhưng khi về đường dẫn admin thì ta thấy có 1 giá trị value là secret-database/db.json



* Ta truy cập vào thì thấy được flag
* Nhưng khi nộp thì lại sai do flag đã được mã hóa
* Ta dùng cipher indentify để xác định thì nó là MD5

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sau khi giải mã thì ta được flag là “badboy”
* Challenge 6: Encrypted Database

Ảnh có chứa văn bản

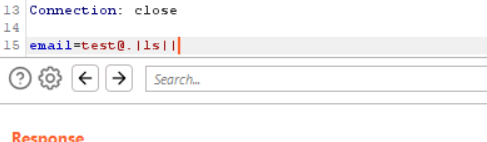
Mô tả được tạo tự động

* Khi truy cập vào trang web thì nó hiện cho ta 1 ô để nhập email và không chấp nhận nếu không có ký tự “@” và “.”

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta dùng burpsite để bắt gói tin sau đó gửi đến repeater

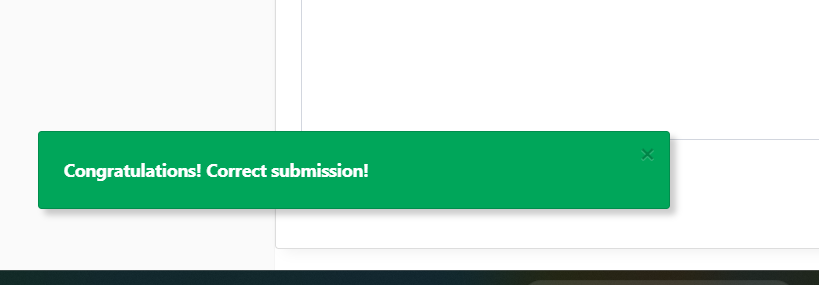


* Ta thử thực thi 1 lệnh trên hệ thống

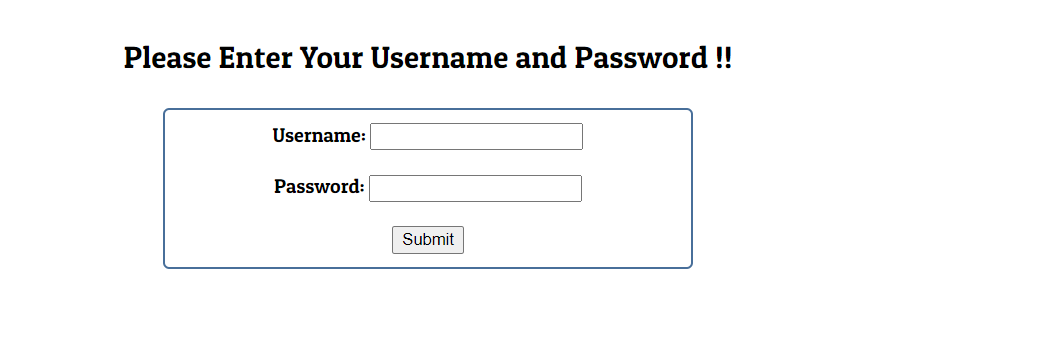
Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta thấy trang trả về 1 file .gz đó là flag của mình



* Challenge 7: Who am i



* Khi truy cập vào challenge thì ta có 1 trang web đăng nhập

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Khi inspect thì ta thấy được tài khoản Guest

