**CVE-2022-4839**

**Firmware info:**

Tên ứng dụng: Memos

Loại lỗ hổng: Cross-Site Scripting (XSS)

Phiên bản xây dựng: Memos 0.9.0

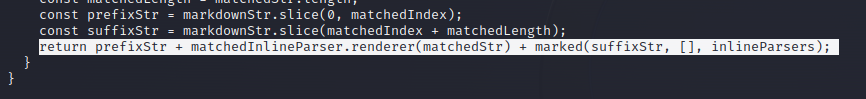
Các phiên bản bị ảnh hưởng: < Memos 0.9.1

Liên kết tải xuống: https://github.com/usememos/memos/archive/refs/tags/v0.9.0.zip

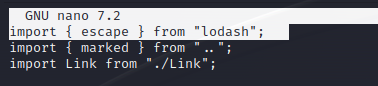
**Description and Impact**

Lỗ hổng này cho phép kẻ tấn công thực thi các đoạn mã JavaScript độc hại trên trang web mục tiêu. Kẻ tấn công lợi dụng khả năng nhúng iframe hoặc chèn HTML động để thực thi mã JavaScript độc hại khi trang web hoặc iframe được tải.

**Root-casue**

****

prefixStr không được áp dụng hàm marked() mà được nối trực tiếp vào chuỗi kết quả nên không được xử lý và biên dịch Markdown thành HTML.

****

Hàm escape từ thư viện Lodash được sử dụng để thoát (escape) các ký tự đặc biệt trong chuỗi, đặc biệt là các ký tự HTML có thể gây nguy cơ XSS. Hàm này chuyển đổi các ký tự có thể bị trình duyệt diễn giải thành mã HTML hoặc JavaScript sang các thực thể HTML an toàn. Các ký tự mà escape() sẽ chuyển đổi:

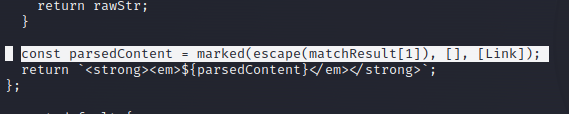
& thành &amp;

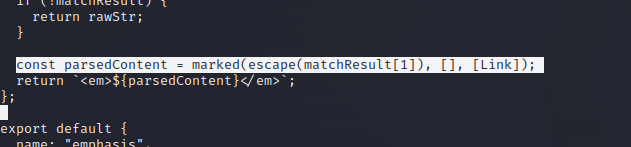
< thành &lt;

> thành &gt;

" thành &quot;

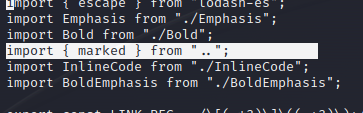
' thành &#39;

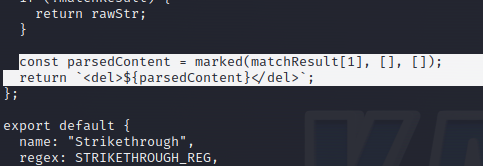
****

****

escape(matchResult[1]): Trước khi nội dung được phân tích cú pháp bởi marked(), nó được thoát bởi hàm escape() từ Lodash.

Hàm escape() sẽ chuyển đổi các ký tự đặc biệt có thể gây ra vấn đề bảo mật, như <, >, &, " và ', thành các thực thể HTML tương ứng (ví dụ: < thành &lt;, > thành &gt;, v.v.).

****

****

Hàm marked() được gọi để chuyển đổi nội dung Markdown trong chuỗi matchResult[1] thành HTML.

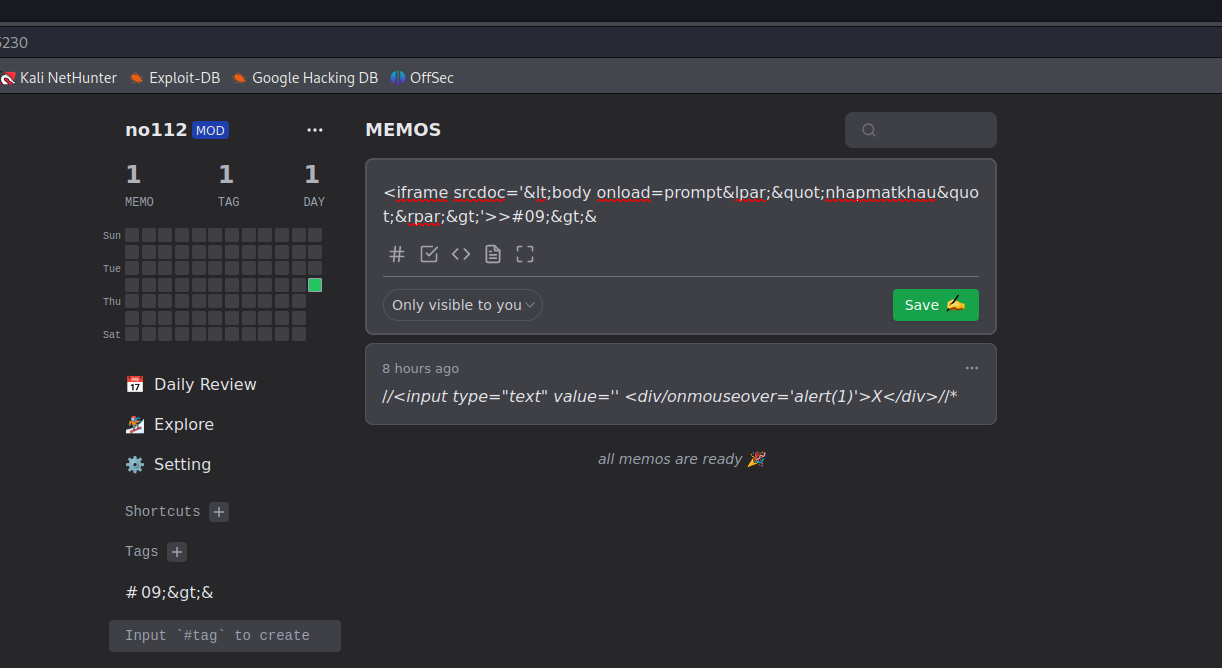
**Steps to reprocedure**

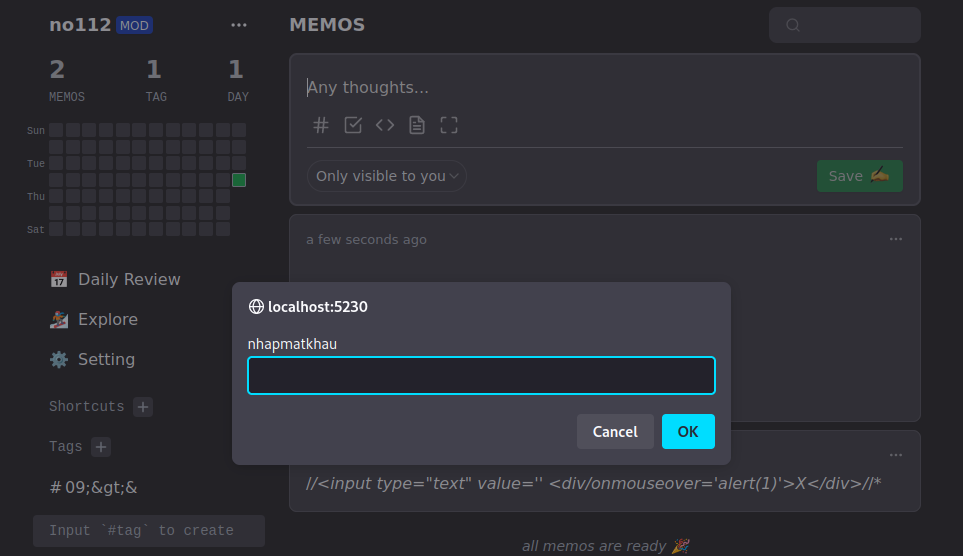
* Đăng nhập vào cổng thông tin.
* Tạo bài viết với xss paylaod.
* Lưu nó lại.

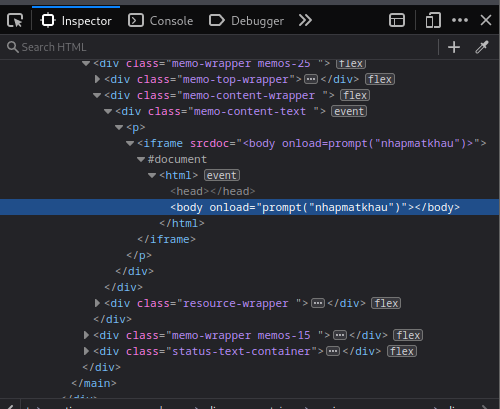
**Payload:**

<iframe srcdoc='&lt;body onload=prompt&lpar;&quot; nhapmatkhau&quot;&rpar;&gt;'>>#09;&gt;&

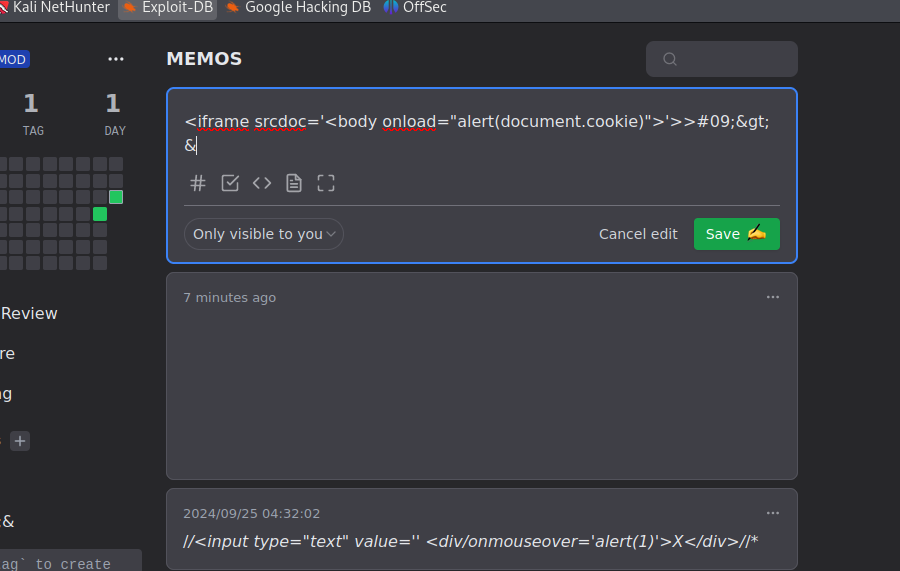
**Poc:**

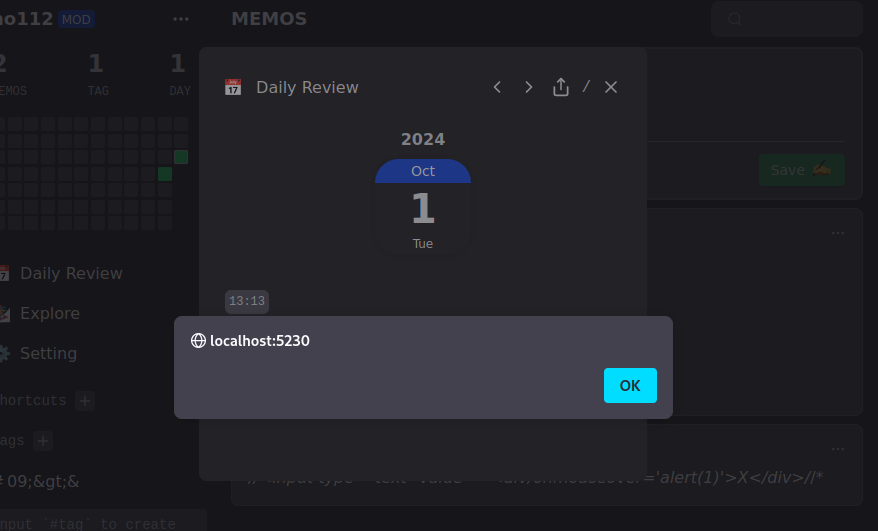
****

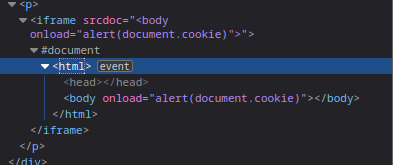
****

****

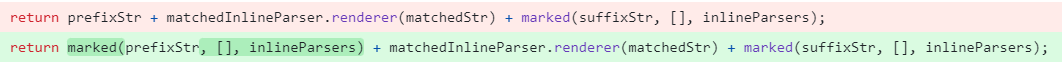
**<iframe srcdoc='<body onload="alert(document.cookie)">'>>#09;&gt;&**

****

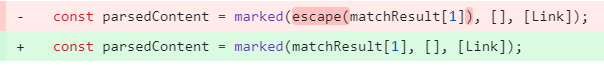
****

****

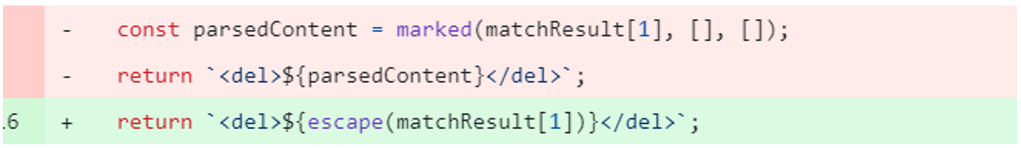
**Recommends**

****

Sửa đổi để prefixStr và suffixStr đều được xử lý qua hàm marked trước khi ghép vào kết quả cuối cùng.

****

Sửa đổi để chuỗi matchResult[1] không qua bất kỳ bước xử lý "escape" nào trước khi đưa vào hàm marked, chuỗi sẽ được xử lý trực tiếp bởi marked mà không có sự kiểm tra hay xử lý các ký tự đặc biệt trước đó.

****

Sử dụng hàm escape thay vì marked để tránh việc marked chuyển đổi cú pháp Markdown thành HTML để attacker có thể lợi dụng đê truyền payload vào gây lỗi.