**REPORT**

**VULNBLOG**

**Reflected XSS**

Reflected XSS là lỗ hổng XSS khai thác thông qua các tham số được phản chiếu lại với người dùng. Ví dụ như một trang web có chức năng tìm kiếm và truy vấn được thực hiện qua tham số search. Nếu tham số search được phản chiếu lại với người dùng và nó không được kiểm soát để tránh các kĩ thuật tấn công XSS. Thì chúng ta có thể tấn công XSS thông qua các tham số này, ví dụ như lừa người dùng nhấp vào link:

http://example.com/?search=<script>alert(1)</script>

**Stored XSS**

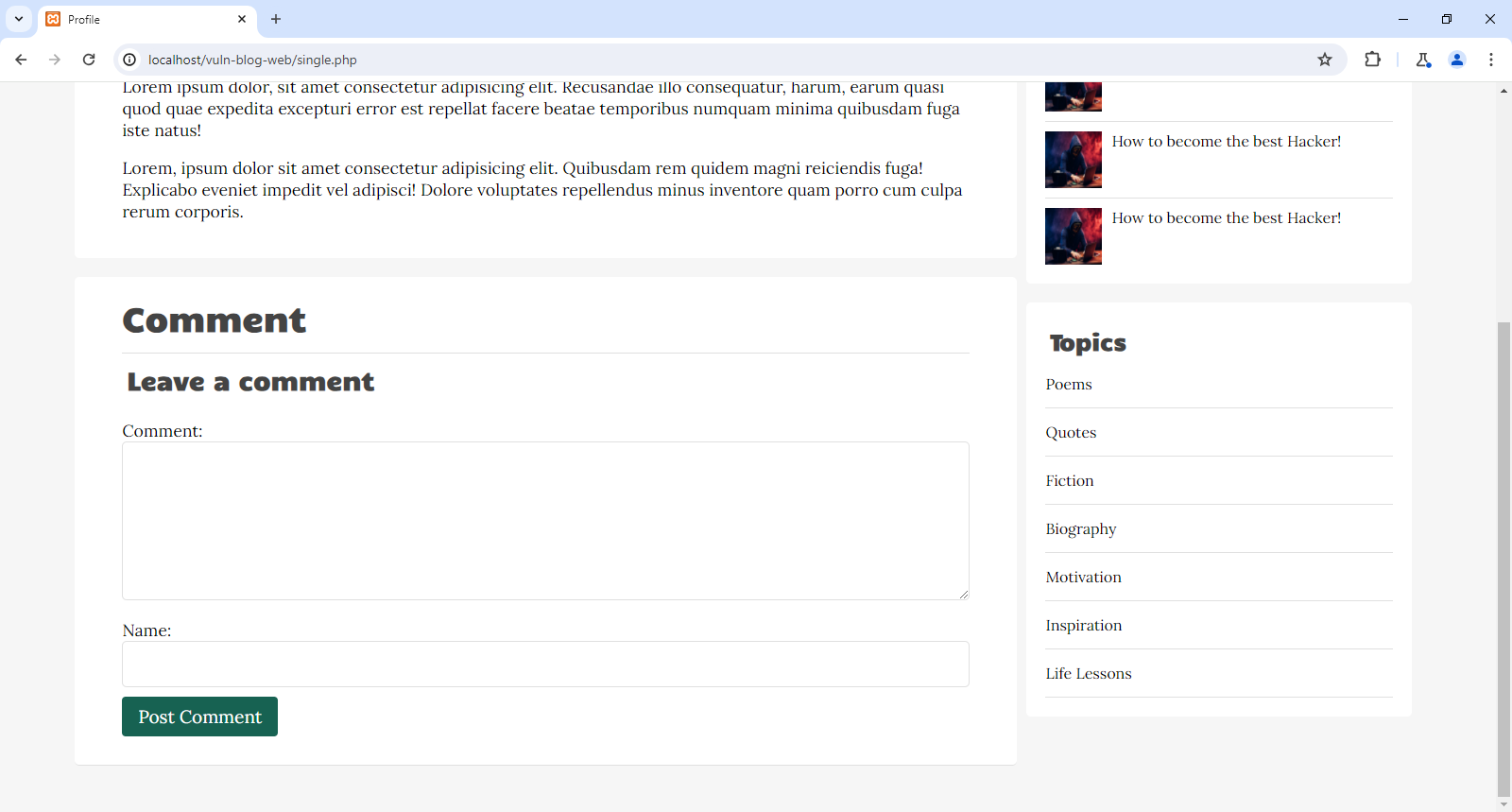
Stored XSS là lỗ hổng khai thác các phần sẽ được lưu vào cơ sở dữ liệu khi được thực hiện. Ví dụ như phần comment, các chức năng đăng kí, đăng nhập,... Khi này, chúng ta có thể khai thác bằng cách inject các đoạn script như <script>alert(1)</script>. Nếu người dùng vô tình truy cập vào các phần comment hoặc tên của một người dùng bị inject thì sẽ bị khai thác dữ liệu.