Ảnh có chứa văn bản

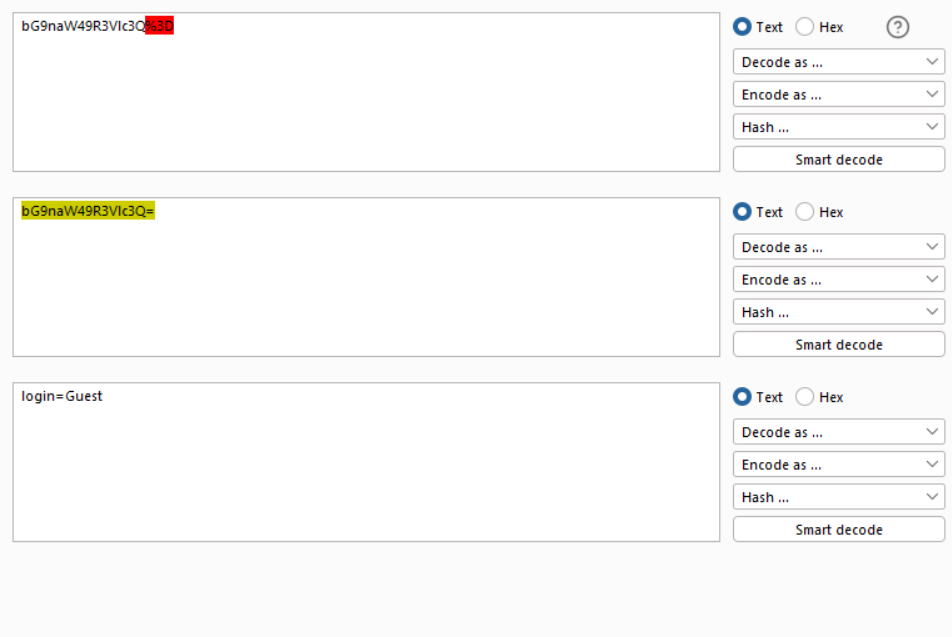
Mô tả được tạo tự động

* Ta thấy acces denied do không phải tài khoản admin

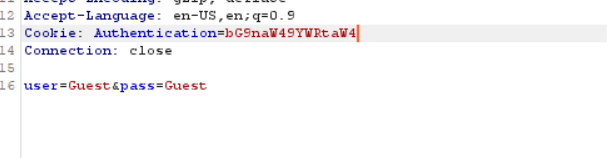
Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta thấy có phần Authentication trong cookie
* Khi giải mã thì ta thấy



* Cookie được lưu ở dạng base 64 với login=guest nên ta thay đổi login thành admin sau đó encode lại ở dạng base 64

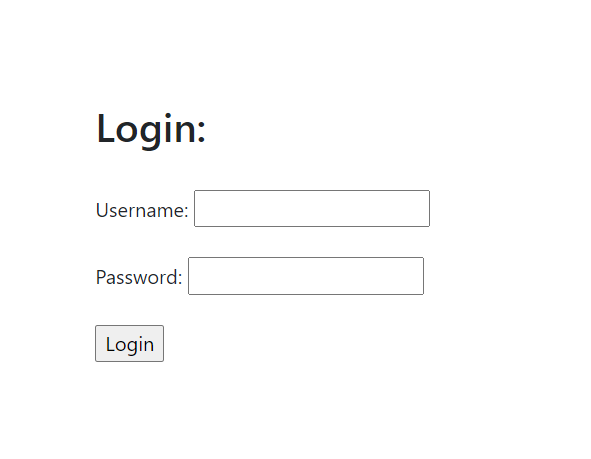


* Thay thế cookie cũ bằng cái mới

Ảnh có chứa văn bản

Mô tả được tạo tự động

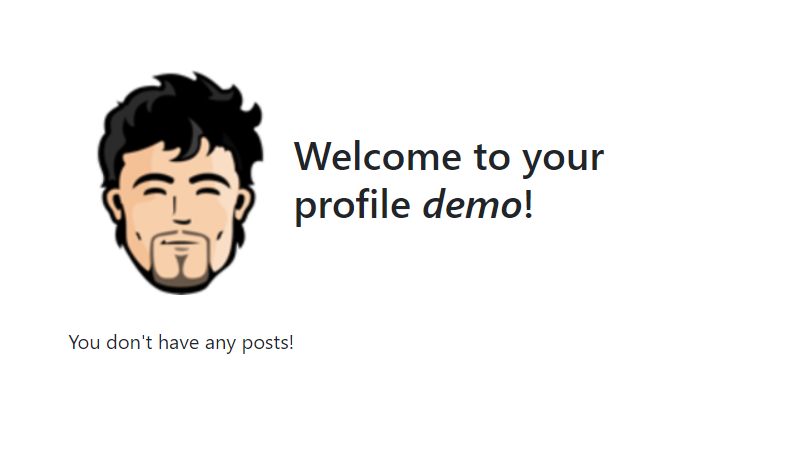
* Kết quả ta đã ở admin và có được flag
* Challenge 8: Blue Inc.



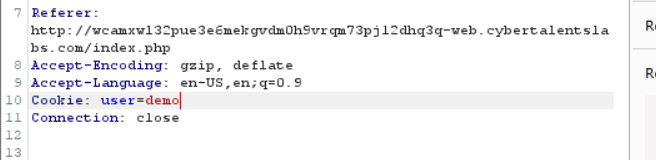
* Khi truy cập vào trang web thì ta thấy có phần login
* Ta dùng tài khoản demo được cung cấp trong challege để truy cập

Ảnh có chứa văn bản

Mô tả được tạo tự động



* Khi qua profile ta thấy không có gì nhưng khi dùng burpsite bắt trước khi vào profie



