New issue

Jump to bottom

XSS vulnerability in [insert video] #3880

Closed **W2Ning** opened this issue on Apr 16, 2020 · 13 comments

W2Ning commented on Apr 16, 2020

Steps to reproduce the problem.

1.Go to the Official demo
https://froala.com/wysiwyg-editor/
2.Click on the [+] button
3.Click on [insert video] button
4.Click on [Embedded Code] button
5.Paste the payload

```
<EMBED/SRC=" A6Ly93d3cudzMub3JnLzIwMDAvc3ZnIiB4bWxucz0iaHR0cDovL3d3dy53My5vcmcv
MjAwMC9zdmciIHhtbG5zOnhsaW5rPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L3hs aW5rIiB2ZXJzaW9uPSIxLjAiIHg9IjAiIHk9IjAiIHdpZHRoPSIxOTQiIGhlaWdodD0iMjAw
ICIgaWQ9InhzcyI+PHNjcmlwdCB0eXBlPSJ0ZXh0L2VjbWFzY3JpcHQiPmFsZXJ0KCJUaGVyZSBpcyBhIFhTUyIpOzwvc2NyaXB0Pjwvc3ZnPg==">
```

Recording.

https://www.youtube.com/watch?v=WE3b1iSnWJY

👍 4

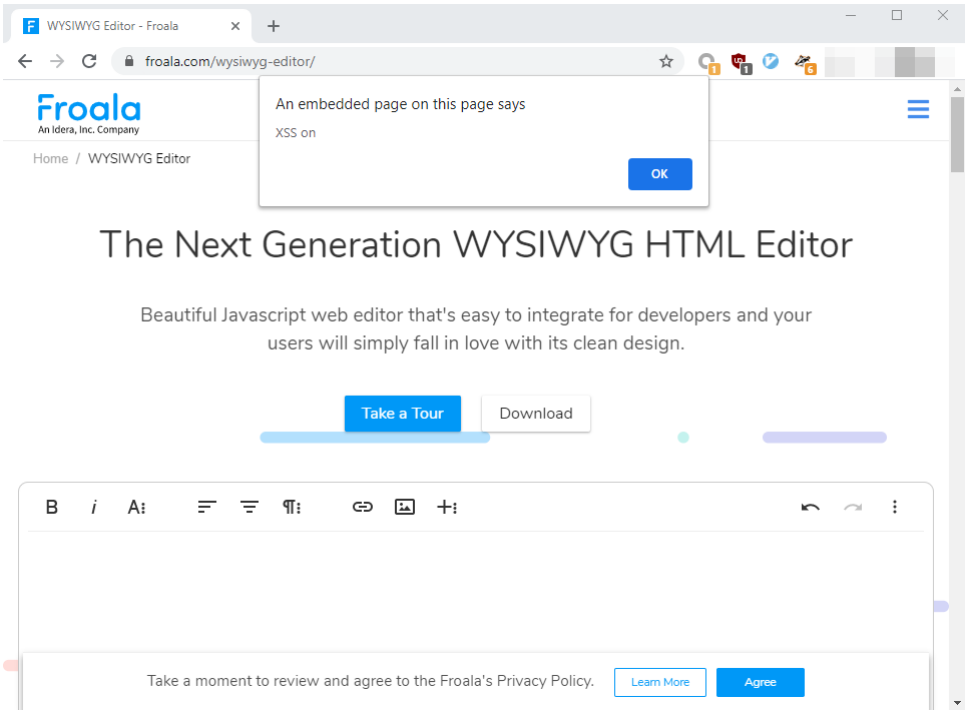
emanuelduss commented on Apr 20, 2020 • edited

Nice find!

But be aware that you don't have access to the origin of the attacked website.

E.g. changing the XSS payload to `alert("XSS on " + document.domain)`, you will just get `XSS on .`

Screenshot:



This means you don't have access to the domains cookies, web storage, etc.

Do you have an idea / PoC what could be done using your injection?

emanuelduss commented on Apr 20, 2020 • edited

Furthermore, it's probably the same bug like in issue #3270 that was closed but not fixed. It's still possible to execute this payload.

W2Ning commented on Apr 20, 2020 Author

> Furthermore, it's probably the same bug like in issue #3270 that was closed but not fixed. It's still possible to execute this payload.

