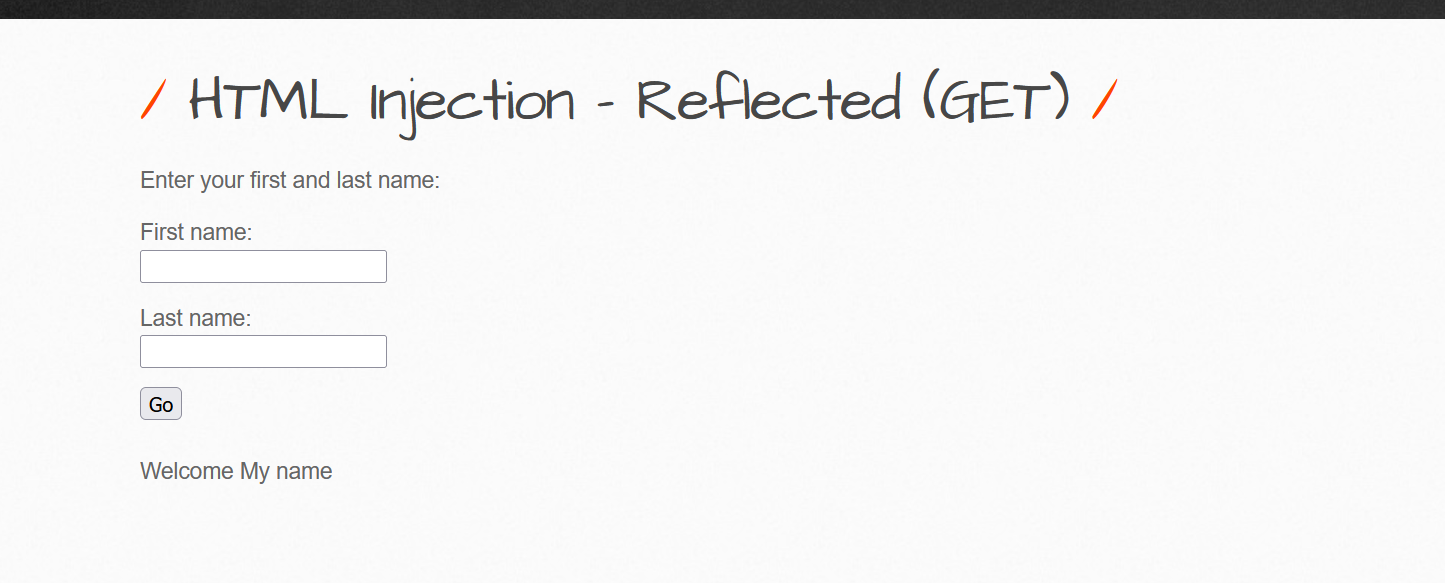
**\* HTML Injection – Reflected (GET):**

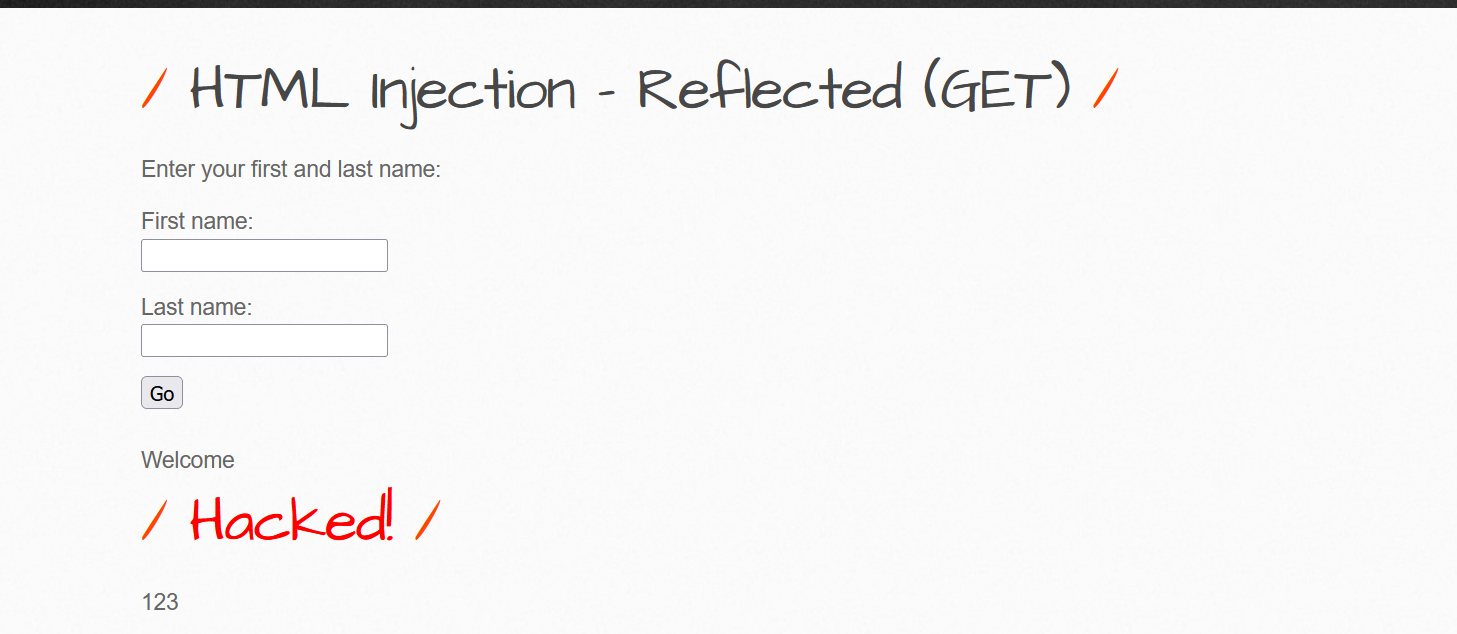
 Đây là dạng tấn công **chèn mã HTML (hoặc JS nhẹ)** vào **tham số GET (trên URL)**.