**Dom Based XSS**

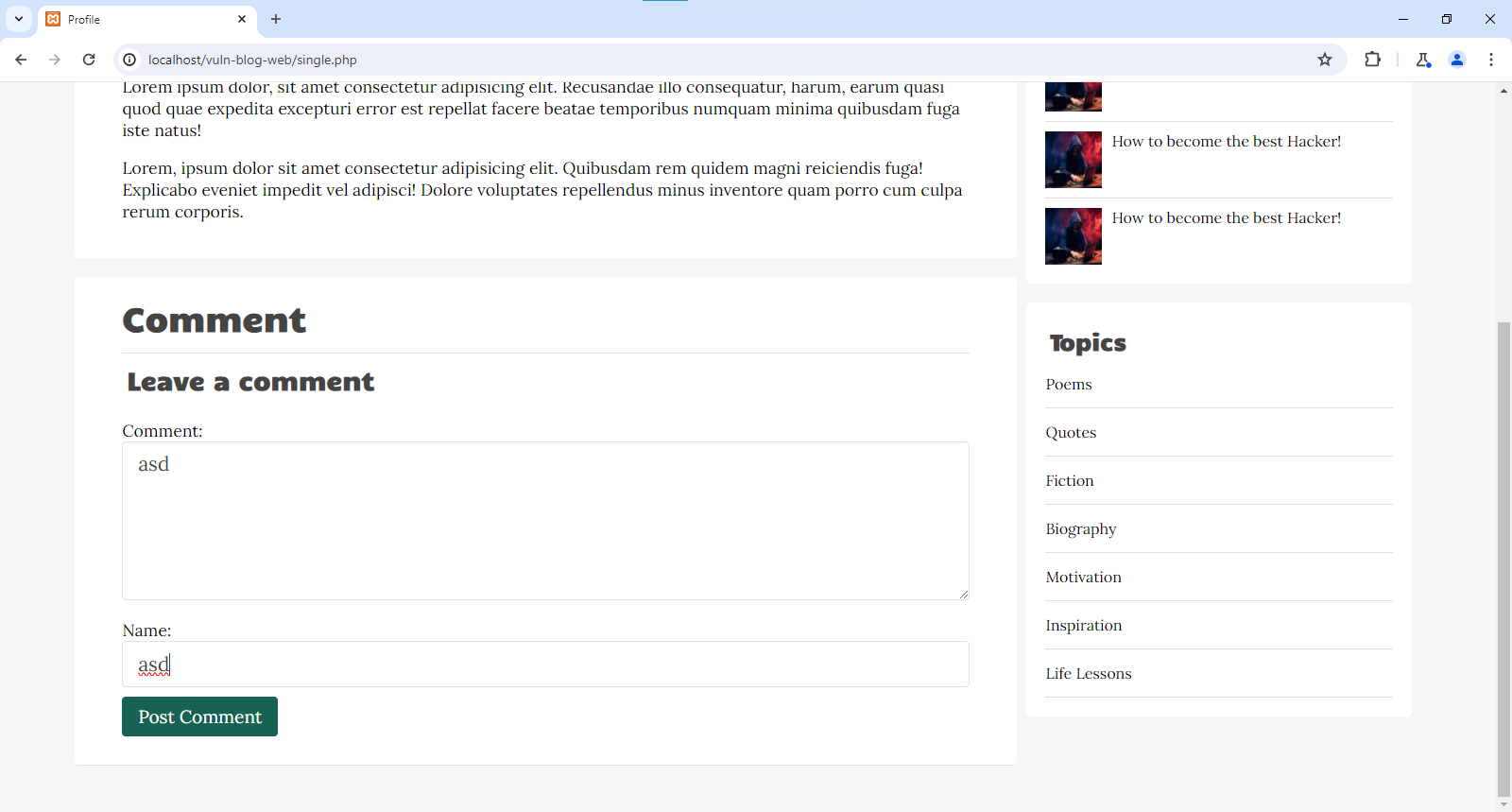
Dom Based XSS là lỗ hổng XSS liên quan tới sinks và sources. Trong đó sources là phần mà kẻ tấn công có thể kiểm soát như document.cookie, location.hash,… Và sinks là các hàm hoặc cái object như eval(), document.body.innerHTML. Và lỗ hổng xảy ra khi dữ liệu từ các sources không được kiểm tra sẽ được truyền vào các sinks. Và kẻ tấn công có thể inject các đoạn script độc hại thông qua các sources để khai thác XSS.