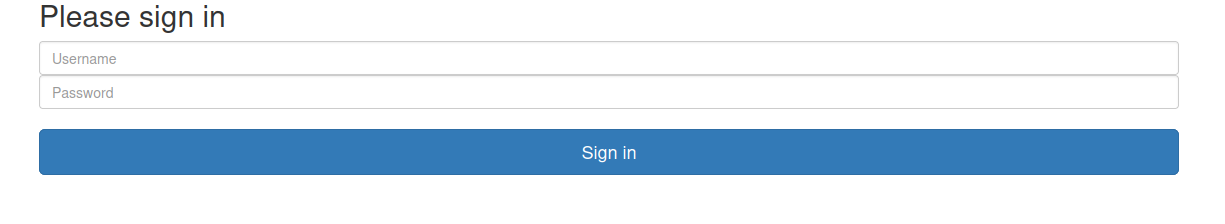
* Ta thấy cookie với user là demo
* Ta thay đổi demo thành admin xem sao

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Và ta đã thấy được flag trong profile của admin

Challenge 9: Easy Message



* Khi truy cập vào challenge ta được 1 trang web đăng nhập và không có gì thêm
* Em đã thử inspect cũng như burpsite nhưng không có thông tin gì hữu ích
* Tới đây em dùng dirsearch để xem các subdomain

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Khi đã thử qua các subdomain thì có /robots.txt có thông tin

Ảnh có chứa văn bản

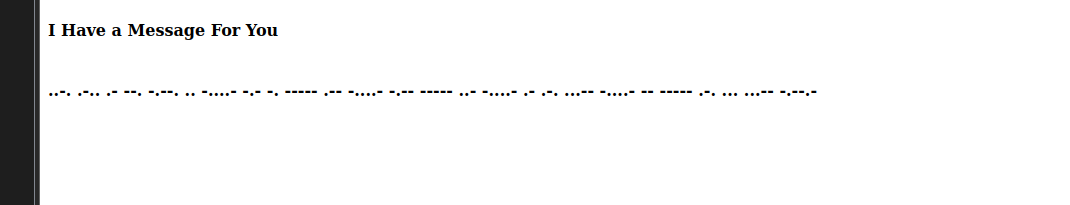
Mô tả được tạo tự động

* Khi thay thế /robots.txt ta được 1 trang web chứa mã PHP

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Mã cho ta biết nếu username và pass là “Cyber-Talent” sau khi được mã hóa base64 thì ta sẽ đi tới hàm succes\_login()



* Khi đăng nhập vào thì ta được 1 mã Morse

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Khi giải mã thì ta có được flag

Challenge 10: Cheers

Ảnh có chứa văn bản

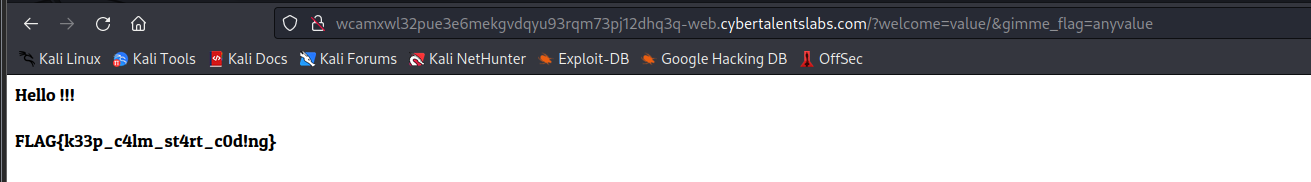
Mô tả được tạo tự động

* Khi truy cập vào challenge thì được 1 trang xuất hiện lỗi
* Lỗi này ta chỉ việc thêm ?welcome=value vào URL là được

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta được 1 lỗi khác
* Ta thêm &gimme\_flag=anyvalue vào URL và nhấn enter



- Tới đây ta có được flag

Challenge 11: Got Controls

Ảnh có chứa văn bản

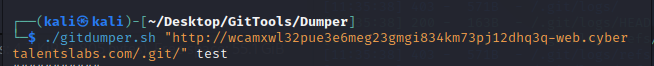
Mô tả được tạo tự động

* Khi truy cập challenge ta thấy được 1 trang web và có 1 subdomain dẫn đến flag.php

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Khi truy cập vào thì ta không thể xem file này trực tiếp được
* Tới đây ta sẽ sử dụng 1 tool để xem các thư mục git



* Nó sẽ lưu vào folder test mà mình đặt tên
* Sau đó ta cũng sử dụng tool này để trích xuất các tệp đối tượng trong thư mục con

Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sau khi trích xuất vào trong folder dst thì ta di chuyển vào và có 1 foler