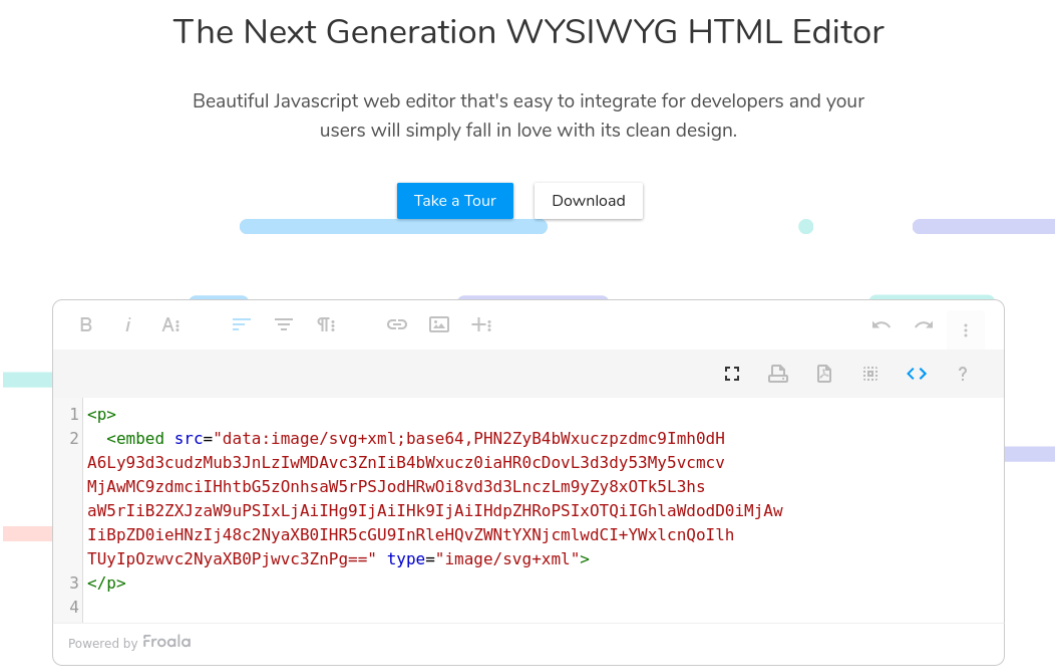
To be honest, I was really inspired by that issue.
But the vulnerability point reported by him was indeed fixed.

I used a similar payload to successfully create a XSS at another injection point.
That's why I submit this issue.

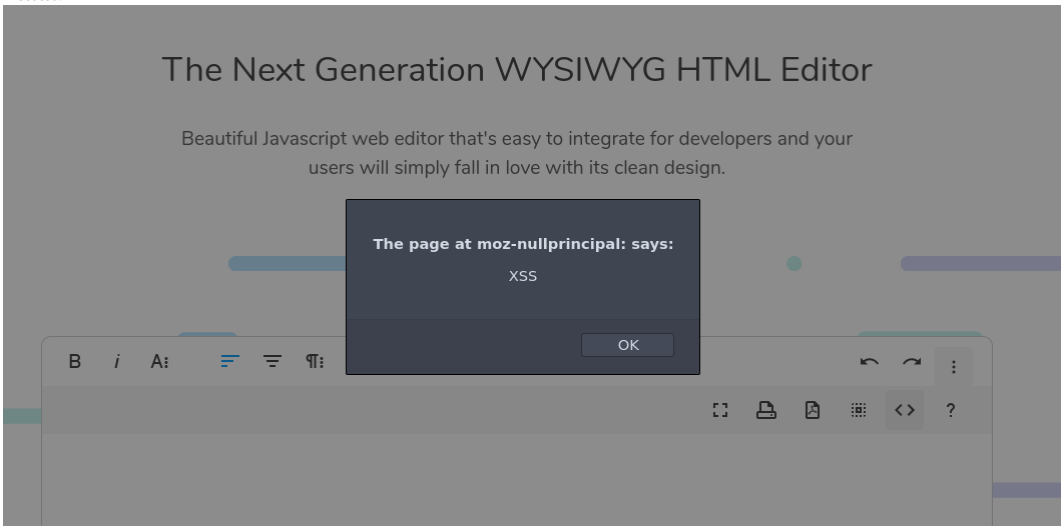
emanuelduss commented on Apr 20, 2020

No, the vulenrability of him is still not really fixed. It may not be possible by inserting this payload in via an URL, but when the payload is inserted in the source code view, the JavaScript is still executed.

Input:



Executed:



Firefox also shows that the origin is not the origin where the editor is installed but a null origin.

This is still an issue, because the editor could be used to load potentially malicious user input from e.g. an API.