**1. Chức năng Comment**

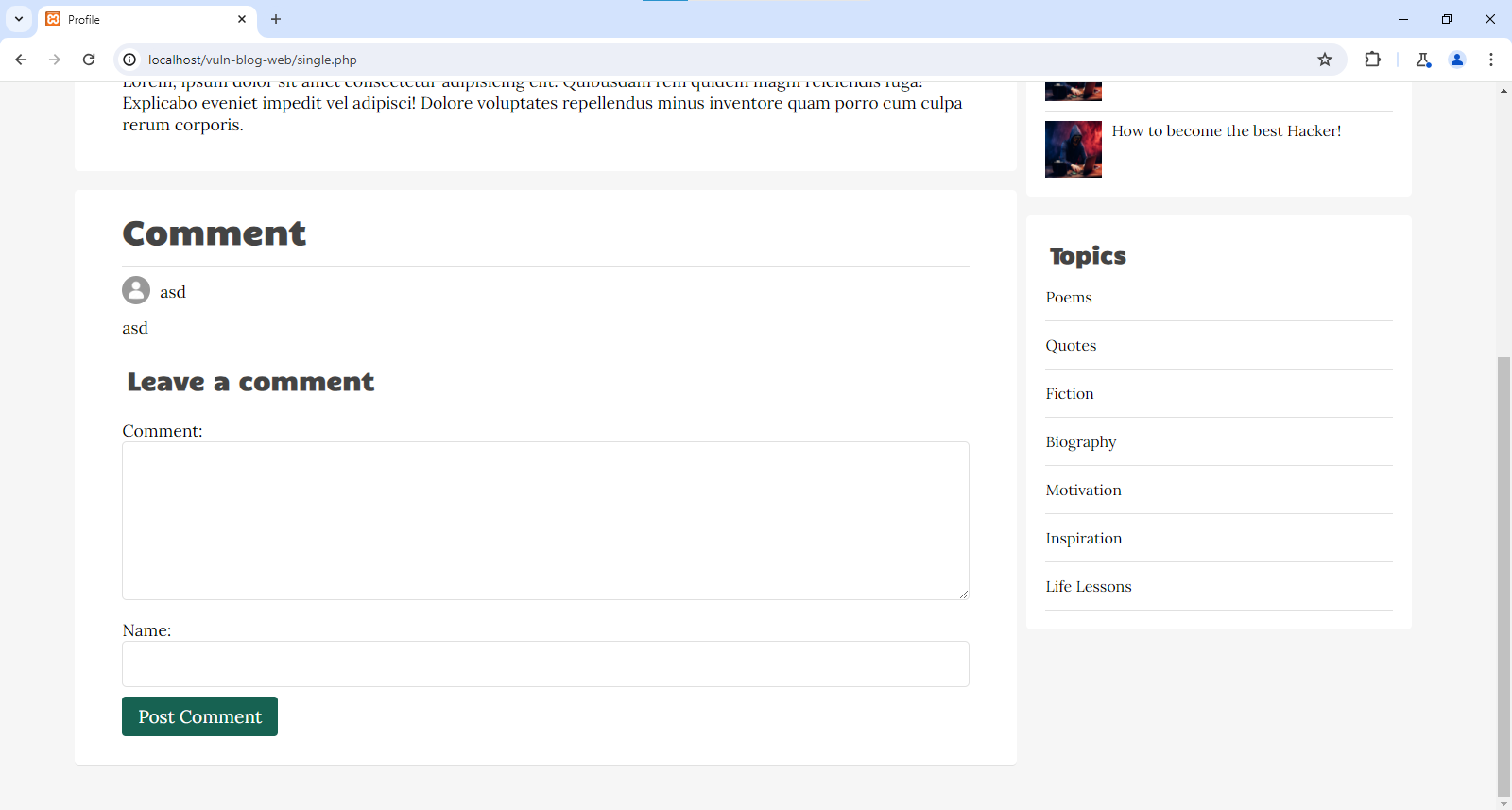
Tiếp cận vào một bài post bất kì, ta sẽ thấy được bài post có một phần comment:



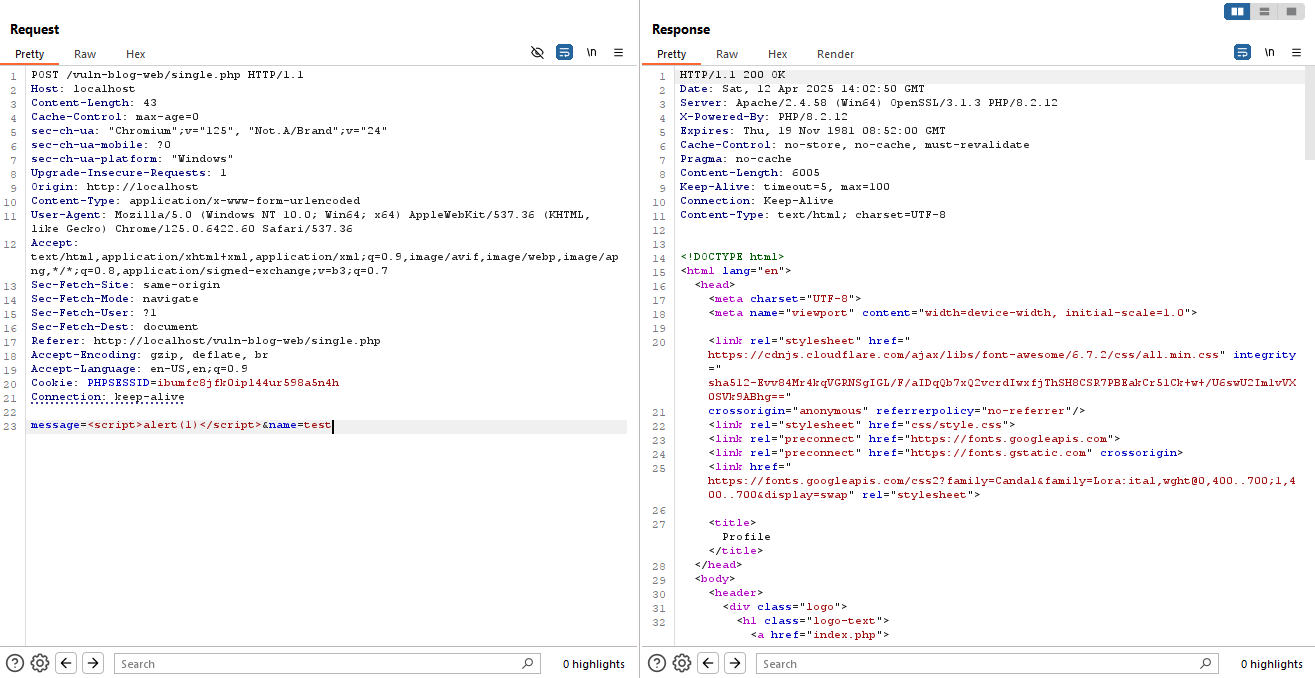
Ta sẽ nhập thử các giá trị để kiểm tra chức năng này:



