New issue

Jump to bottom

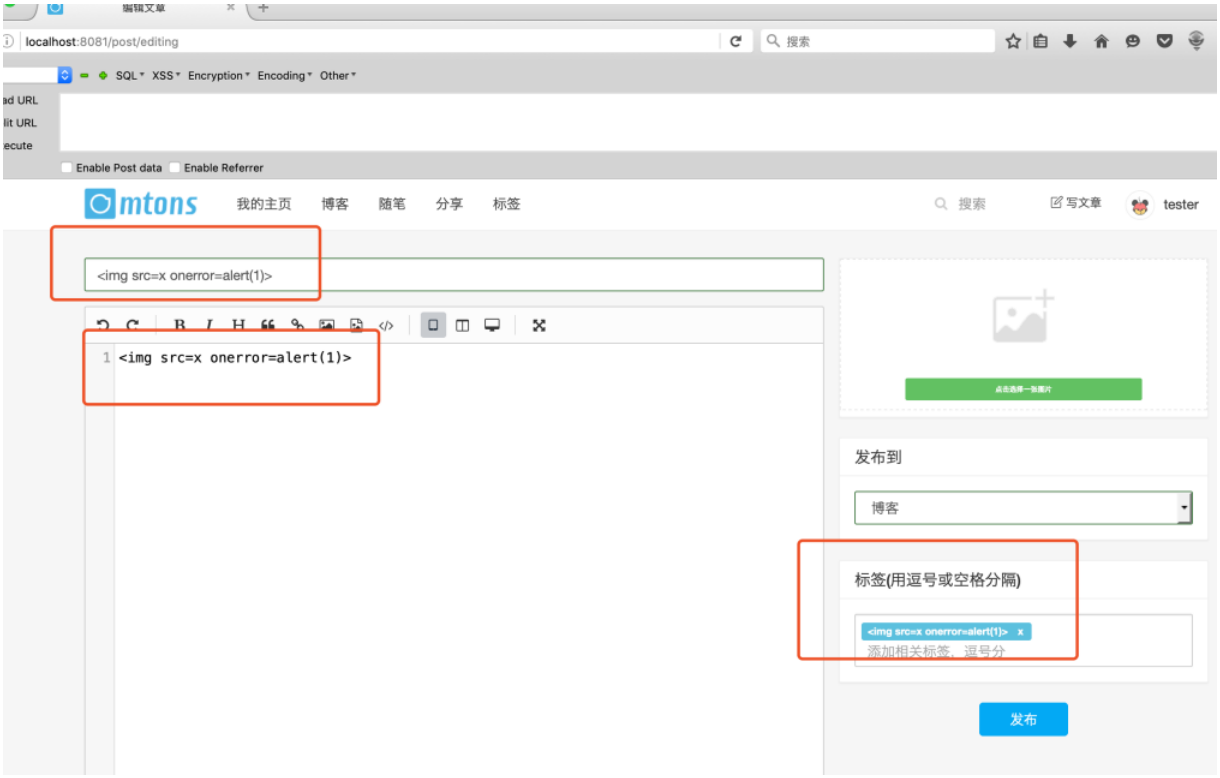
There are two stored XSS vulnerability #27

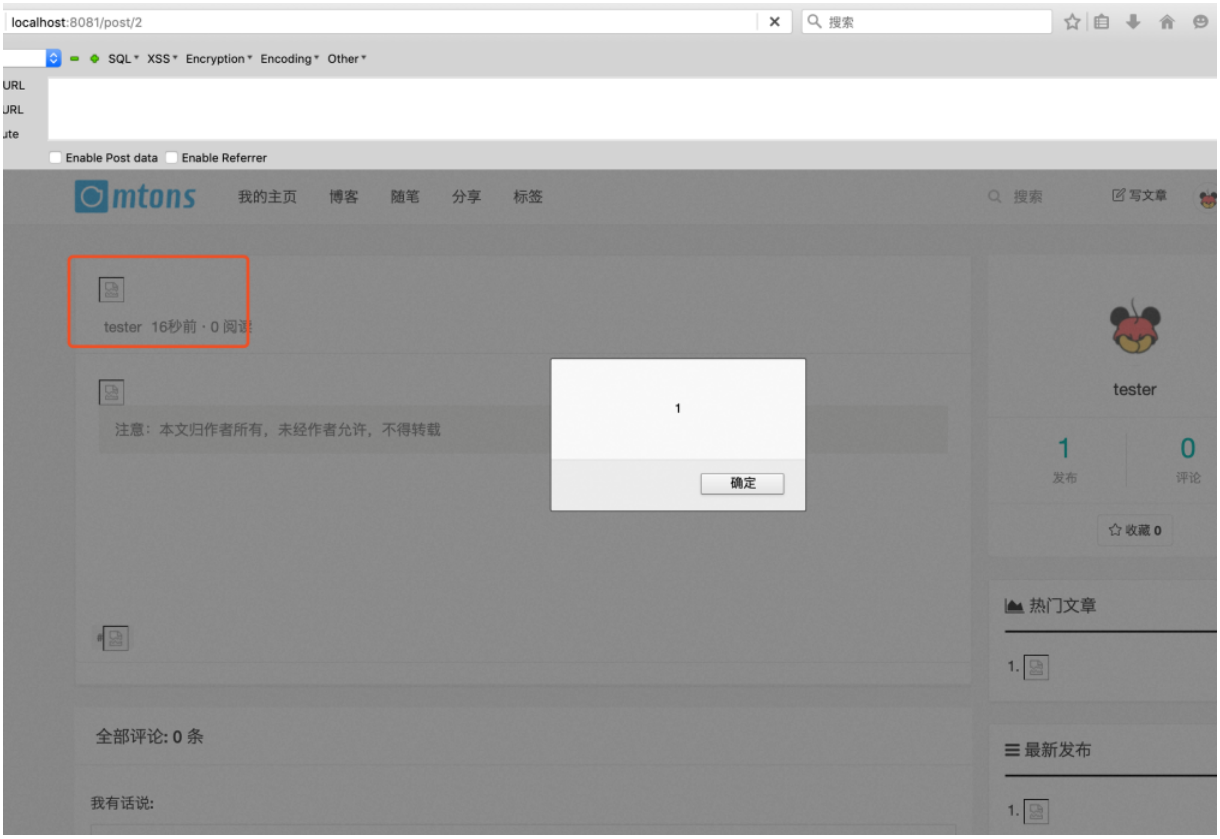
Open m4yfly opened this issue on Jun 13, 2019 · 0 comments

m4yfly commented on Jun 13, 2019

A xss vulnerability was discovered in mblog.
In mblog3.5, stored XSS exists via the `/post/editing` value parameter, which allows remote attackers to inject arbitrary web script or HTML.
poc

```
xss payload:
<img src=x onerror=alert(1)>
```

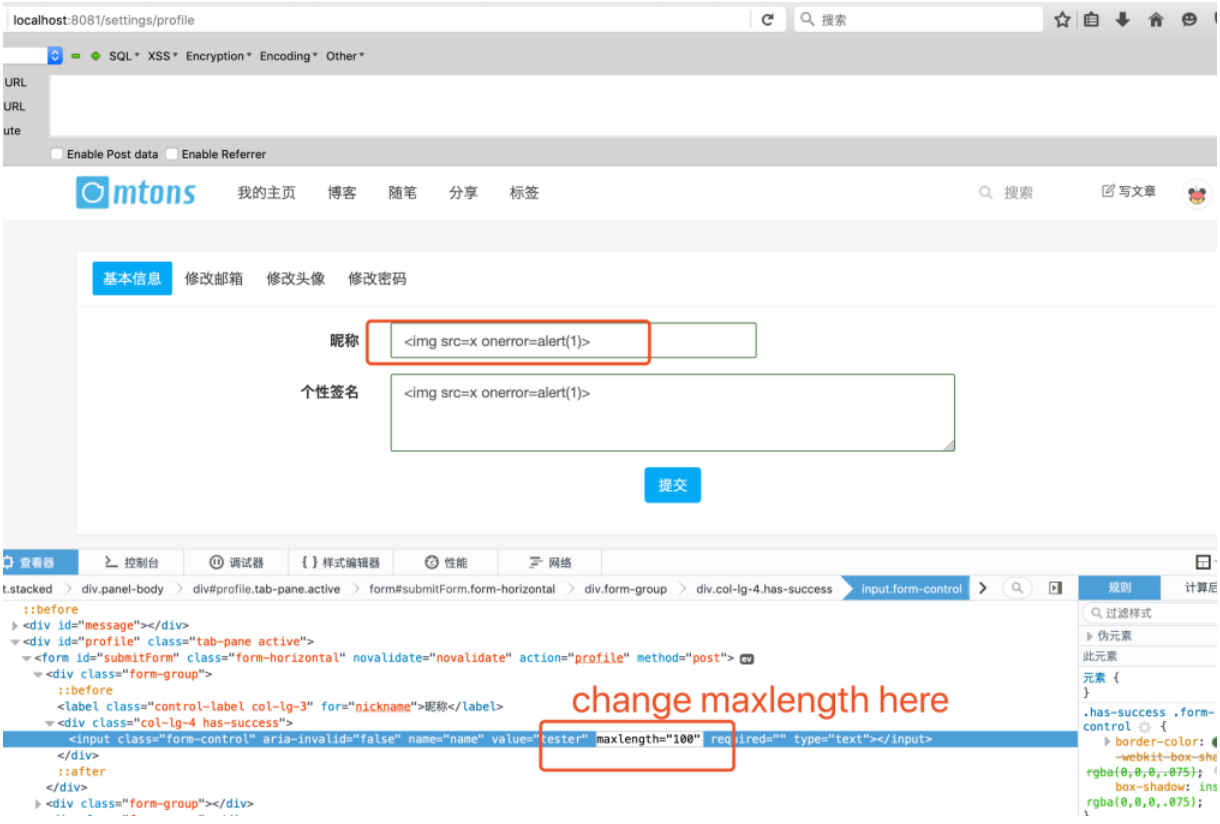


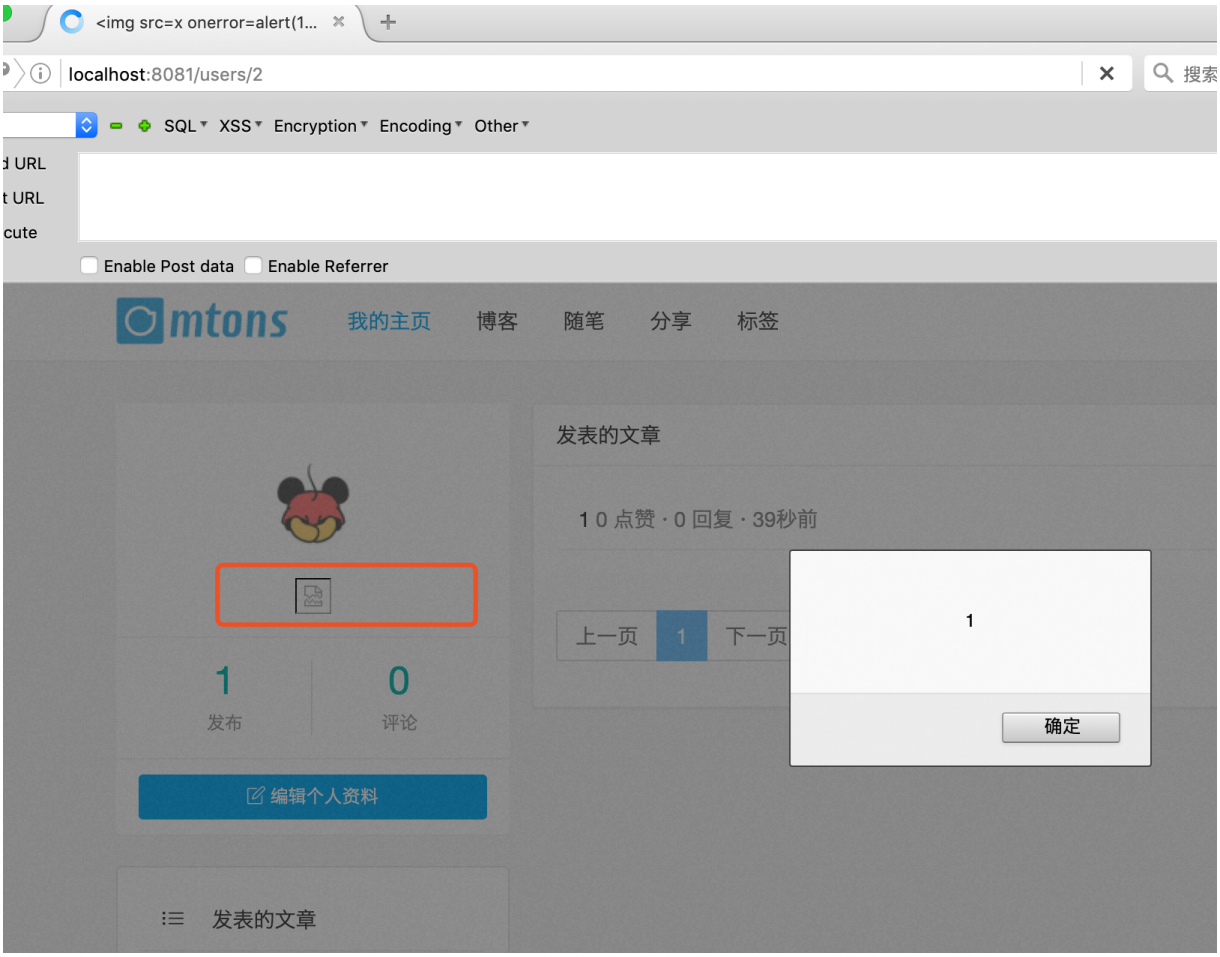


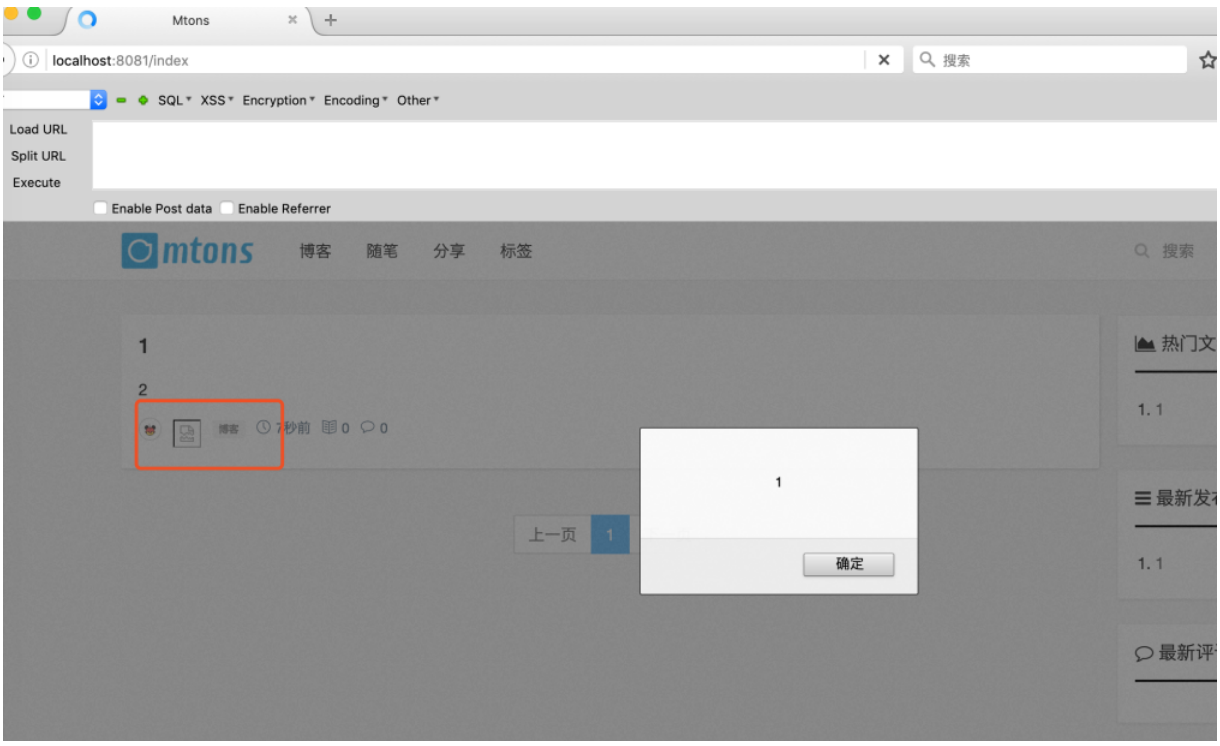
Another stored XSS exists via the `/settings/profile` value parameter, which allows remote attackers to inject arbitrary web script or HTML.

poc

```
xss payload:
<img src=x onerror=alert(1)>
```







Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant