

New issue

[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 adding user without `_xsrf` token

The screenshot shows the Chrome DevTools network tab with a selected POST request to `/hub/api/users`. The request is shown in the 'Request' pane, and the response is shown in the 'Response' pane. The 'Inspector' pane on the right shows the request cookies and headers.

Request:

```
1 POST /hub/api/users HTTP/1.1
2 Host:
3 Content-Type: application/json
4 X-Requested-With: XMLHttpRequest
5 Content-Length: 36
6 Connection: close
7 Referer: https:// /hub/admin
8 Cookie: jupyterhub-hub-login="2|1:0|10:1605683199|20:jupyterhub-
9
10 {
11   "admin":true,
12   "username":"peter"
13 }
```

Response:

```
1 HTTP/1.1 201 Created
2 server: TornadoServer/6.0.4
3 content-type: application/json
4 date: Thu, 19 Nov 2020 06:53:24 GMT
5 x-jupyterhub-version: 1.1.0
6 access-control-allow-headers: accept, content-type, authorization
7 content-security-policy: frame-ancestors 'self'; report-uri /hub
8 content-length: 179
9 connection: close
10
11 {
12   "kind":"user",
13   "name":"peter",
14   "admin":true,
15   "groups":[
16   ],
17   "server":null,
18   "pending":null,
19   "created":"2020-11-19T06:53:24.723862Z",
20   "last_activity":null,
21   "servers":null
22 }
```

Inspector:

Query Parameters (0)

Request Cookies (1)

NAME	VALUE
jupyterhub-hub-login	"2 1:0 10:1605683199 ..."

Request Headers (7)

NAME	VALUE
Host	
Content-Type	application/json
X-Requested-With	XMLHttpRequest
Content-Length	36
Connection	close
Referer	
Cookie	jupyterhub-hub-login...

Screen Capture of successfully deleting user without `_xsrf` token

The screenshot shows the Chrome DevTools network tab with a selected DELETE request to `/hub/api/users/peter`. The request is shown in the 'Request' pane, and the response is shown in the 'Response' pane. The 'Inspector' pane on the right shows the request cookies and headers.

Request:

```
1 DELETE /hub/api/users/peter HTTP/1.1
2 Host:
3 Content-Type: application/json
4 X-Requested-With: XMLHttpRequest
5 Connection: close
6 Referer: https:// /hub/admin
7 Cookie: jupyterhub-hub-login="2|1:0|10:1605683199|20:jupyterhub-hub-login|44:OWV1OWRmYjAyNDc
8 xOGp5W112mG55mV1YmRkXzI4MmI=|16f8c2863d6c8fc199983024118cd2dc88
9 f140c9eaa683c7f9e4fa09cf157896"
```

Response:

```
1 HTTP/1.1 204 No Content
2 server: TornadoServer/6.0.4
3 date: Thu, 19 Nov 2020 06:54:12 GMT
4 x-jupyterhub-version: 1.1.0
5 access-control-allow-headers: accept, content-type, authorization
6 content-security-policy: frame-ancestors 'self'; report-uri /hub/security/csp-report; default-src 'none'
7 connection: close
8
9
```

Inspector:

Query Parameters (0)

Body Parameters (0)

Request Cookies (1)

NAME	VALUE
jupyterhub-hub-login	"2 1:0 10:1605683199 ..."

Request Headers (6)

NAME	VALUE
Host	
Content-Type	application/json
X-Requested-With	XMLHttpRequest
Connection	close
Referer	
Cookie	jupyterhub-hub-login...

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

 jhespeter added the **bug** label on Dec 10, 2020

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! 🍕

If you haven't done so already, check out [Jupyter's Code of Conduct](#). Also, please try to follow the issue template as it helps other other community members to contribute more effectively.




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](#) appears to have been assigned for this issue.

 minrk closed this as completed on Sep 9

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