👍 1

W2Ning commented on Apr 21, 2020 Author

😱

emanuelduss commented on Apr 21, 2020

I found another issue (a real XSS where you have access to the origin of the domain) and reported to Froala. They told me that my new XSS issue and also this old issue (I also told them that this issue is not yet fixed), will be fixed in the next version. I reported in December and they can't tell me when the new version will be released. :(

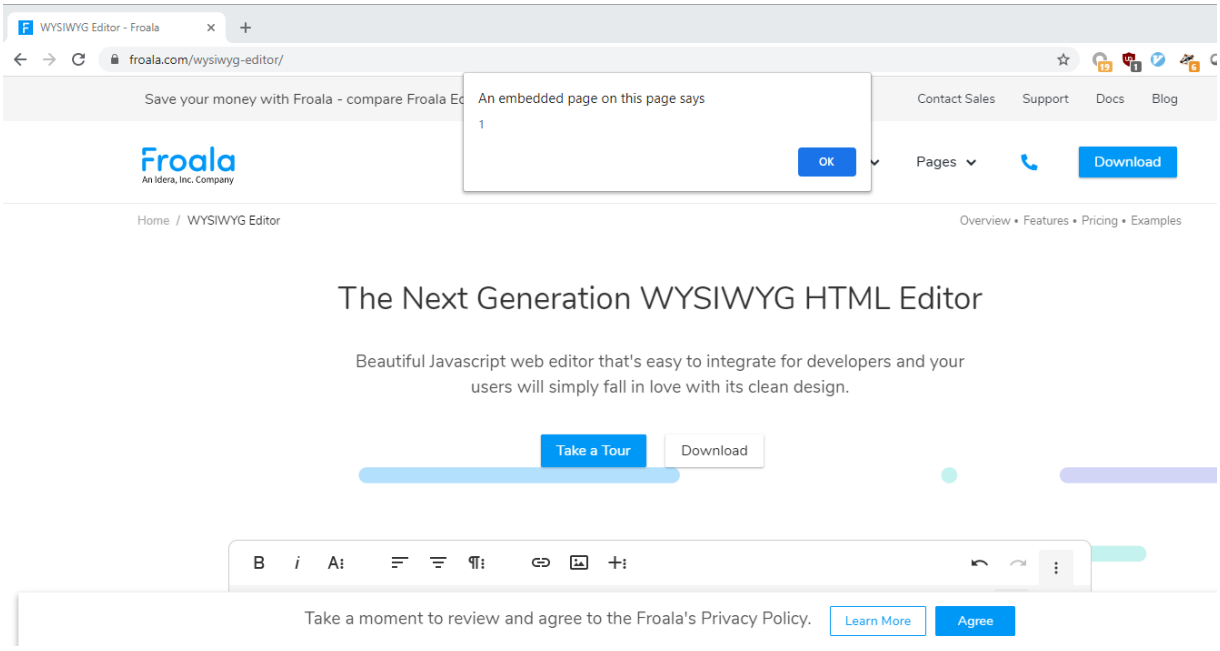
emanuelduss commented on Apr 21, 2020

Btw, the issue #3039 is also still not fixed.

Payload:

```
<object data='data:text/html;base64,PHN2Zy9vbmxvYWQ9YWxlcnQoMSk+'>
```

Executed:



But also not in the origin of the website.

W2Ning commented on Apr 21, 2020 — Author

> I found another issue (a real XSS where you have access to the origin of the domain) and reported to Froala. They told me that my new XSS issue and also this old issue (I also told them that this issue is not yet fixed), will be fixed in the next version. I reported in December and they can't tell me when the new version will be released. :(

Man, feel sad for you.

emanuelduss commented on Apr 22, 2020

I asked for more details yesterday and then I got a mail where they denied that there would be any XSS issue in the editor. It was like they just closed the issue and ignored my reporting, despite they first confirmed the vulnerability.

So I did a more technical explanation and a PoC on how it could be exploited and now they will fix it again. It should be fixed in this quarter, so it looks like it does not have high priority at the moment.

Just for info ;-)

1

W2Ning commented on Apr 23, 2020 — Author

Great patience.

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!

JamieSlome commented on May 8, 2020

A fix has been suggested (#3911)!

JamieSlome mentioned this issue on May 8, 2020

huntr.dev - Cross Site Scripting (XSS) Fix #3911

Open

ilyaskarim commented on Jun 29

Fixed in V4.0.11: https://froala.com/wysiwyg-editor/changelog/#4.0.11

ilyaskarim closed this as completed on Jun 29

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants