

[New issue](#)

[Jump to bottom](#)

Stored XSS via filename parameter in '/api/storage/upload/PostImage' #316

 **Closed**

tuando243 opened this issue on Jul 7 · 1 comment

Assignees



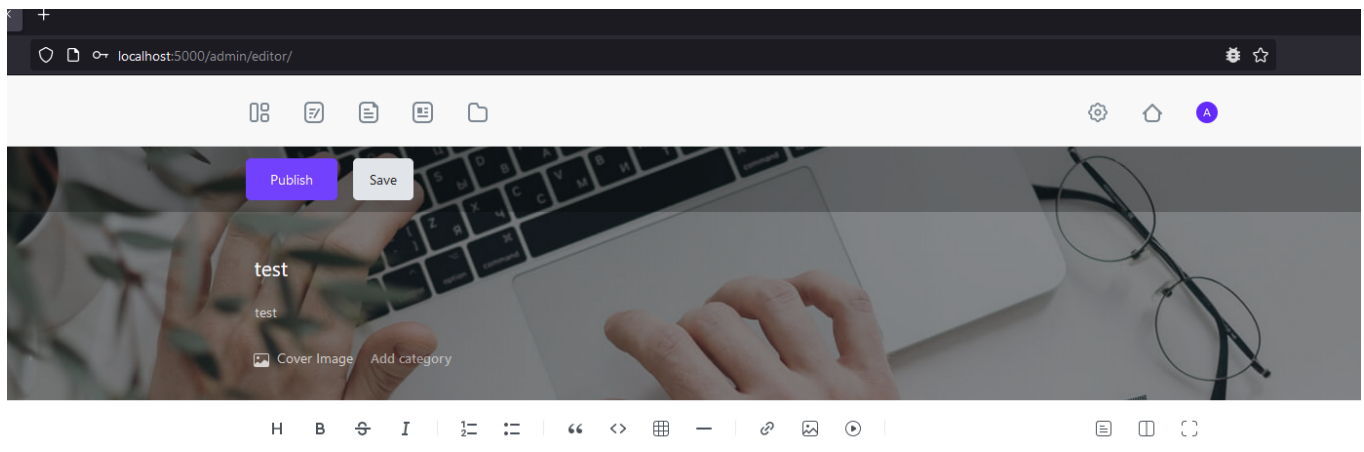
tuando243 commented on Jul 7 • edited ▼

Describe the bug

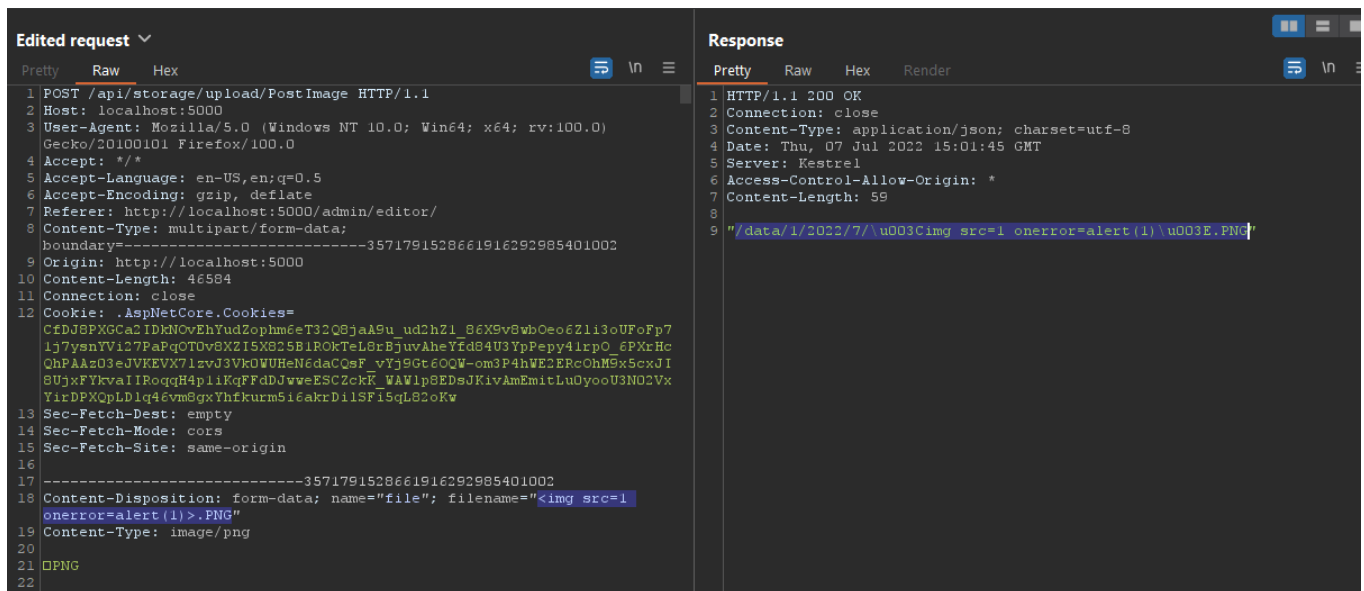
Stored XSS exists in Blogifier 3.0 via filename parameter in '/api/storage/upload/PostImage'.

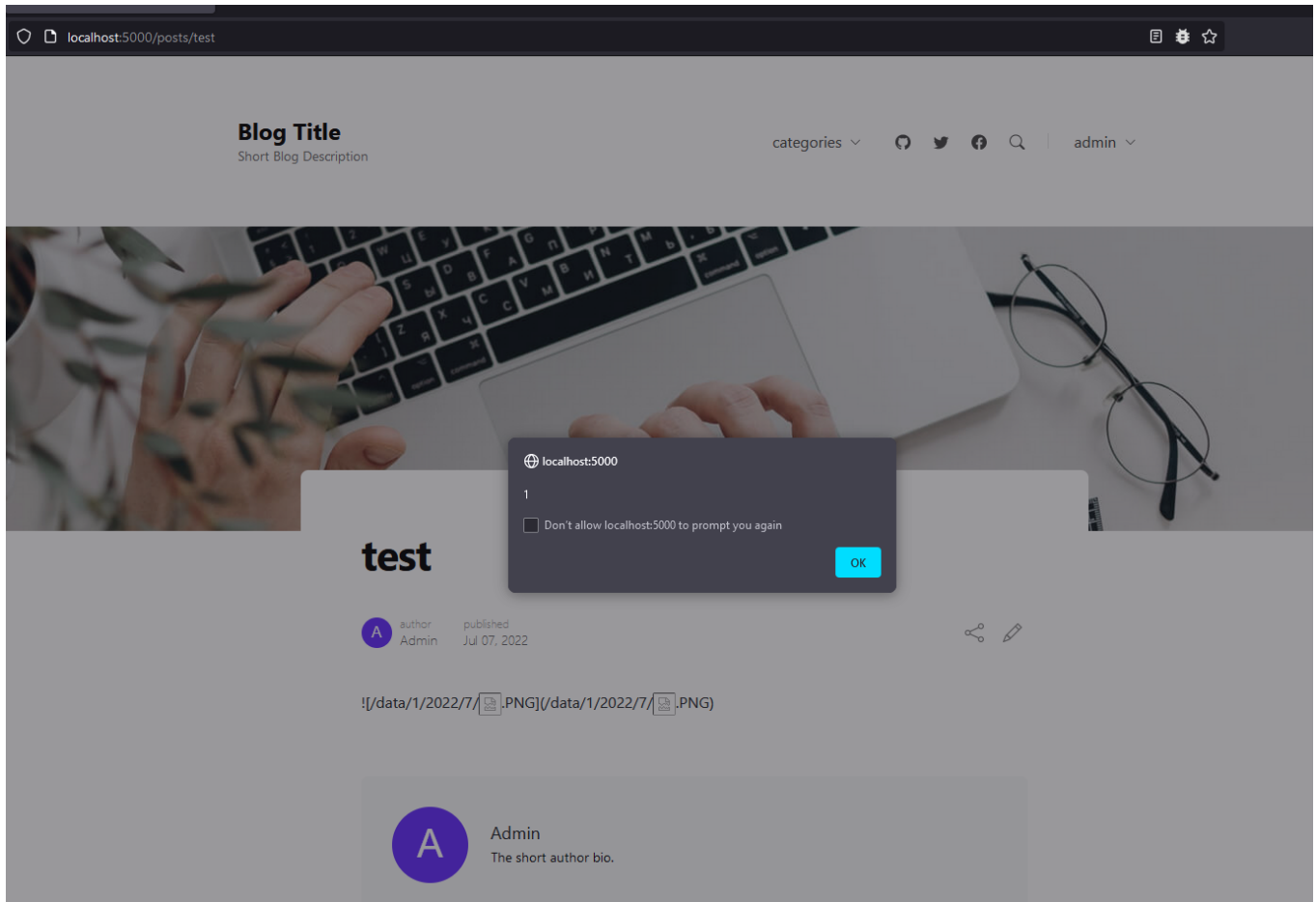
Steps to reproduce

1. Login as admin.
2. Click on 'New post'.
3. Click on 'Insert Image' and insert the following payload `` in filename field.
4. Click on Save, Publish and View the post.



[[data/1/2022/7/.PNG]]





  **farzindex** assigned **rxTUR** on Jul 7


rxTUR commented on Jul 9

Collaborator

Fixed with commit [97fcdac](#)

 **rxTUR** closed this as completed on Jul 9

Assignees

 **rxTUR**

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

