

[New issue](#)[Jump to bottom](#)

Another Filter bypass leading to XSS #348

🔒 ClosedTheGrandPew opened this issue on Apr 12, 2020 · 12 comments · Fixed by [#353](#)

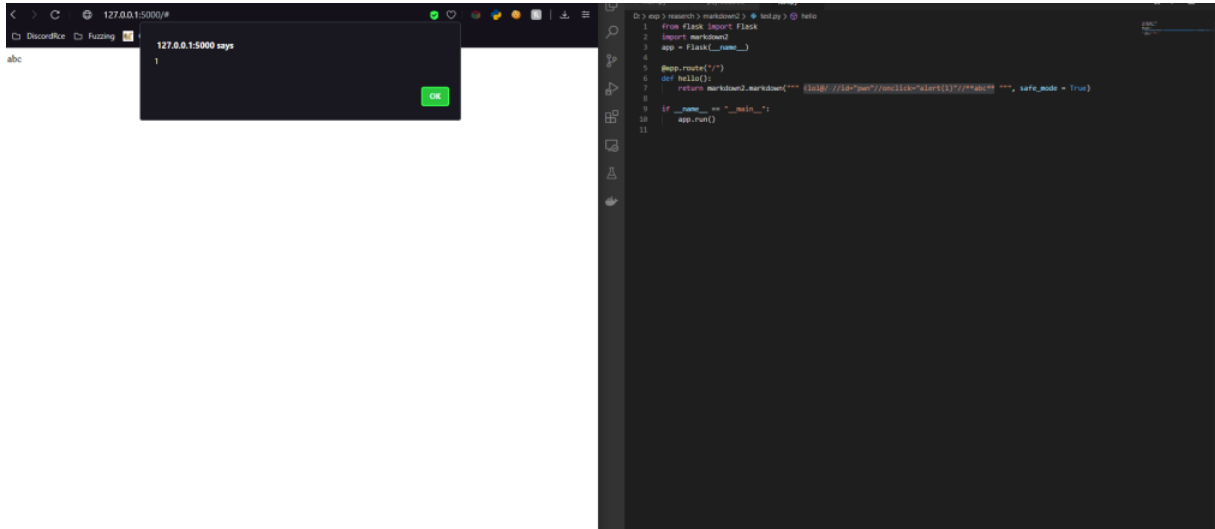
TheGrandPew commented on Apr 12, 2020

On the latest release (2.3.8) a payload like this one can lead to xss and bypass `safe_mode` when set to true.

```
<lol@/ //id="pwn"//onclick="alert(1)"//**abc**
```

The Problem:

I think its due to just bad regex's not detecting non alphanumeric tags.

4

avramit commented on Apr 13, 2020

It seems like the parser doesn't escape tags that don't match the following pattern, so everything that isn't `[a-zA-Z0-9_]` can be used to bypass the escaping mechanism

[python-markdown2/lib/markdown2.py](#)
Line 2167 in 4d2fc79

```
2167 _incomplete_tags_re = re.compile("<(/?w+[\s/]+?)")
```

The following payload will also work:

```
<x- onclick="alert(1)"**Click Me*
```

TheGrandPew commented on Apr 14, 2020 · edited

[Author](#)

Has been assigned [CVE-2020-11888](#).

 v1dhun mentioned this issue on May 1, 2020

FIX: Filter bypass leading to XSS 418sec/python-markdown2#1

🔒 Closed xurble mentioned this issue on May 1, 2020

Fix for issue 348 - incomplete tags with punctuation after as part of... #351

🔒 Closed

xurble commented on May 2, 2020 · edited

I didn't see the PR from @v1dhun before I submitted mine. However, having had more time to think about it, they're both flawed.

Mine can be defeated by this:


```
<x:// onclick="alert(1)"**Click Me*
```

The other can be defeated by this

```
<x- onclick = "alert(1)"**Click Me*
```

Also, it breaks a bunch of unit tests.

This needs a little more thought

 **xurple** mentioned this issue on May 2, 2020

Issue 348 #353

→ Merged

vidhun commented on May 3, 2020

Hi @xurple,
I updated the code with checking white-spaces, Now its working fine. Could you please check it

huntr-helper commented on May 3, 2020

👋 Hey! We've recently opened a bug bounty against this issue, so if you want to get rewarded 💰 for fixing this vulnerability 🕷️, head over to <https://huntr.dev>!

xurple commented on May 4, 2020

@vidhun I think we've both fixed it right now. Either would be OK, or the maintainers might have a better idea altogether.

kravietz commented on May 4, 2020 • edited

Regex is going to be always bypassed as it assumes specific syntax while combinations for a renderable HTML are practically unlimited. This is one of the fundamental recommendations from [OWASP XSS Prevention Cheat-sheet](#).

I'd recommend running the input text through [bleach](#) which is a whitelist-based HTML sanitizer.

I had a look at the `markdown2` code but to be honest I don't know the code base enough to be able to see an obvious place to plug it in.

👍 1

 **nicholasserra** closed this as completed in #353 on May 4, 2020

nicholasserra commented on May 4, 2020

Collaborator

I merged @xurple PR as it was on the main repo. LGTM, thank you!

I'm a little hesitant to introduce another library like bleach to sanitize final output. But it may be a good solution. Needs investigating.

👍 1

kravietz commented on May 4, 2020 • edited

@nicholasserra Yes, that's the classic dilemma. As developer I would probably prefer a big fat notice in the documentation stating that the main purpose of the library is *not* to sanitize untrusted code but to render Markdown, just to set the expectations right.


thmo commented on May 8, 2020

Does this warrant a new release?
The 2.3.8 release is about a year old...

xurple commented on May 9, 2020

If it sways your thinking, the library is flagged by sentry, which is how I discovered the issue.

👍 1

 **mcrot** mentioned this issue on May 11, 2020

Upgrade markdown2 if possible ContactEngineering/TopoBank#458

🔒 Closed

nicholasserra commented on May 11, 2020

Collaborator

2.3.9 is now released

👍 1

 **onegreyonewhite** added a commit to vstconsulting/polemarch that referenced this issue on May 12, 2020

 1.7.4 ...

9c07d62

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone


No milestone

Development

Successfully merging a pull request may close this issue.

 **Issue 348**

zoo-digital/python-markdown2

 **Fix for issue 348 - incomplete tags with punctuation after as part of...**

zoo-digital/python-markdown2

8 participants

