**REPORT**

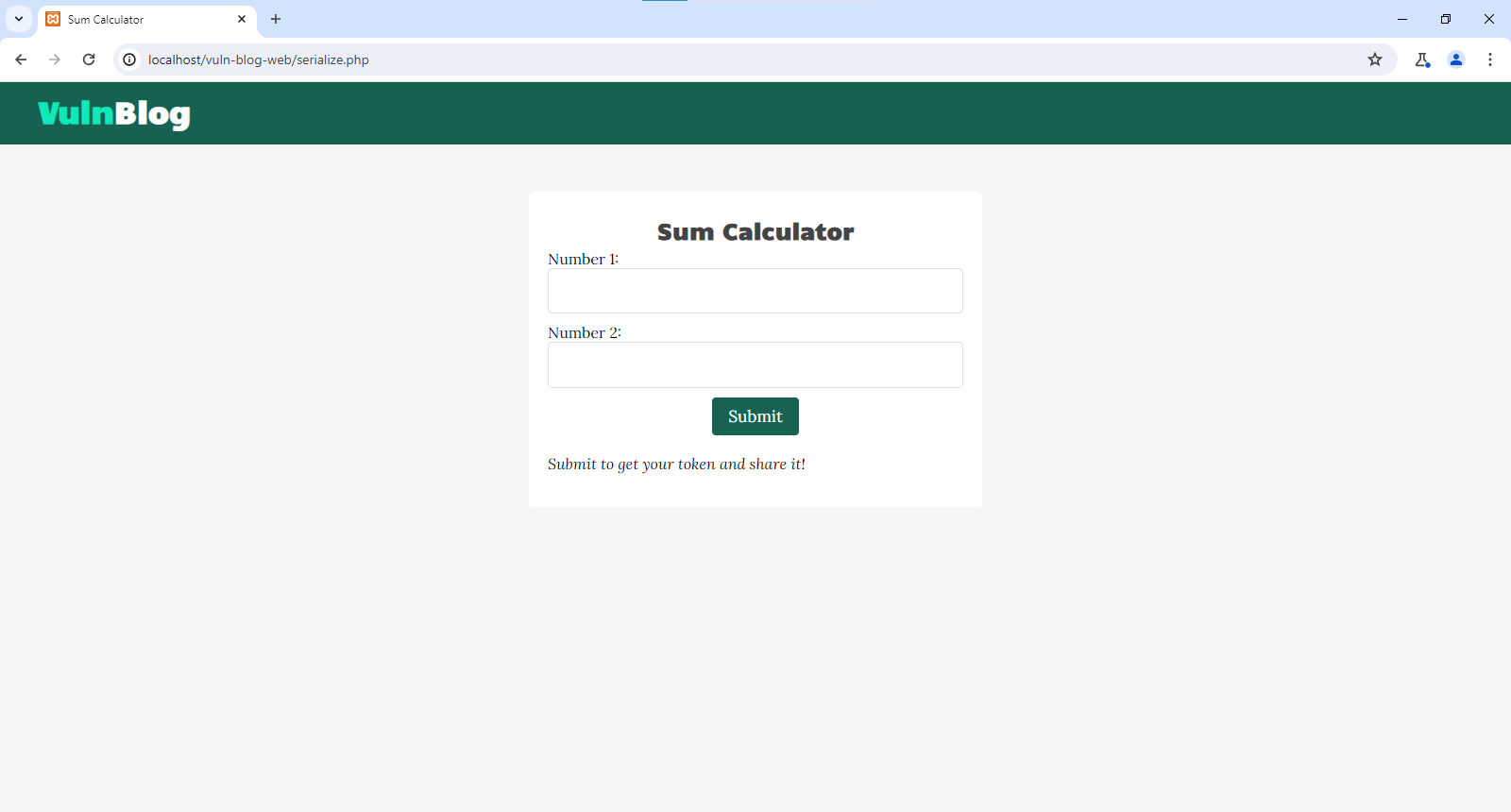
**VULNBLOG**

**Insecure Deserialization**

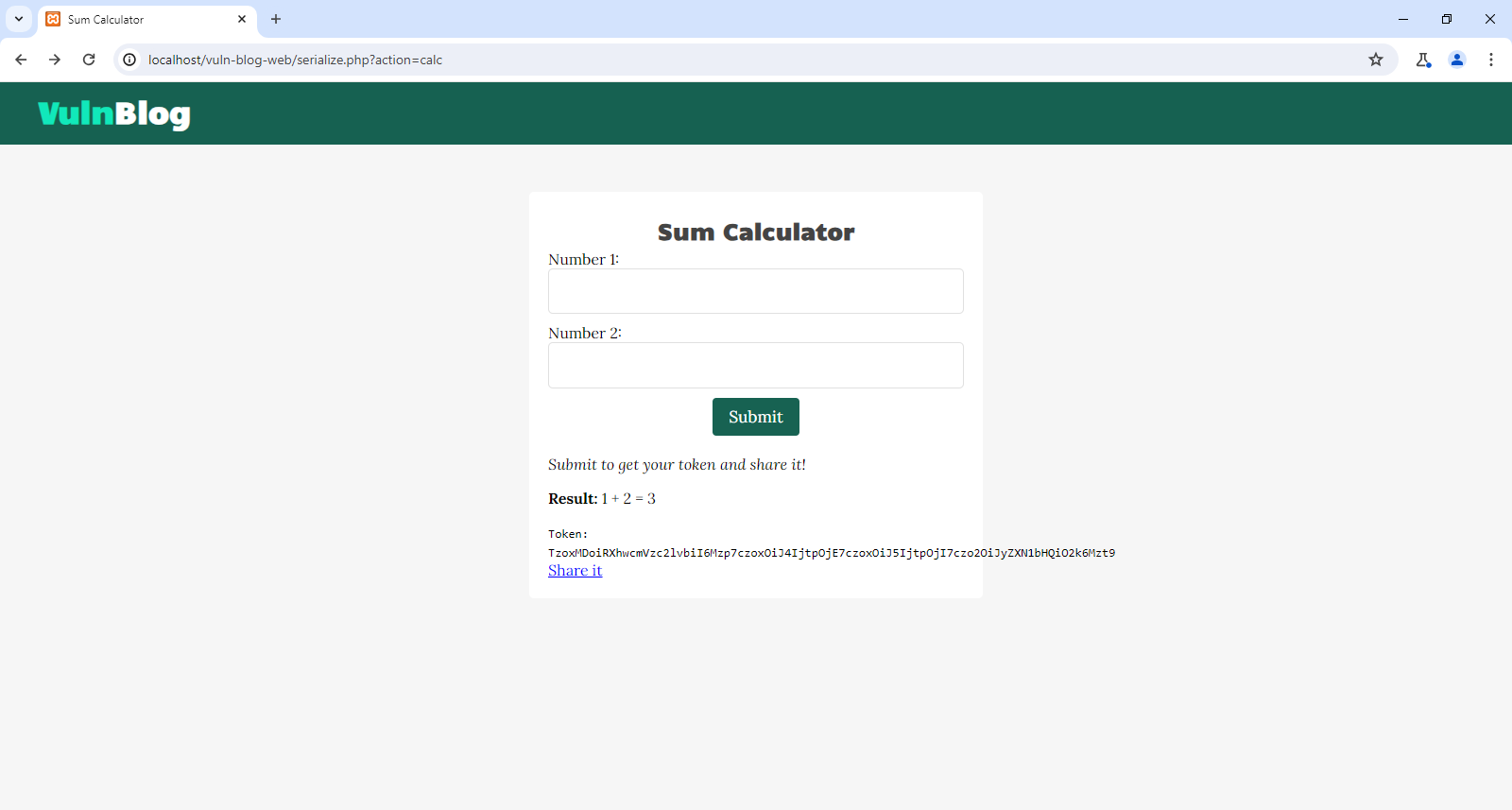
Insecure Deserialization là lỗ hổng xảy ra khi dữ liệu do người dùng kiểm soát được deserialized bởi một ứng dụng web. Điều này có thể tạo điều kiện cho kẻ tấn công kiểm soát các serialized object, từ đó truyền các dữ liệu độc hại vào trong đoạn code của ứng dụng để thực hiện ý đồ mong muốn.

**Chức năng Sum Calculator**

Quan sát trang web, ta thấy có một tính năng cho phép thực hiện cộng 2 số lại với nhau:



Ta sẽ thử input các giá trị bất kì để kiểm tra chức năng này:



Kết quả trả về cho ta một token và một đường dẫn “Share it”.

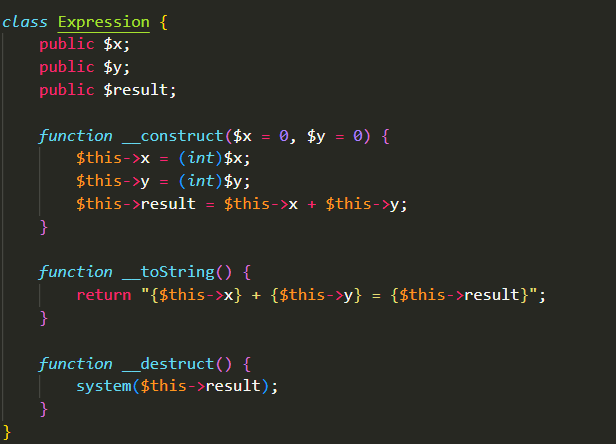
Đầu tiên thì ta sẽ base64 decode token này để xem nội dung của nó:



Kết quả trả về một object tên Expression với các biến x, y và result:

* x: biến kiểu int với giá trị là 1 do chúng ta nhập vào ở input Number 1.
* y: biến kiểu int với giá trị là 2 do chúng ta nhập vào ở input Number 2.
* result: biến kiểu int với giá trị là 3 tương ứng với 1 + 2.

Ta sẽ xem qua source code của object này:

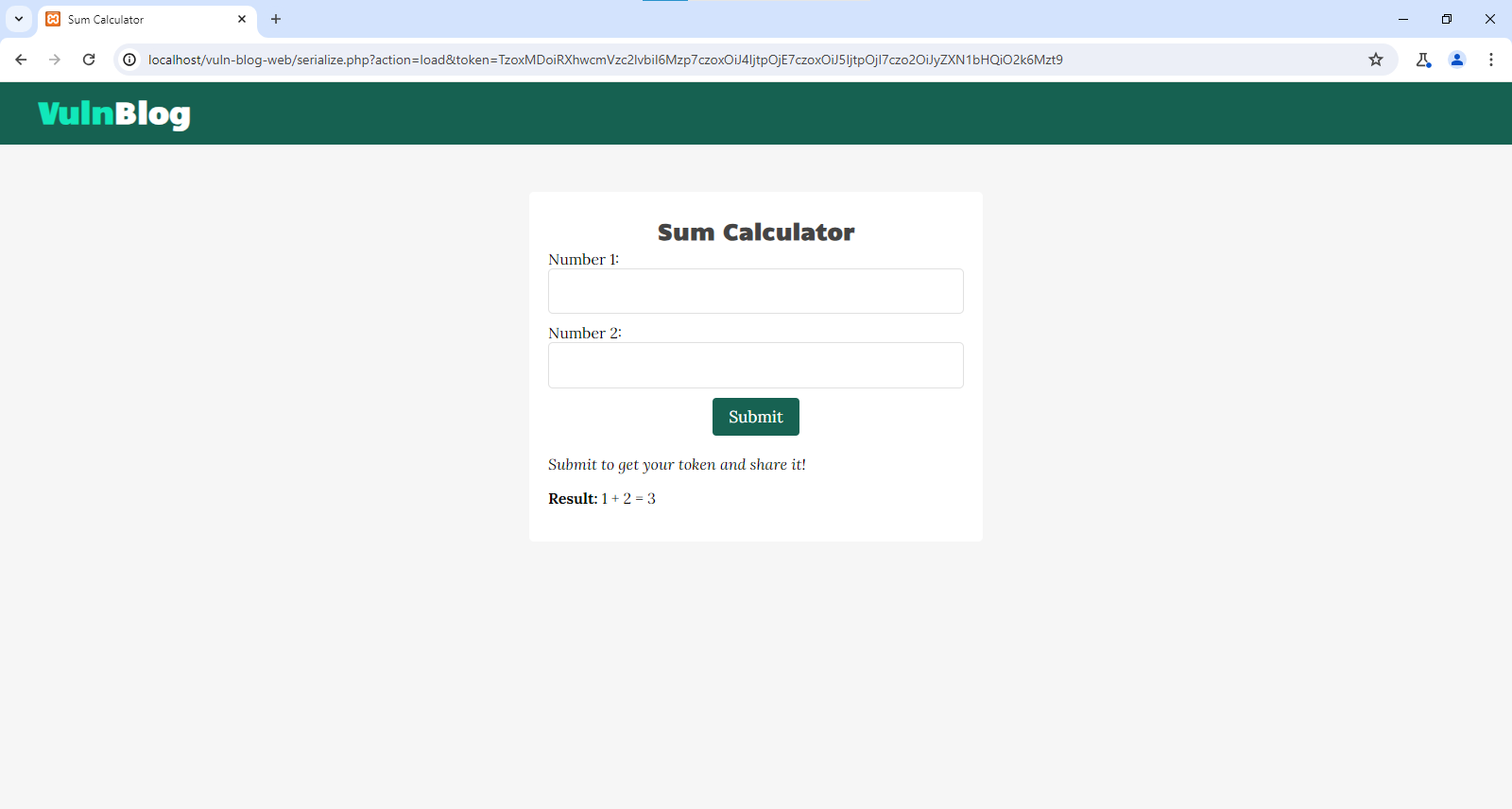


Class Expression này có các chức năng sau:

* Hàm \_\_construct: sẽ nhận input là x và y tương ứng với 2 số chúng ta đã nhập vào, sau đó sẽ tính toán result bằng cách cộng 2 số này lại.
* Hàm \_\_toString: sẽ trả về chuỗi x + y = result, tương ứng với 1 + 2 = 3 để hiển thị cho người dùng thấy kết quả.
* Hàm \_\_destruct: hàm này sẽ thực thi hàm system với kết quả của biến result.

Nhìn qua thì ta sẽ tập trung khai thác vào hàm destruct, vì hàm này có sử dụng hàm system. Nếu chương trình chạy như bình thường là cộng 2 số và trả về biến result để hàm này thực thi hàm system thì sẽ chẳng có ý nghĩa gì ngoài việc dọn dẹp bộ nhớ.

Tiếp theo, ta sẽ thử click vào đường dẫn “Share it” để kiểm tra chức năng này:

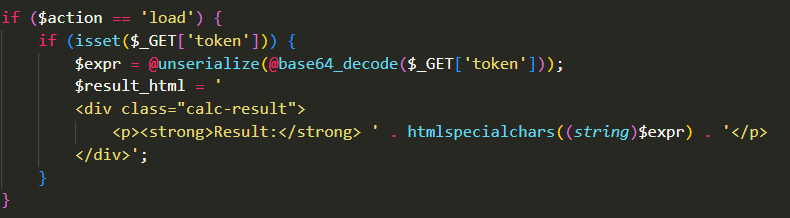


Ta sẽ sử dụng Burp Suite để quan sát rõ hơn:



Khi chức năng này được click thì trang web sẽ đổi giá trị của tham số action thành load và kèm theo một tham số token với giá trị là token trước đó ta nhận được khi cộng 2 số.

Nhìn qua source code thì chức năng này sẽ thực hiện deserialize với giá trị được truyền qua tham số token:



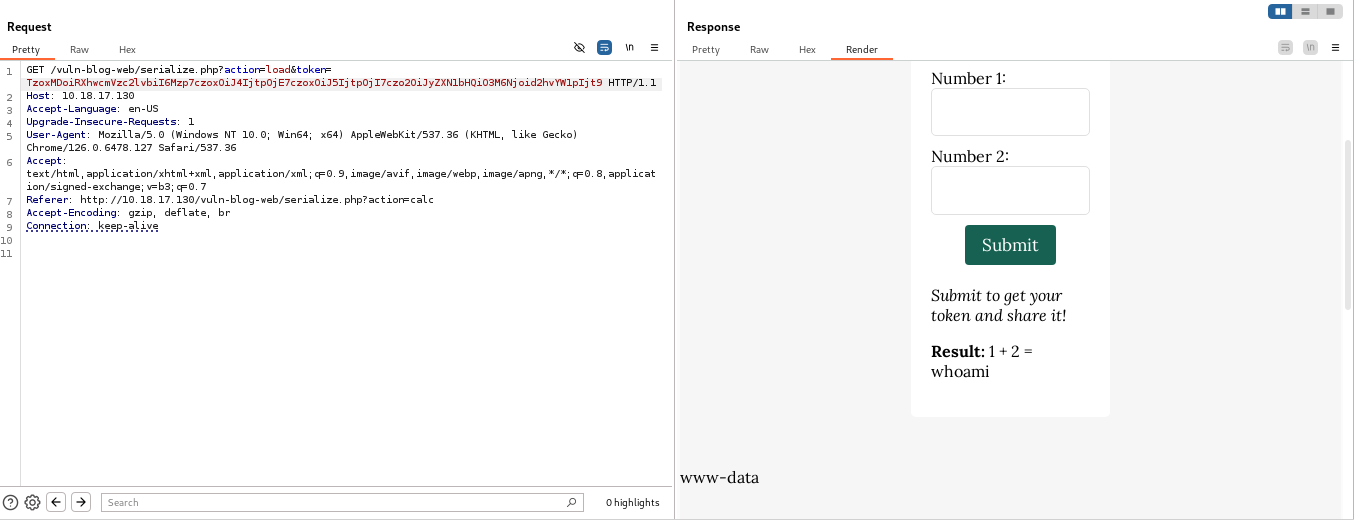
Lợi dụng chức năng này, ta sẽ inject vào giá trị result và để chức năng này deserialize, từ đó thực hiện các lệnh tùy ý.

Ta sẽ thử thực thi lệnh whoami:



Ta sẽ cần đổi giá trị nhận vào của result từ int sang string và độ dài sẽ là 6 tương ứng với whoami.

Thực hiện base64 encode sau đó sử dụng Burp Suite để gửi request:

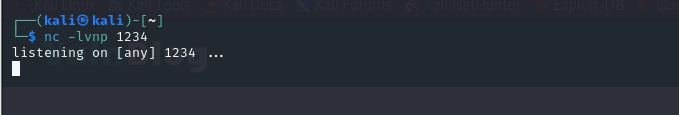


Chúng ta đã thành công inject được lệnh whoami.

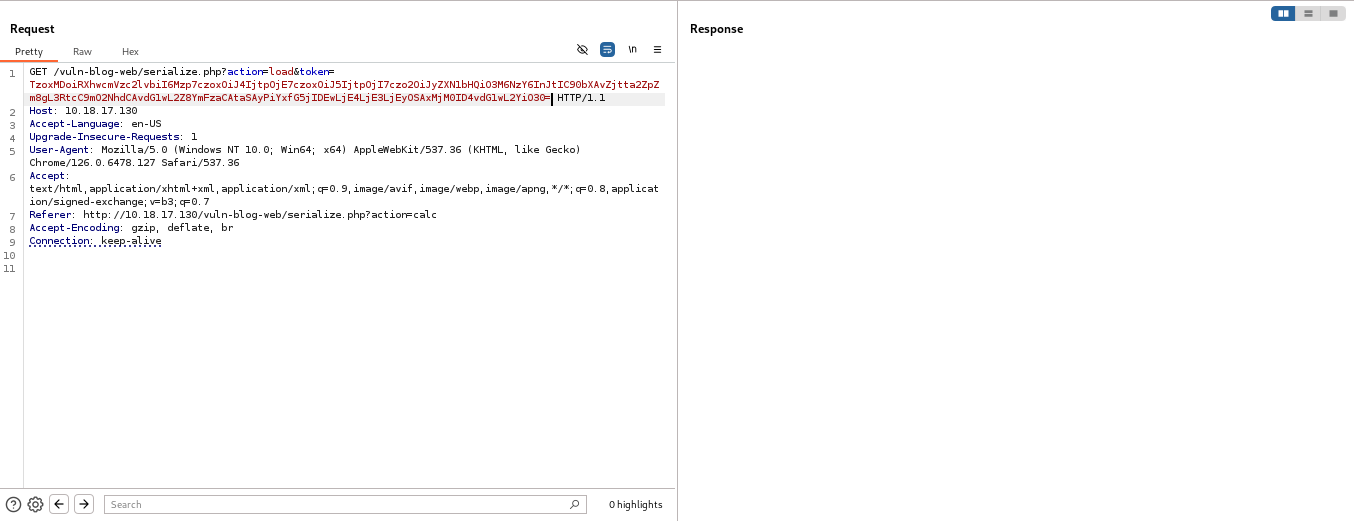
Tiếp theo, ta sẽ thực hiện kết nối reverse shell với chuỗi serialize như sau:



Trên máy attacker, thực hiện lắng nghe ở port 1234:



Sử dụng Burp Suite để base64 encode và gửi request:



Chúng ta đã thành công kết nối reverse shell:

