Closed · Issue created 2 years ago by GitLab SecurityBot

Stored XSS in merge request because of target branch

HackerOne report #1030189 by `ashish_r_padelkar` on 2020-11-09, assigned to @kaunghtet:

Report | Attachments | How To Reproduce

Report

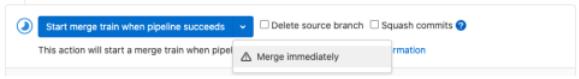
Summary

Hello,

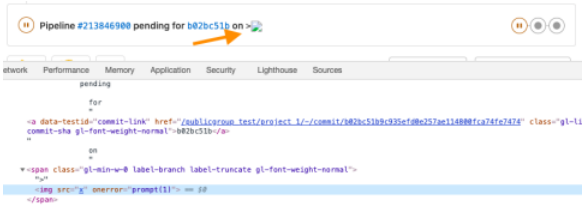
I Found a stored XSS in merge request which triggers for everyone in public project as merge requests are available for everyone. Currently Gitlab.com is prevented because of CSP.

Steps to reproduce

1. Create a file at `-/new/master/` and in `Target Branch` section put branch name as XSS payload `"><img/src='x'onerror=prompt(1)>`.
2. Create a merge request now at `/-/merge_requests/new`. Select `Target Branch` as above branch with XSS payload and create a merge request.
3. As soon as you create merge request, you should see below button



4. Click on `Merge Immediately`
5. It will create a pipeline and appears as a note which triggers this XSS



Output of checks

This bug happens on GitLab.com

Regards,
Ashish

Impact

Stored XSS in merge request

Attachments

Warning: Attachments received through HackerOne, please exercise caution!

- Screenshot_2020-11-10_at_00.52.04.png
- Screenshot_2020-11-10_at_00.53.36.png

How To Reproduce

Please add reproducibility information to this section:

1.
2.
3.

Edited 2 years ago by Kaung Htet Aung

Drag your designs here or click to upload.

Tasks 0

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

Linked items 0

Link issues together to show that they're related or that one is blocking others. Learn more.

Activity

GitLab SecurityBot changed due date to February 08, 2021 2 years ago

GitLab SecurityBot added HackerOne security labels 2 years ago

GitLab SecurityBot added Weakness CWE-79 priority 3 severity 3 scoped labels 2 years ago

GitLab SecurityBot added security-group-missing security-triage-appsec labels 2 years ago

Kaung Htet Aung changed the description 2 years ago

Kaung Htet Aung added Category:Source Code Management frontend labels 2 years ago

Kaung Htet Aung added group source code devops create scoped labels 2 years ago

Kaung Htet Aung @kaunghtet · 2 years ago
@danielgruesso @m_gill I have confirmed this XSS occurring at target branch name within pipeline info.

Michelle Gill @m_gill · 2 years ago Developer
Thanks @kaunghtet !

Please register or sign in to reply

Kaung Htet Aung removed security-group-missing label 2 years ago

Kaung Htet Aung removed security-triage-appsec label 2 years ago

GitLab SecurityBot @gitlab-securitybot · 2 years ago Author Reporter
This issue is ready for triage as per HackerOne process.

About this automation: AppSec Escalation Engine

Michelle Gill added Category:Code Review label 2 years ago

Michelle Gill removed Category:Source Code Management label 2 years ago

Michelle Gill changed milestone to %13.8 2 years ago

GitLab Bot added Accepting merge requests label 2 years ago

GitLab Bot @gitlab-bot · 2 years ago — Maintainer

Setting label(s) Category:Source Code Management section dev based on group source code.

GitLab Bot added Category:Source Code Management label 2 years ago

GitLab Bot added section dev scoped label 2 years ago

Dheeraj Joshi @djadmin · 2 years ago — Developer

This should be fixed by #241939 (closed) and probably #241960 (closed) too.

André Luís @andr3 · 2 years ago — Developer

Moving to proper group.

André Luís added group code review scoped label and automatically removed group source code label 2 years ago

André Luís removed Category:Source Code Management label 2 years ago

André Luís changed weight to **2** 2 years ago

Kai Armstrong changed milestone to %13.9 2 years ago

Michelle Gill mentioned in issue create-stage#12785 (closed) 1 year ago

André Luís @andr3 · 1 year ago — Developer

This has been picked up as Deliverable for %13.9.

André Luís added Deliverable label 1 year ago

André Luís assigned to @jerasmus 1 year ago

GitLab Bot removed Accepting merge requests label 1 year ago

Costel Maxim @cmaxim · 1 year ago — Developer

CVE requested: https://gitlab.com/gitlab-org/cves/-/issues/136

Jacques Erasmus added workflow in dev scoped label 1 year ago

Costel Maxim @cmaxim · 1 year ago — Developer

This issue was fixed in the 13.8.2 release.

Costel Maxim closed 1 year ago

Jacques Erasmus added workflow verification scoped label and automatically removed workflow in dev label 1 year ago

Costel Maxim mentioned in issue #322469 (closed) 1 year ago

Dominic Couture mentioned in issue #205305 1 year ago

GitLab SecurityBot @gitlab-securitybot · 1 year 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 keep confidential label.

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

Dominic Couture made the issue visible to everyone 1 year ago