

New issue

<> Code ⊙ Issues 146 % Pull requests 26 ⊙ Actions ⊞ Projects □ Wiki

Jump to bottom

Anti-CSRF token is not working in Admin panel #3304

○ Closed jhespeter opened this issue on Dec 10, 2020 · 2 comments

Labels bug

jhespeter commented on Dec 10, 2020 • edited ▼

Bug description

In JupyterHub's Admin panel, the _xsrf token is not working for add/delete user features.

Current mechanism to protect add/delete user features against CSRF attack is solely rely on checking the Referer header value.

Although current referer header examination seems to be strict enough, it could still be bypassed if user is fooled to install malicious browser plugin or there exists any escape techniques.

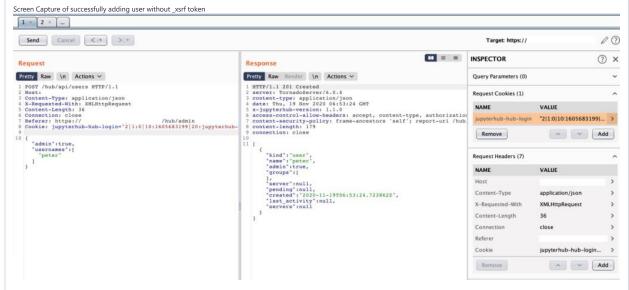
Expected behaviour

Implement anti-CSRF techniques like Double Submit Cookie, so that JupyterHub could prevent CSRF attack.

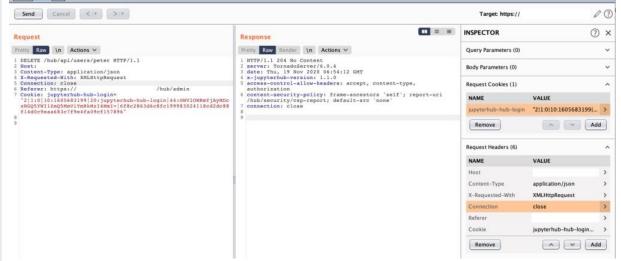
Actual behaviour

Even if the _xsrf token is removed the add/delete user requests could still be accepted & processed by server.

That could lead to a possible CSRF attack.



Screen Capture of successfully deleting user without _xsrf token



How to reproduce

- 1. Log in JupyterHub console with admin privilege
- 2. Click Control Panel button
- 3. Click Admin tab
- 4. Click Add User button / Delete User button

- 5. Use proxy technique to intercept the packet sent
- 6. Modify the packet by removing the _xsrf token
- 7. Send the request & see the request is accepted

Your personal set up

- OS: Kubernetes 1.12 + , Helm charts 3.0 + , ubi 7.8+
- Version(s): JupyterHub 1.1.0, Python 3.8

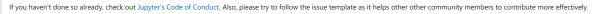
Reference

OWASP - Cross-Site Request Forgery Prevention Cheat Sheet

 $https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html \# double-submit-cookie$

welcome bot commented on Dec 10, 2020

Thank you for opening your first issue in this project! Engagement like this is essential for open source projects!





You can meet the other Jovyans by joining our Discourse forum. There is also an intro thread there where you can stop by and say Hi! 🤞

Welcome to the Jupyter community! 🞉

carnil commented on Apr 29

CVE-2020-36191 appers to have been assigned for this issue.

minrk closed this as completed on Sep 9

Assignees

No one assigned

Labels

bug

Projects

Milestone No milestone

Development

No branches or pull requests

3 participants