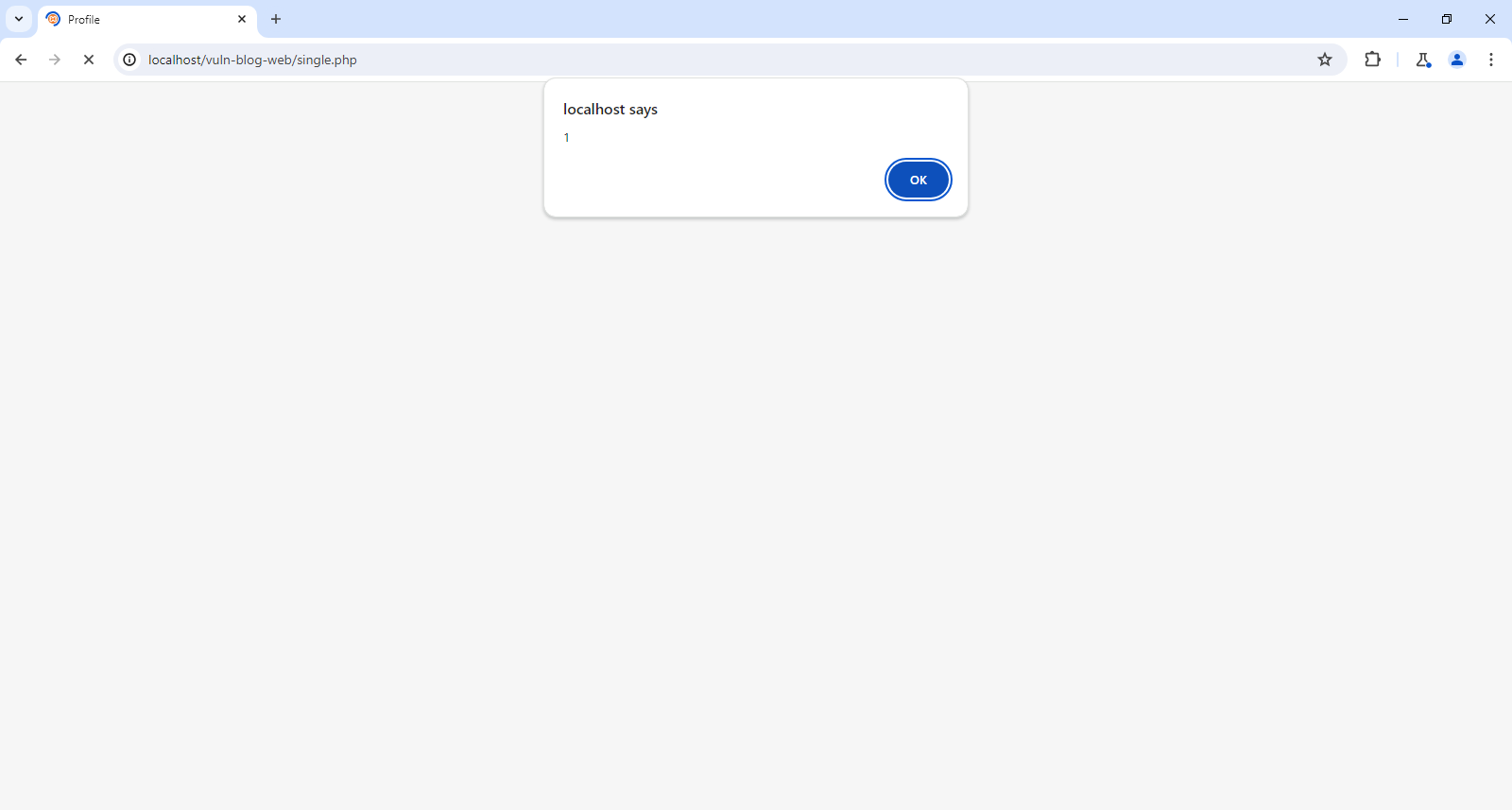
Các thông tin chúng ta đã nhập sẽ được hiển thị ở phần Comment:



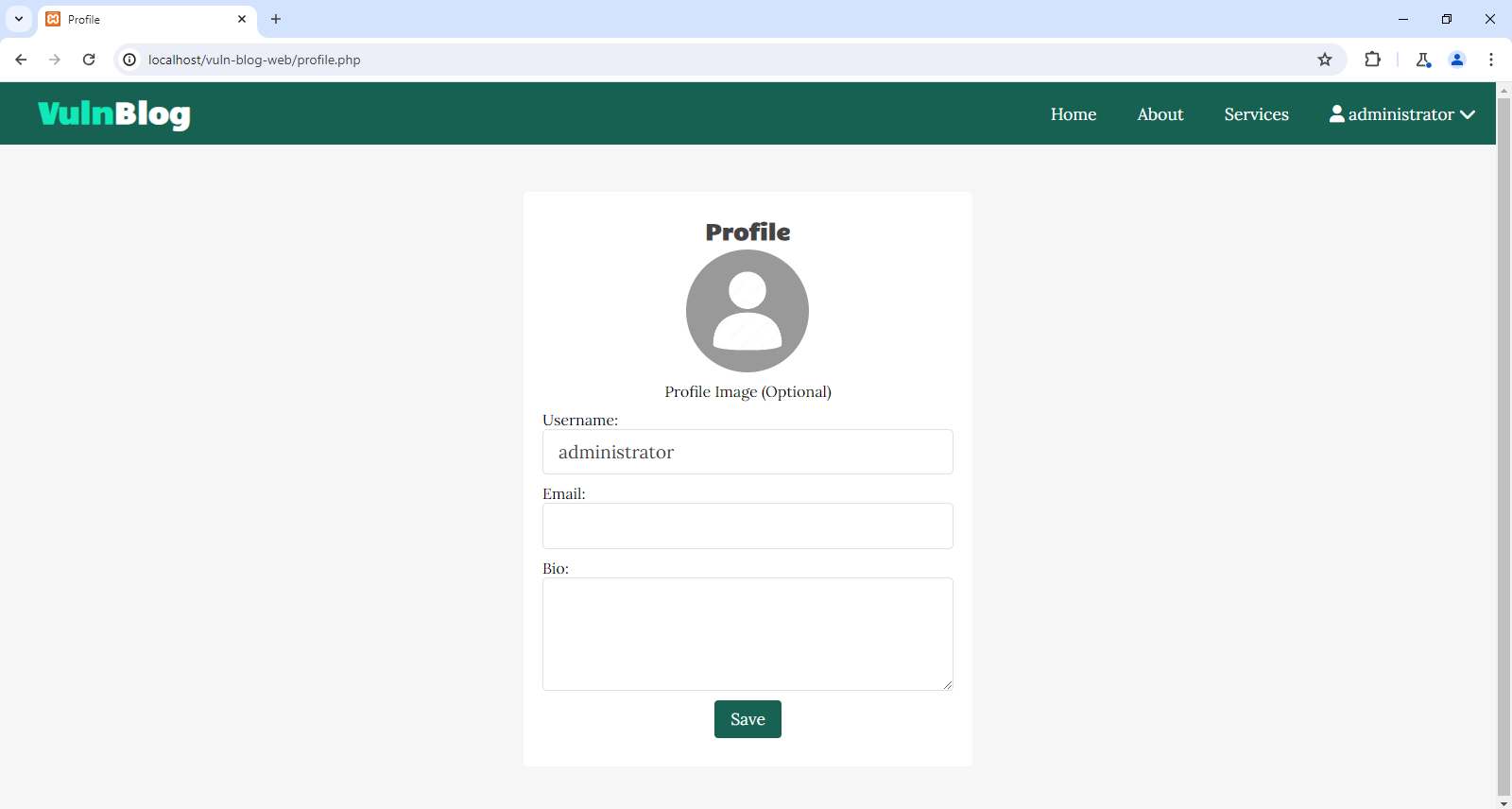
Chúng ta sẽ sử dụng Burp Suite để kiểm tra XSS:



Khi này, reload lại trang thì chúng ta sẽ thấy lỗ hổng XSS đã được khai thác:



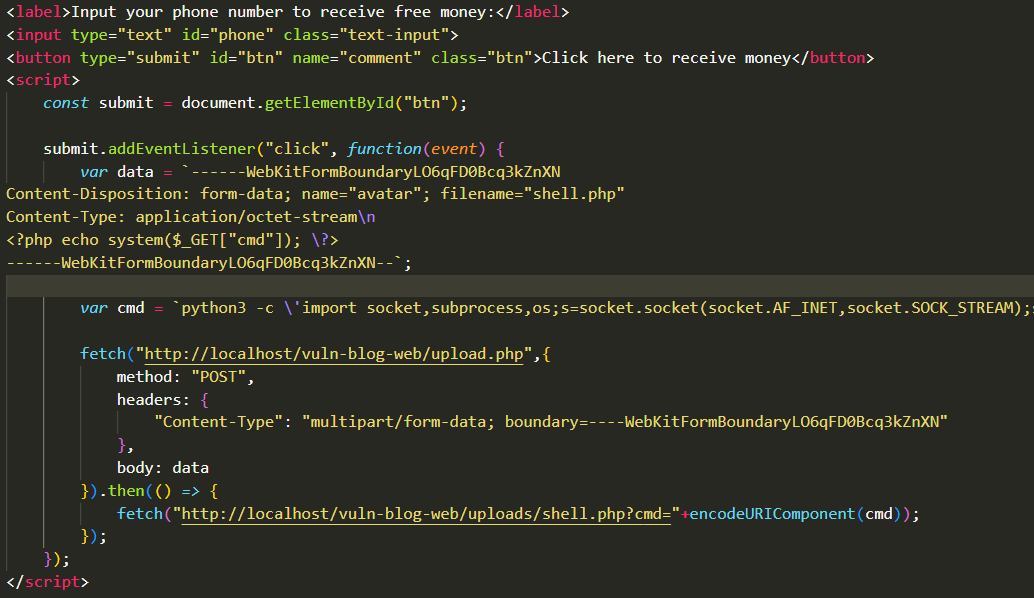
Trong ứng dụng này, tài khoản có quyền admin sẽ có chức năng upload avatar:



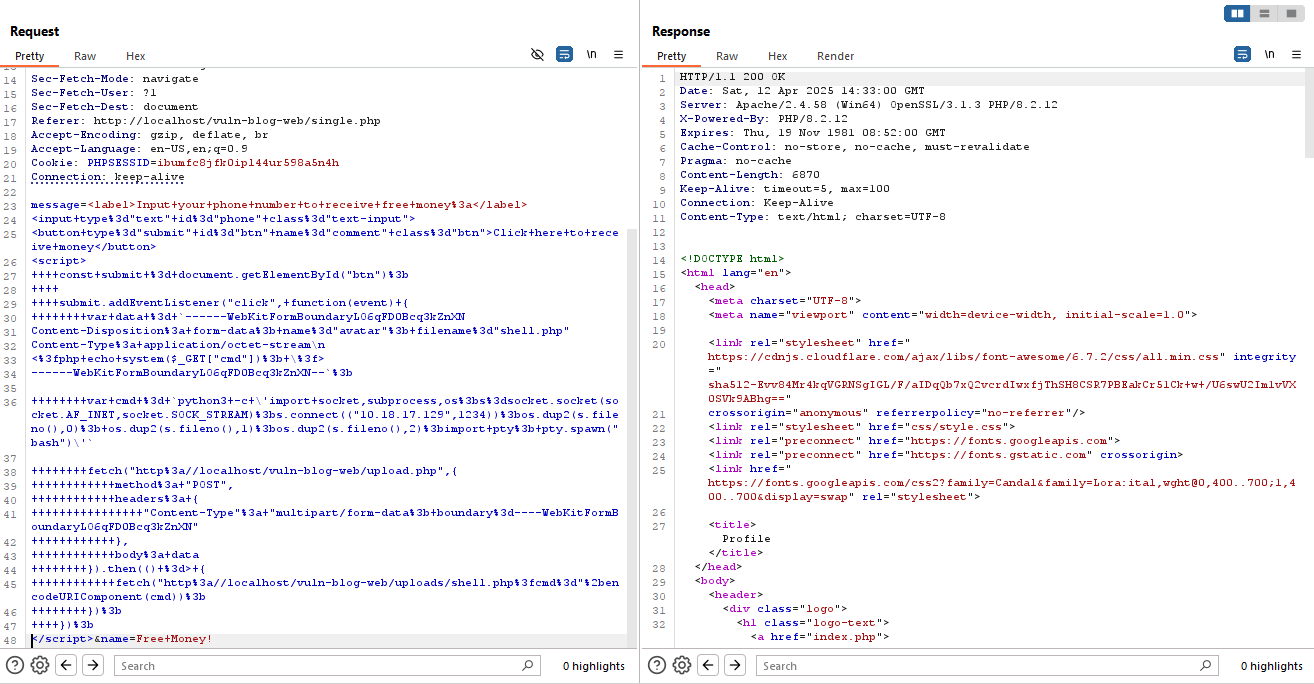
Ta sẽ tận dụng chức năng này để upload lên một file shell nhằm thực hiện RCE.

Để thực hiện điều đó, ta sẽ khai thác stored XSS ở phần Comment để tạo ra một CSRF form và dụ các tài khoản admin click vào đó.

