

Logged-in user can unsubscribe anyone from any list using specially crafted POST request (CVE-2021-40347)

I'm forwarding this security report from Kevin Israel (Wikipedia user PleaseStand), who discovered this on lists wikimedia.org and filed a reporti n our tracker. https://phabricator.wikimedia.org/1289798, Using a specially crafted POST request, a logged-in user can unsubscribe anyone from any list.

Reproduction steps:

- Subscribe to a mailing list with address A and confirm the subscription
 Create an account using address B, and visit a mailing list page that you are not subscribed to, you should see the subscription form and an address
- 3. Using your browsers inspector, change the form's URL by replacing subscribe with unsubscribe/
- 4. Change the name attribute on the address <select> to "email".

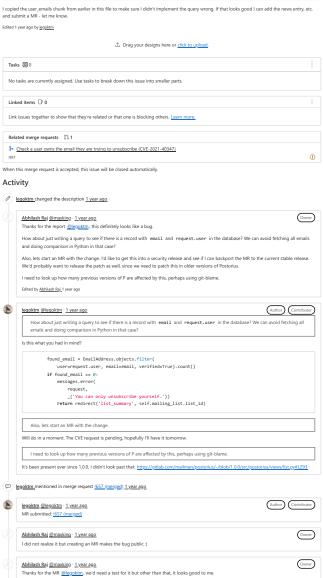
 5. Change the value of the selected option to be address A.

 6. Click the "Subscribe" button.

You'll see that address A has now been unsubscribed. Additionally, address B now knows that A was subscribed to the list, allowing for leaking the subscriber list as they'd receive an error like ""a@example.com is not a member address of ..." if A was not subscribed.

Here's a patch that I've tested works functionally and deployed to lists.wikimedia.org:

```
diff --git a/src/postorius/views/list.py b/src/postorius/views/list.py
index f03f1c13..1864c71f 100644
--- a/src/postorius/views/list.py
+++ b/src/postorius/views/list.py
subscribeView(MailingListView):
      request,
```



legoktm_changed title from Logged-in user can unsubscribe anyone from any list using specially crafted POST request to Logged-in user can unsubscribe anyone from any list using specially crafted POST request (CVE-2021-40347) 1_year.ago

Author Contributor

I did not realize it but creating an MR makes the bug public :(