 Server **không lọc dữ liệu đầu vào**, nên mã HTML bạn nhập sẽ **được phản hồi nguyên xi vào trang web**.

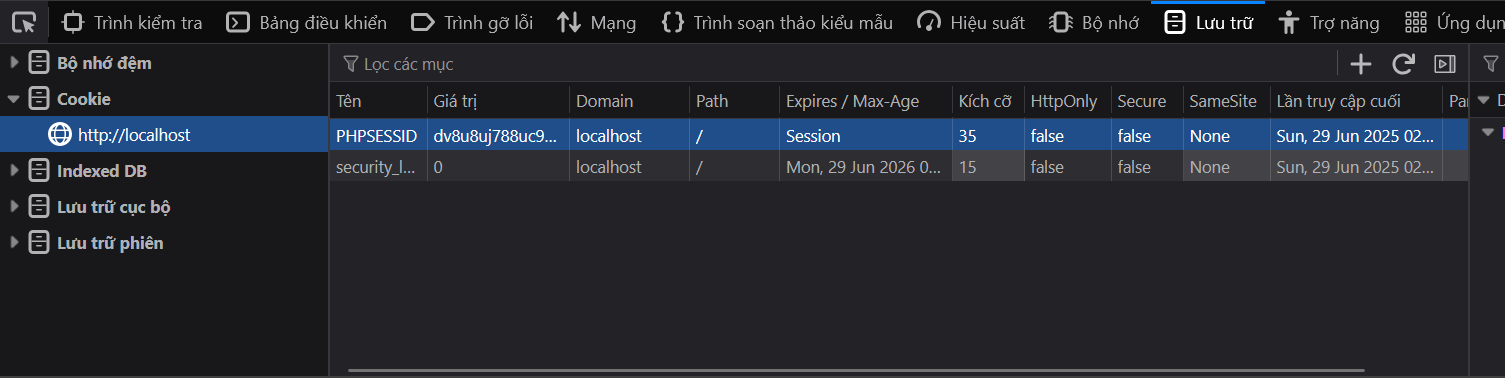
 Khi người dùng khác truy cập URL độc đó → **mã HTML của bạn sẽ được hiển thị**.

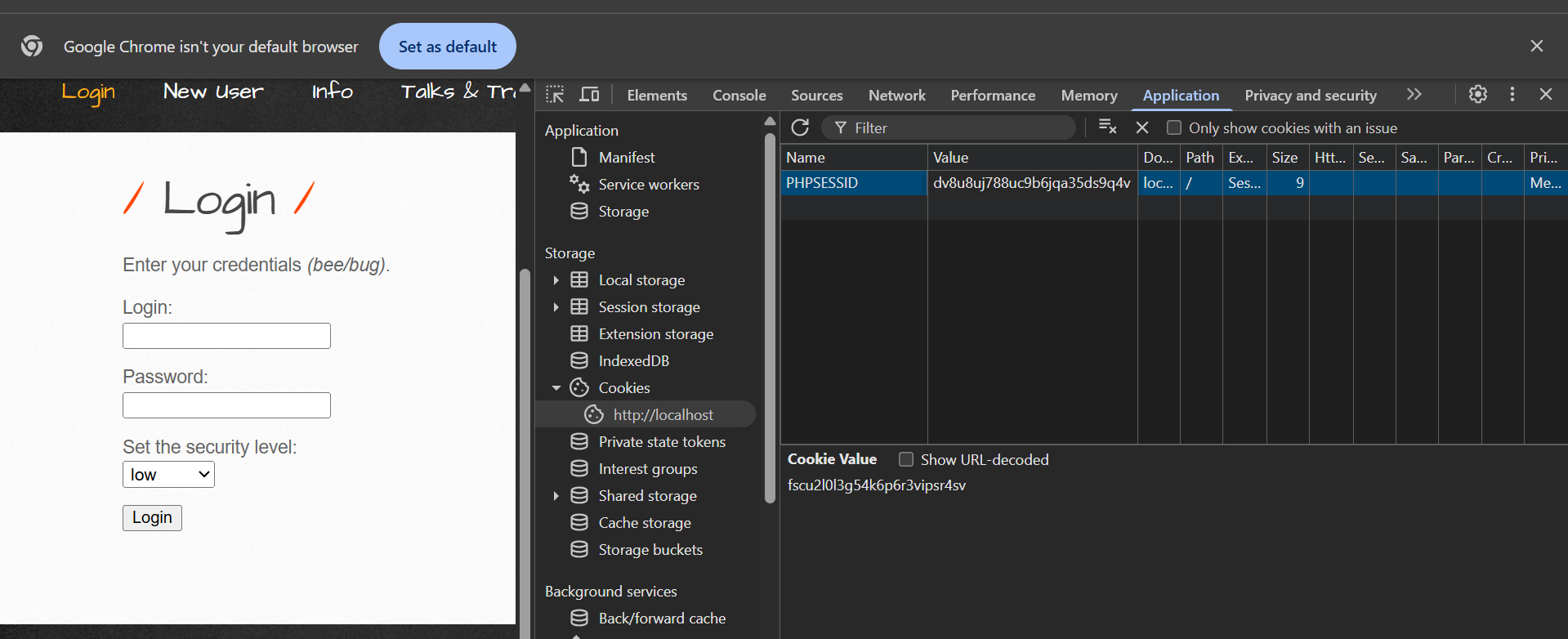
Trang web bình thường:  


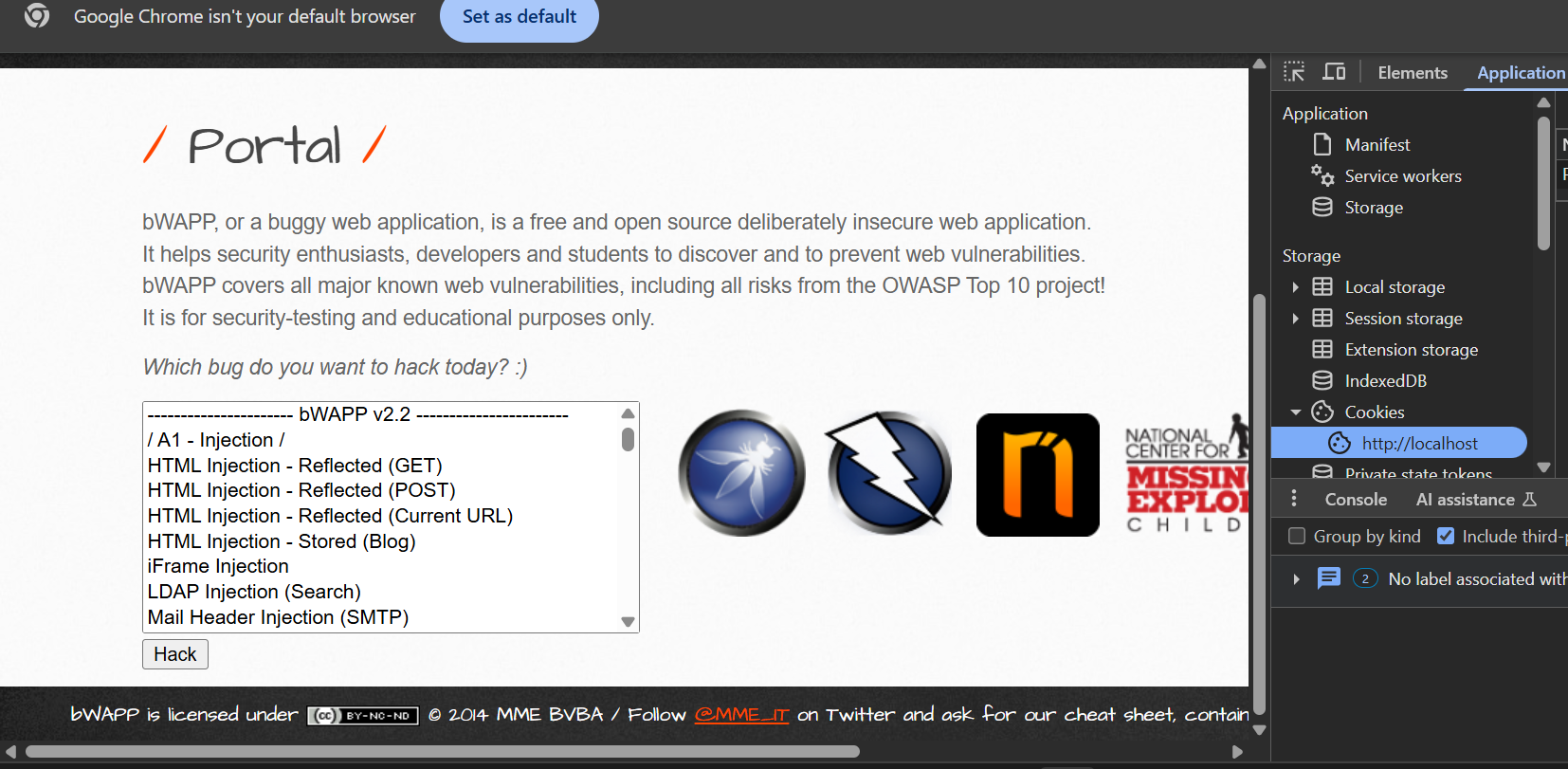
Thực hiện chèn mã độc:  


