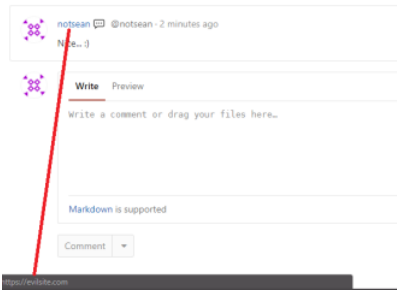


Add into our name and bypass "/" being used in URL to create a valid URL + custom image on snippets

[HackerOne report #46024](#) by zseano on 2018-12-11:

Summary: For some reason GitLab allow for certain HTML tags in our name which renders when we visit a snippet. Using this we can actually trick the user into visiting our URL when they click our username.

Description: When setting your name, using will render a valid link, except using will not work. However if we use notsean, it allows it through and we get this result. The use of \ is important since / is filtered.



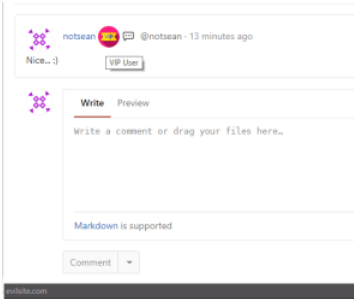
If a user is to click onto my name to visit my profile, they will actually be redirected to my site instead. To see it in action, visit <https://gitlab.com/snippets/1788795> and check out my comment from my account [@notsean](#), hover over my profile and you'll see it redirects to evilsite.com

We can then be a bit more clever and add an image icon, add the "title" attribute, and we can build a perfect phisher to either harvest their credentials, OR redirect to a GitLab Oauth application and gain access via that (users are more likely to just click ALLOW, especially if they think they will get some VIP upgrade... :D)

Steps To Reproduce:

(Add details for how we can reproduce the issue)

1. Visit your GitLab account settings and set your name to `<a href=http:\\evilsite.com¬sean <img src=https:\\www.bugbountynotes.com\\assets\\img\\vip.png" title="VIP User"` - Replace notsean with your username to look real.
2. Go comment on a snippet and people will see a 'VIP' badge next to your name, hover over it will show 'VIP User', and clicking it will redirect to our site. The perfect scenario for an attacker! :)



Impact

Add custom HTML to our name and trick user into handing over their credentials or giving us access to their gitlab account via a rogue application designed to look like it will get them a "VIP" upgrade (this is just an example)

Attachments

Warning: Attachments received through HackerOne, please exercise caution!

- [gitlab-bug.png](#)
- [gitlab-href.png](#)

Testing Activity

[@fsanpedro](#)

- Test that the user name is rendering the html name but as text and not as html

Security Testing Activity

[@vi](#)

- Test that names are rendered safely

MR Breakdown

[@fsanpedro](#)

- In https://gitlab.com/gitlab-org/gitlab/blob/master/app/views/shared/notes/_note.html.haml#L35 we call the method `sanitize` to clean the user name. Nevertheless, that method ends up calling `html_safe`. Therefore, if the `a` attribute is allowed, the user name will be rendered as html.

We can easily fix by replacing the method `sanitize` with `simple_sanitize`. Nevertheless, this method removes all html tags from the name. To be compliant with other parts of the platform, we shouldn't do this. In other features, we just render the user name without removing any data, just showing it as text instead of as HTML.


- The fix will pass by removing the call to `sanitize` in that line, and just show the user name directly as text.

[@vi](#)


- The rendering of the user's name can be modified to not call `html_safe`, which will fix the rendering of any existing malicious user names

Edited 2 years ago by [Darius Satchar](#)


📁 Drag your designs here or [click to upload](#)

Tasks 

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.


Linked items 

Relates to


 HTML injection issue in snippets via name parameter

#26673


🕒 13.2 📅 Apr 23, 2019

 Denial of Service on Snippets Page via User Comments


#222867

 Hyperlink injection in full name field of user profile

#300713

📅 May 2, 2021 

Activity




GitLab SecurityBot @gitlab-securitybot · 4 years ago

Author

Reporter

[HackerOne comment](#) by zseano:
Did not realise it would be posted publicly on "explore snippets". Moved my snippet to "private" to prevent anyone from seeing the issue, please let me know if I need to do anything to give you access to the priv snippet or if you need help replicating



GitLab SecurityBot @gitlab-securitybot · 4 years ago


Author

Reporter


[HackerOne comment](#) by gitlab-securitybot-api:
Hi @zseano,

Thank you for submitting this report. We will investigate the issue as soon as possible. Due to our current workload, we will get back within 14 business days with an update.


Best regards, GitLab Security Team




Antony Saba added priority 3 severity 3 · scoped labels 4 years ago



Antony Saba added Create (DEPRECATED) label 4 years ago




Antony Saba changed due date to February 23, 2019 4 years ago



Antony Saba @asaba · 4 years ago

Contributor


cc @jramsay




James Ramsay (ex-GitLab) @jramsay-gitlab · 4 years ago

Contributor

/cc @jeremy @lmcandrew




James Ramsay (ex-GitLab) added Manage (DEPRECATED) label and removed Create (DEPRECATED) label 4 years ago




Dennis Appelt @dappeit · 3 years ago

Developer


This also works in the breadcrumbs navigation <https://gitlab.com/gitlab-org/gitlab-ce/issues/57529#note-140195700>



Douwe Maan mentioned in issue gitlab-ce#57529 3 years ago




Antony Saba added denovo manage · scoped label 3 years ago



Antony Saba @asaba · 3 years ago

Contributor

[@jeremy](#) [@jramsay](#), This issue is past the Due Date, not sure if it was missed due to missing stage labels, but cc'ing both of you since this was changed to -Manage, but the related gitlab-ce#57529 was assigned to -Create.



Jeremy Watson (ex-GitLab) @jeremy-wl · 3 years ago

Contributor


This issue is past the Due Date, not sure if it was missed due to missing stage labels

Thanks [@asaba](#), I'm aware of this one and tracking it. We don't have the capacity on [Manage-to-pick-up gitlab-ce#3713901](#) issues, we're still working through the gitlab-ce-3713902 backlog.


We have [many](#) of these issues and many of them will miss due dates unless some of these go to other teams or Manage hires to our 2019 plan.

cc [@lmcandrew](#)


Edited by [Jeremy Watson \(ex-GitLab\)](#) 3 years ago




Jeremy Watson (ex-GitLab) changed milestone to %Next 3-4 releases 3 years ago



GitLab Bot added Accepting merge requests label 3 years ago



Jeremy Watson (ex-GitLab) added to epic 61322 3 years ago




Jeremy Watson (ex-GitLab) @jeremy-wl · 3 years ago

Contributor


[@and3](#), is this -Create since this is only rendering on Snippets? 🤔

Ah, I see comments in <https://gitlab.com/gitlab-org/gitlab-ce/issues/57529#note-154274012> that make me think otherwise


Edited by [Jeremy Watson \(ex-GitLab\)](#) 3 years ago



Virginia Alexieva added group optimize · scoped label 3 years ago




Virginia Alexieva added group authentication and authorization · scoped label and automatically removed group optimize label 3 years ago




Virginia Alexieva @valexieva · 3 years ago

Contributor


[@jeremy](#)




Jeremy Watson (ex-GitLab) added group not owned · scoped label 3 years ago




Jeremy Watson (ex-GitLab) changed milestone to %12.7 3 years ago




GitLab Bot changed due date to February 23, 2019 3 years ago



GitLab Bot changed milestone to %12.7 3 years ago



GitLab Bot moved from gitlab-ce#55279 3 years ago




Alexander Dietrich @adietrich · 3 years ago

Developer


This is one of two [group not owned](#) security issues that are not [feature](#) issues and therefore have a remediation goal. (Interestingly, it has a --"group:access" label at the same time, I thought that wasn't supposed to be possible.)

If --"group:access" is not correct, who would be more appropriate?


CC [@hurbanc](#)



Virginia Alexieva added group source code · scoped label and automatically removed group authentication and authorization group not owned labels 3 years ago




Virginia Alexieva added Category:Snippets label 3 years ago



Virginia Alexieva @valexieva · 3 years ago

Contributor

[@adietrich](#), adding [@rbikai](#) because I think this is directly related to snippets, so he can prioritize.




Kai Armstrong @rbikai · 3 years ago

Developer

[@adietrich](#), I don't think this is --snippets. Unless this is a rendering issue? But it seems like we're probably not sanitizing the user input where they can create a username. I'm guessing it happens that we render that differently in snippets, but this should be sanitized long before it gets there.

I'd be inclined to also say --"group:access" based on "user".




Alexander Dietrich @adietrich · 3 years ago

Developer

Right, it seems like --snippets is just one of the places the HTML injection can show up.

[@dappeit #26673 \(closed\)](#) seems to be a duplicate or very similar to this issue, so the same group:: should be used?



Virginia Alexieva @valexieva · 3 years ago

Contributor

[@jeremy](#)

Please [register](#) or [sign in](#) to reply

✓

Virginia Alexieva added `group: authentication and authorization` scoped label and automatically removed `group: source code` label 3 years ago

🕒

Jeremy Watson (ex-GitLab) changed milestone to %13.0 3 years ago

🚩

GitLab Bot @gitlab-bot · 2 years ago

Maintainer

Setting `category: authentication and authorization` based on `--"group:access"`.

🚩

GitLab Bot @gitlab-bot · 2 years ago

Maintainer

Setting `category: authentication and authorization` based on `--"group:access"`.

✓

GitLab Bot added `category: authentication and authorization` label 2 years ago

🕒

Jeremy Watson (ex-GitLab) changed milestone to %13.12 2 years ago

👤

Michelle Gill @m.gill · 2 years ago

Developer

@dsatcher

how do you feel about picking up this issue based on this thread [gitlab.com/Product#624 \(comment 347433720\)](#)?

👤

Darva Satcher @dsatcher · 2 years ago

Maintainer

@m.gill

, yes we can take this one on.

/cc @phika

Please [register](#) or [sign in](#) to reply

💬

Darva Satcher mentioned in issue #26673 (closed) 2 years ago

✓

Darva Satcher added `group: editor` (`discuss` `create`) scoped labels and automatically removed `group: authentication and authorization` (`show` `manage`) labels 2 years ago

✓

Darva Satcher added `workflow: planning breakdown` scoped label 2 years ago

✓

Darva Satcher removed `workflow: planning breakdown` label 2 years ago

⚖

Darva Satcher changed weight to 1 2 years ago

✎

Darva Satcher changed the description 2 years ago

🕒

Darva Satcher removed milestone 2 years ago

🕒

Darva Satcher changed milestone to %13.2 2 years ago

👤

Darva Satcher @dsatcher · 2 years ago

Maintainer

@brouillon

.

Can you review our security testing plan for this issue? I think that it is simple, but just checking in with you.

👤

Juan Brouillon @jbrouillon · 2 years ago

Contributor

@dsatcher

the testing plan looks good to me. Regarding the fix, removing `html_safe` should fix the issue, and if there is some HTML that needs to be rendered we should use safe alternatives like the `tag` and `safe_join` ActionView helpers.

/cc @vi @fisanpedro

👤

Francisco Javier López @fisanpedro · 2 years ago

Contributor

Thanks

@brouillon

I took a look at other places where we render user names and we just show plain text.

BTW, @brouillon do you think this issue has to be fixed using the security workflow?

👤

Juan Brouillon @jbrouillon · 2 years ago

Contributor

@fisanpedro

Ideally, yes. The severity of the issue is low but it is a valid vulnerability.

👤

Francisco Javier López @fisanpedro · 2 years ago

Contributor

👍

Thanks!!

Please [register](#) or [sign in](#) to reply

✓

Darva Satcher added `workflow: ready for development` scoped label and automatically removed `workflow: scheduling` label 2 years ago

✓

Juan Brouillon added `status: ready` (`complete`) scoped label 2 years ago

✓

Kai Armstrong added `backlog` label 2 years ago

💬

Darva Satcher mentioned in issue create-stage#12685 (closed) 2 years ago

✓

Kai Armstrong added `status: manage` scoped label and automatically removed `status: create` label 2 years ago

✓

Kai Armstrong added `unreviewable` label 2 years ago

💬

Kai Armstrong mentioned in issue #222867 (closed) 2 years ago

🔒

Jeremy Matos marked #222867 (closed) as a duplicate of this issue 2 years ago

✓

Jeremy Matos marked this issue as related to #222867 (closed) 2 years ago

👤

Darva Satcher assigned to @fisanpedro 2 years ago

👤

Francisco Javier López @fisanpedro · 2 years ago

Contributor

@vi

I think you haven't work in a security issue before and, since from the developing part this one is quite easy, you can learn how this workflow goes.

👤

Darva Satcher @dsatcher · 2 years ago

Maintainer

@fisanpedro

.

Thanks! Good idea 👍

Please [register](#) or [sign in](#) to reply

👤

Francisco Javier López assigned to @vi 2 years ago

👤

Francisco Javier López unassigned @fisanpedro 2 years ago

✓

GitLab Bot removed `Acception: merge requests` label 2 years ago

✓

Vijay Hawoldar added `workflow: in review` scoped label and automatically removed `workflow: ready for development` label 2 years ago

✓

Vijay Hawoldar added `workflow: verification` scoped label and automatically removed `workflow: in review` label 2 years ago


👤

Vijay Hawoldar @vi · 2 years ago

Developer

This has now been fixed in https://gitlab.com/gitlab-org/security/gitlab/-/merge_requests/651


 [Vijay Hawoldar](#) closed 2 years ago

 **GitLab SecurityBot** @gitlab-securitybot · 2 years ago

Author

Reporter


This [HackerOne](#) [security](#) issue was closed 30 days ago and may become public.

Please ensure the following items are true and add a  reaction:

- Issue description and comments do not contain sensitive data belonging to GitLab.
- Issue does not reveal private information of the reporter (i.e. session IDs, passwords).

If the issue needs to stay confidential, please add the [https://confidential](#) label.

If you removed confidential data from the issue description before making it public, make sure that the description history entry is deleted.


 **Jeremy Matos** @jeremymatos · 2 years ago

Contributor

Making issue public.

Please [register](#) or [sign in](#) to reply

 [Jeremy Matos](#) made the issue visible to everyone 2 years ago

 [Andrew Kelly](#) marked this issue as related to [#300713](#) (closed) 1 year ago

Please [register](#) or [sign in](#) to reply