CVE-2022-25022 - DOM-Based XSS

February 25, 2022

1 Application

`https://github.com/danpros/htmly`

2 Introductory Remarks

Note that `https://www.cvedetails.com/cve/CVE-2021-36703/`, `https://www.cvedetails.com/cve/CVE-2021-36702/` and the corresponding issue `https://github.com/danpros/htmly/issues/481` are different from our vulnerability. A DOM-based XSS was not mentioned in this disclosure.

3 Description of the Vulnerability

In the HTMLy PHP blogging platform (v2.8.1 commit 2d2fa9bd85e6060691cd1cb04557519a8b11ac2b), the unsanitized input from the content field of a blog post directly is previewed in the HTML page in such a way that arbitrary Javascript code executes. This results in a Cross-Site Scripting attack (XSS). As a consequence, a moderator could be tricked into editing a blog post and, thus, become the victim of involuntary crypto mining or credential theft. Note that this vulnerability is fundamentally different from the above XSS vulnerability and will not work on a published blog post because of partial input sanitation. Here is an unlisted (non-public) youtube video that shows the exploit: `https://youtu.be/acookTqf3Nc`.

4 Steps to Reproduce the Exploit

Edit a blog post with `<iframe src="javascript:alert(1)">` as content. Note that no request is necessary to execute the Javascript code.

5 Technical Description of the Vulnerability

The file `Markdown.Editor.js` (in the function `makePreviewHtml`) changes the preview code at runtime and in this context also includes unsafe Javascript code, which is then executed.