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Tới đây ta có được flag

Challenge 12: Easy Access

Ảnh có chứa văn bản

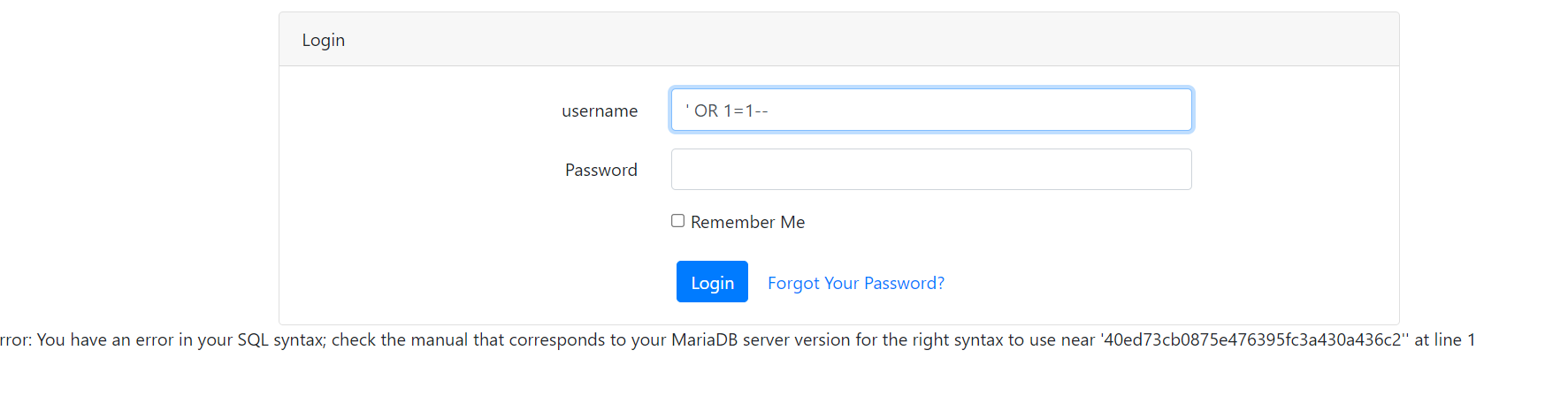
Mô tả được tạo tự động

* Khi truy cập thử thách ta có được 1 form đăng nhập

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta inspect thử thì có được username và password
* Nhưng cũng không có tác dụng gì nhiều
* Ta dùng thử burpsite thì cũng không có gì đặc biệt



* Khi nhập thử không đúng thì ta thấy invalid password
* Ý tưởng là sử dụng SQL injection
* Phần password có 1 đoạn script để chuyển password thành MD5 hash nhưng ký tự đầu tiên là ‘ nhưng ở cuối thì lại không có ký tự để đóng
* Ta thử Admin' OR '1'='1' ' ký tự cuối là để đóng ta không cần nhập gì vào password hoặc nhập bất kỳ gì cũng được và ta có được flag

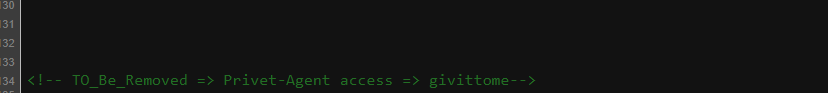
Ảnh có chứa văn bản

Mô tả được tạo tự động

Challenge 13: Private Agent



* Khi truy cập thì trang web bảo ta phải là private agent mới có thể vào



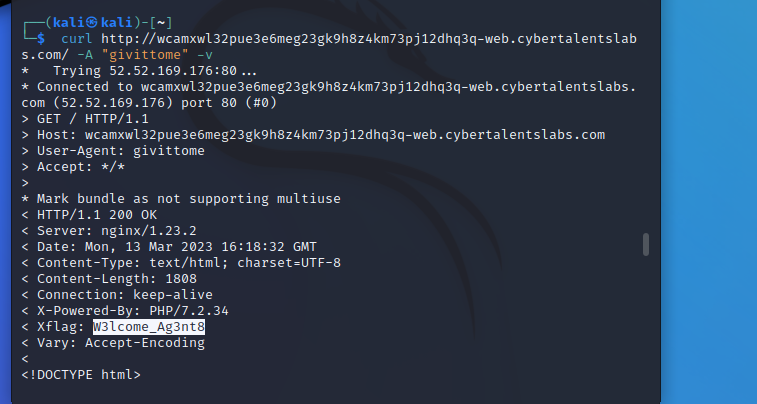
* Khi inspect thì ta thấy agent là givitome thì có thể là private agent

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta thêm vào trong trường user-agent





Ta dùng curl với usergent và -v để xem header và thấy có flag