**HTML INJECTION REFLECTED**

* Giới thiệu qua về HTML injection. HTML injection Là một loại tấn công mà hacker sẽ tiêm những code HTML vào website thông qua những lỗ hổng, với mục đích thay đổi thiết kế hoặc một số thông tin của website, rồi hiển thị cho user. Kết quả, user có thể nhìn thấy những dữ liệu mà hacker đã gửi.
* Những dữ liệu này sẽ khác nhau dựa vào loại tấn công. Nó có thể là 1 vài thẻ HTML, cũng có thể là 1 form hoặc 1 trang web fake. Khi tấn công xảy ra, trình duyệt sẽ hiển thị dữ liệu mà hacker đã tiêm vào
* Các loại HTML Injection chủ yếu là:

Tấn công HTML lưu trữ (stored HTML Injection)

Tấn công HTML phản ánh (reflected HTML Injection)

1. Stored HTML Injection:

Stored HTML injection xảy ra khi đoạn mã HTML độc hại được lưu trữ vào web server và được thực thi mỗi khi user gọi một tính năng phù hợp. Loại tấn công này thường ảnh hưởng đến nhiều người dùng.

2. Reflected HTML Injection:

Với loại tấn công này, các mã độc không được lưu trữ vĩnh viễn trên web server. Reflected HTML Injection xảy ra khi website phản hồi ngay lập tức với đầu vào độc hại. Loại tấn công này thường ảnh hưởng đến từng người dùng độc lập.

Có thể chia thành các loại sau:

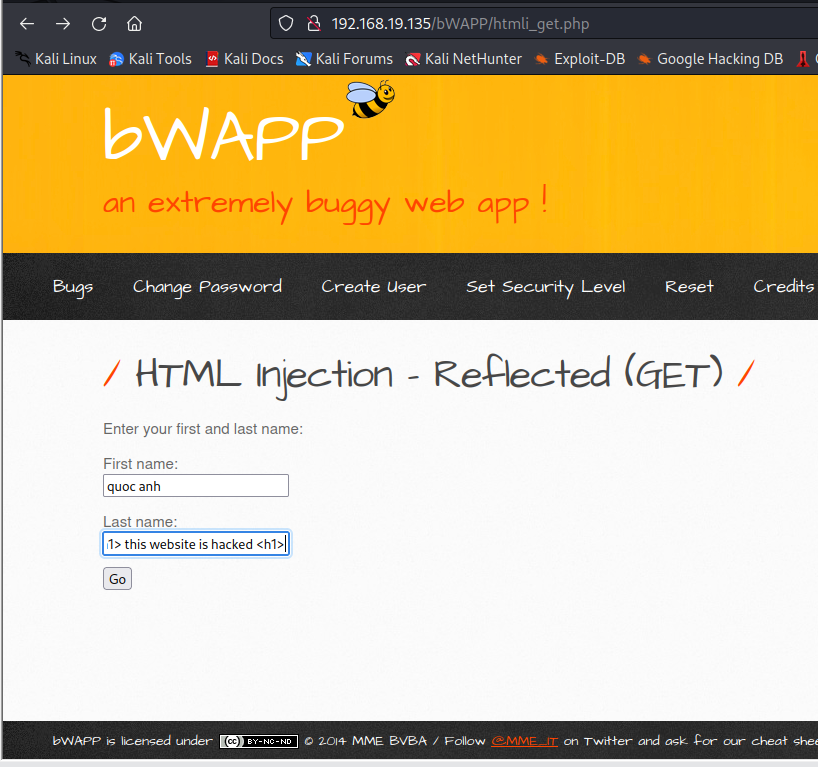
Reflected GET

Reflected POST

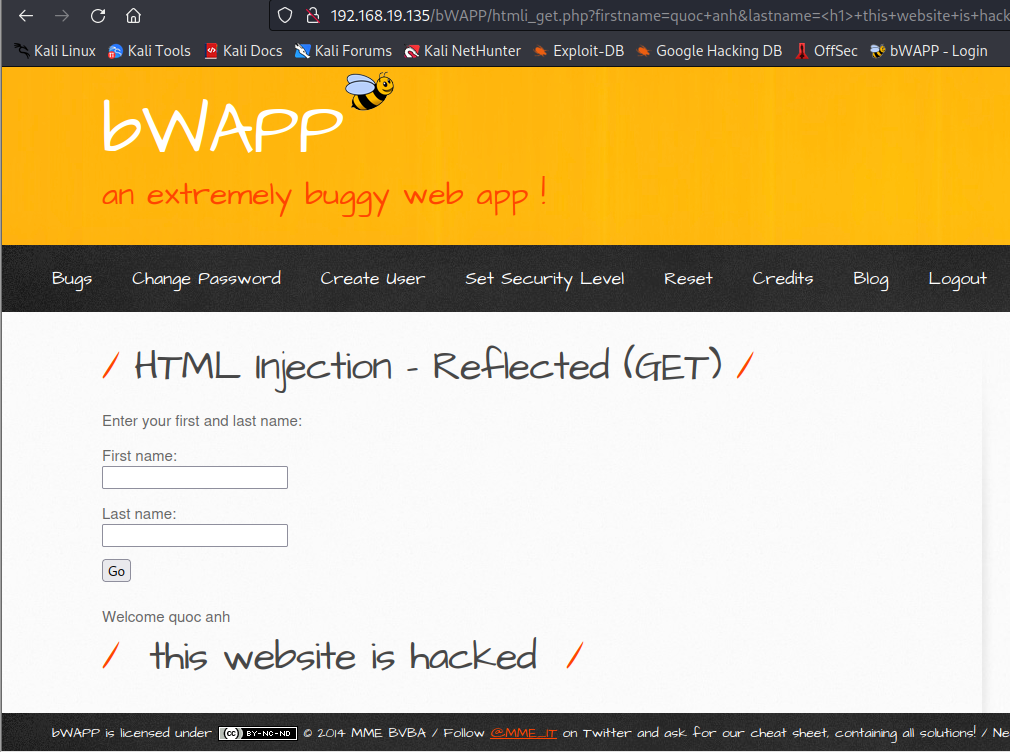
Reflected URL

Bài Lab lần này của mình sẽ tập trung vào HTML injection reflected trên bwapp

1. **Reflected Get**



Đây là giao diện trang web có chứa html reflected. Nhiệm vụ của ta là chèn 1 đoạn lệnh bằng code html với những cú pháp như <p>enter your text </p>,<h1> enter your text</h1> hoặc <a href="https://www.facebook.com">This is a link</a>- code chuyển hướng đến 1 trang web khác. Ta sẽ thử đưa các câu lệnh này vào những chỗ nhập thông tin người dùng qua phương thức get



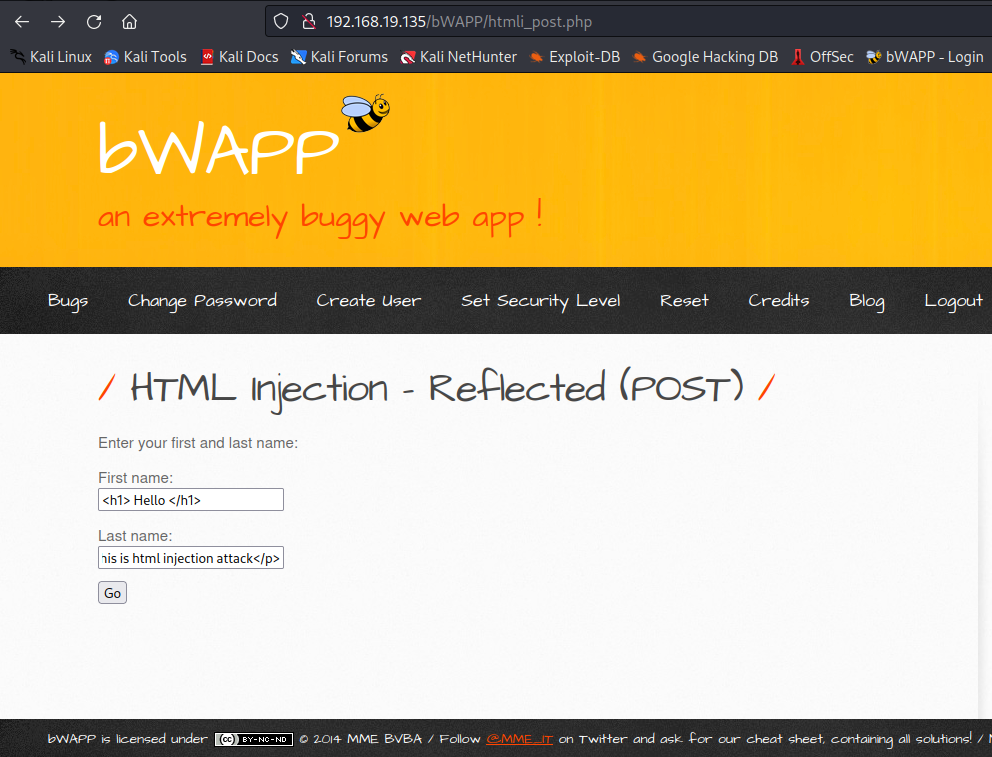
Kết quả sau khi chèn, trang web đã hiển thị thông tin theo mong muốn của ta



Kết qua sau khi chèn <a href="https://www.facebook.com">This is a link</a>

1. **Reflected post**

Tương tự như ở reflected get, ta sẽ chèn câu lệnh html ở 2 mục firstname và last name





Kết quả trả về…