Kết quả:  


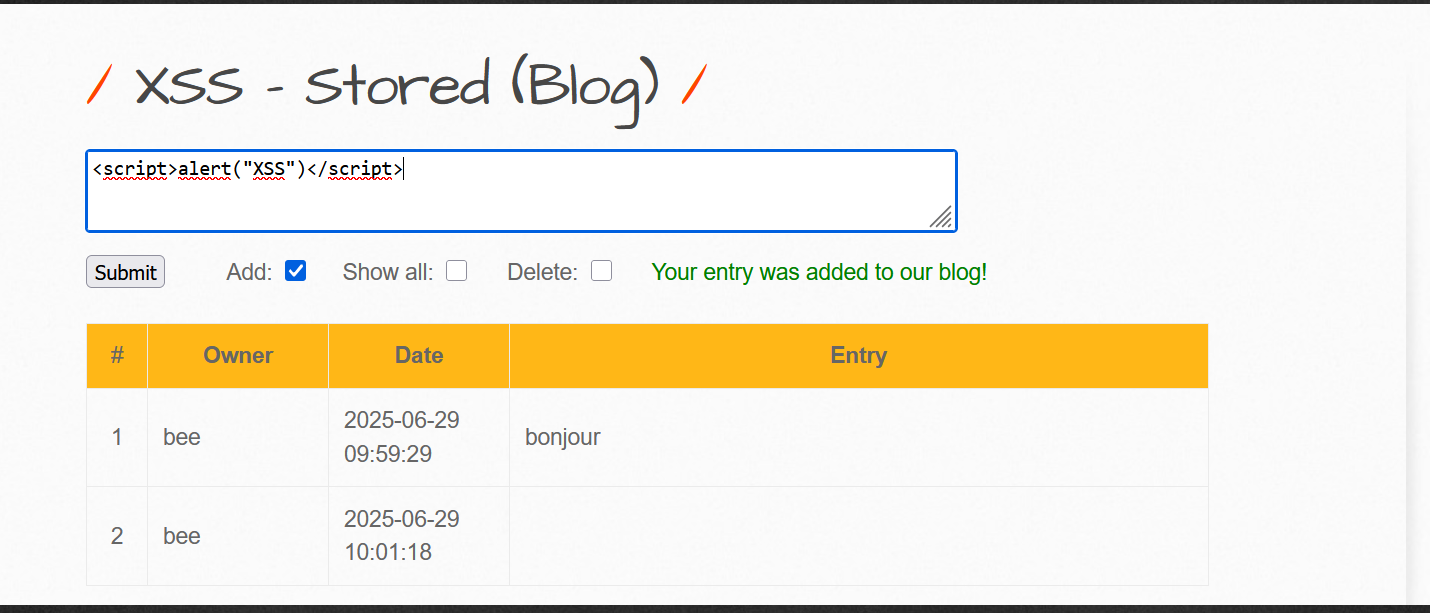
**\* Broken Authentication – Cookie (Secure):**

- Kịch bản giả lập: hacker chiếm được cookie của user và sử dụng cookie đó để chiếm phiên.





**\* XSS – Stored (Blog):** Hacker **chèn mã JavaScript độc hại** vào nội dung bài viết, comment blog, hoặc message. Mã độc này **được lưu (stored)** lại trong **CSDL** hoặc file **→ và sẽ tự động thực thi mỗi khi người dùng khác mở trang đó.**



**\* IDOR - (Insecure Direct Object Reference)**

Là khi một ứng dụng **web truy cập trực tiếp đến tài nguyên (file, bản ghi, thông tin)** thông qua ID như ?id=123, nhưng **không kiểm tra quyền truy cập** của người dùng.

