



0 Emails from Grammarly missing sanitization(lack of validation?) -> HTML injection in emails

Share:

State ☐ Duplicate (Closed)

Disclosed **April 30, 2019 11:39am +0530**

Reported To [Grammarly](#)

Asset [app.grammarly.com](#)
(Domain)

Weakness Violation of Secure Design Principles

Severity Low (0.1 ~ 3.9)

Participants

Duplicate Of [#391090](#)

Visibility Disclosed (Full)

[Collapse](#)

TIMELINE



[metnew](#) submitted a report to [Grammarly](#).

Sep 4th (8 months ago)

Summary:

Emails from Grammarly (e.g. "reset password" email) missing HTML sanitization. That leads to content spoofing in emails.

Steps To Reproduce:

1. Go to "Profile"
2. Find reset password tab (if you're logged in using FB/Google, you won't see this menu)
3. Change email to something like: `user@mail.com` -> `user+<h1>2@mail.com`
4. Find the letter from Grammarly in your inbox, about password reset attempt.
5. `<h1>` tag is noticeable.

Impact

Currently, the impact is miserable - content spoofing in "reset password" emails (sounds like a joke).

However, it's still a bad behavior. I guess that HTML injection through unsanitized/unvalidated input **could affect other Grammarly's email templates**.

1 attachment:

F342004: [grammarly-html-in-emails.mp4](#)



[fidgetspinner](#) HackerOne staff posted a comment.

Sep 7th (8 months ago)

Hi [@metnew](#),

Thanks for your submission. We are currently reviewing your report and will get back to you once we have additional information to share.

Kind regards,

[@fidgetspinner](#)



[fidgetspinner](#) HackerOne staff closed the report and changed the status to ☐ Duplicate ([#391090](#)).


Sep 7th (8 months ago)

Hi [@metnew](#),

Thank you for your submission! Unfortunately, we have already been made aware of this issue, so this submission will be closed as a duplicate. We appreciate the report and look forward to future reports from you.

Kind regards,

[@fidgetspinner](#)

-  [metnew](#) requested to disclose this report. Dec 11th (5 months ago)
-  [andriy_derevyanko](#) agreed to disclose this report. Apr 30th (about 1 hr ago)
-  This report has been disclosed. Apr 30th (about 1 hr ago)