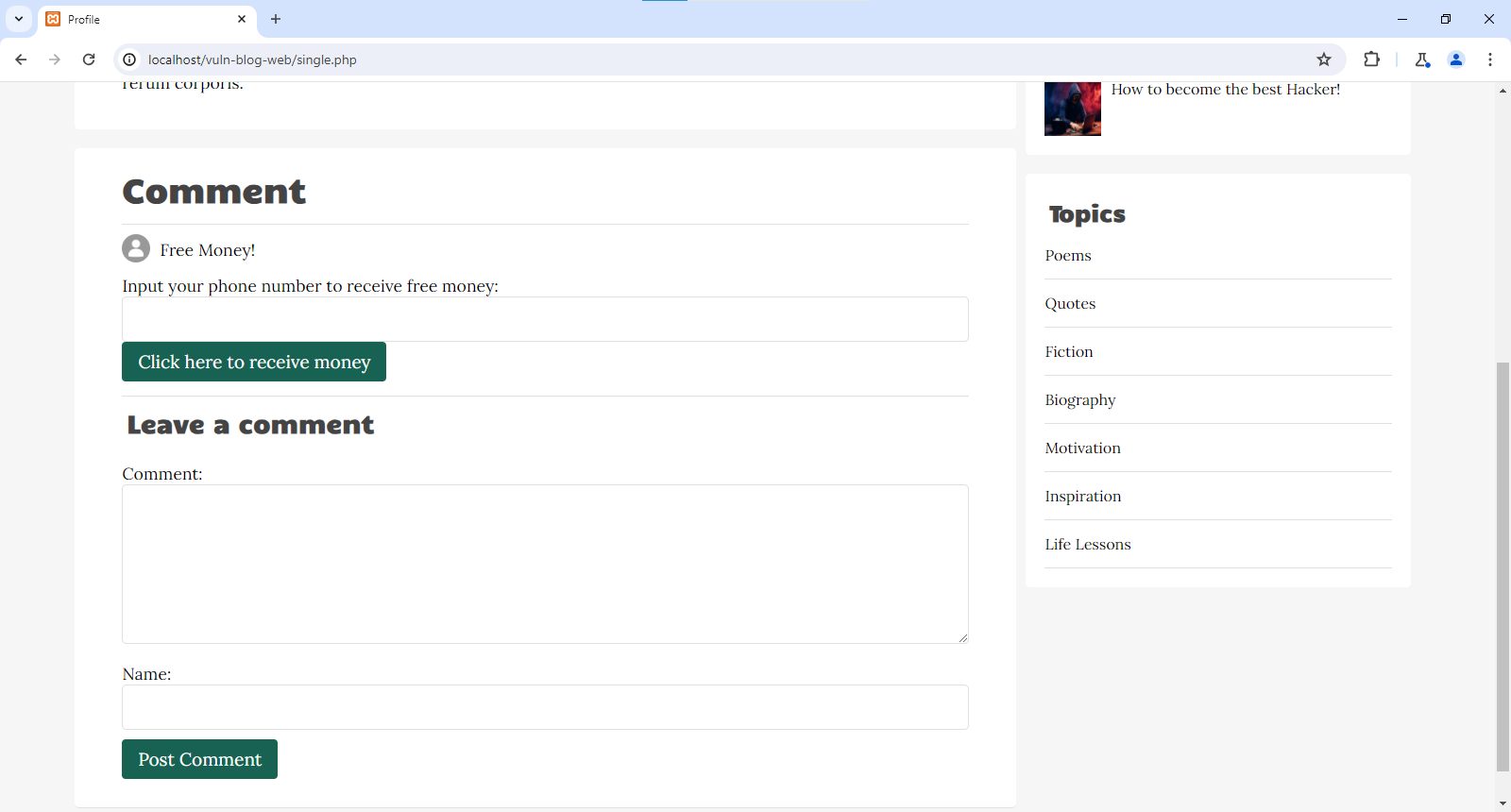
Đây là đoạn code để tạo CSRF form và thực hiện RCE khi admin click vào:



Sử dụng Burp Suite với đoạn code trên để tạo CSRF form:

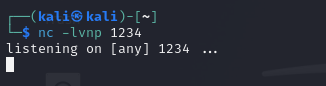


Sau khi tạo thành công, đây là giao diện của CSRF form:



**2. Xâm nhập hệ thống**

Ở trên máy attacker, ta sẽ thực hiện lắng nghe ở port 1234:



Khi bất kì người dùng nào có quyền admin click vào nút ‘Click here to receive money’, chúng ta sẽ thành công kết nối reverse shell:

