huntr

Stored xss bug in go-gitea/gitea

0

✓ Valid Reported on May 6th 2022

Description

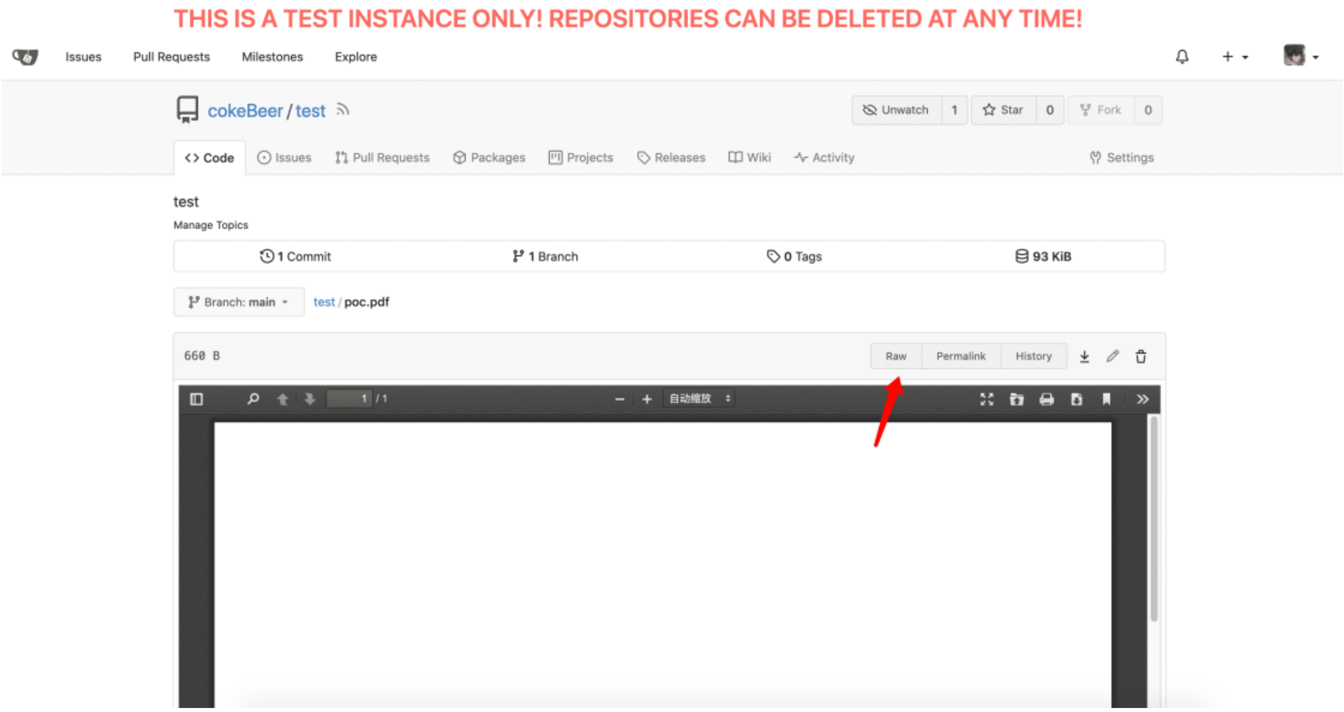
stored xss bug

Proof of Concept

I created a repository on `try.gitea.io` and uploaded a pdf file containing xss vector.

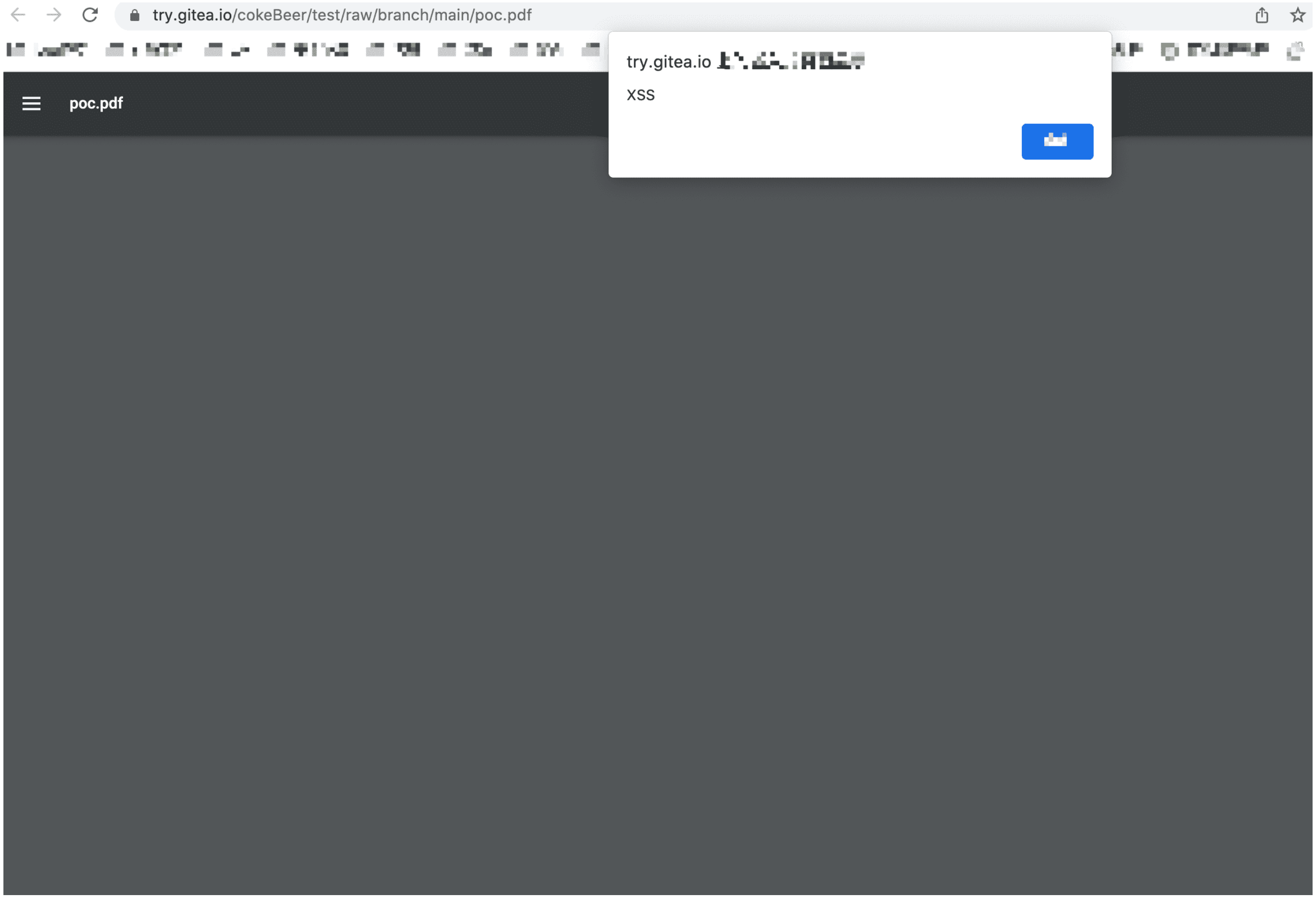
```
https://try.gitea.io/cokeBeer/test/src/branch/main/poc.pdf
```

Just click the "Raw" button



THIS IS A TEST INSTANCE ONLY! REPOSITORIES CAN BE DELETED AT ANY TIME!

The xss vector will be triggered



try.gitea.io/cokeBeer/test/raw/branch/main/poc.pdf

try.gitea.io

xss

Fix Suggestion

prohibit viewing pdf directly by browser's default viewer

Impact

As the repo is public , any user can view the report and when open the attachment then xss is executed. This bug allow executed any javascript code in victim account .

References

- PDF to XSS

CVE
CVE-2022-1928
(Published)

Vulnerability Type

CWE-79: Cross-site Scripting (XSS) - Stored

Severity

Medium (4.4)

Registry

Golang

Affected Version

v1.16.7

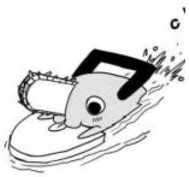
Visibility

Public

Status

Fixed

Found by



cokebeer

@cokebeer

legend

Fixed by

Lauris BH

@lafriks

maintainer

This report was seen 1,043 times.

We are processing your report and will contact the **go-gitea/gitea** team within 24 hours. 7 months ago

cokebeer modified the report 7 months ago

We have contacted a member of the **go-gitea/gitea** team and are waiting to hear back 7 months ago

Lunny Xiao 7 months ago Maintainer

Looks like the pdf file will pop up the window even if running as a local file.

Chat with us

cokebeer 7 months ago Researcher

Yes. I think it is due to brower's feature as a pdf reader . But a xss in local file can't steal cookie or token in a target site because of the wrong host (like file://xxxxxx instead of http://gitea.com) and will be less harmful. Prohibiting viewing pdf directly by browser's default viewer on target site will be safer.

cokebeer 7 months ago Researcher

any feedback?

We have sent a follow up to the **go-gitea/gitea** team. We will try again in 7 days. 7 months ago

We have sent a second follow up to the **go-gitea/gitea** team. We will try again in 10 days. 6 months ago

Lauris BH 6 months ago Maintainer

I wonder does Content-Security-Policy sandbox header would prevent that (similarly as we do for SVG)

cokebeer 6 months ago Researcher

No. The PDF file is view directly by Chrome's PDF viewer. Better just probitting this like github do

Lauris BH 6 months ago Maintainer

But GitHub does display pdf files same as we do just under different subdomain

cokebeer 6 months ago Researcher

A link please? Mainly I foucus on whether the pdf file can be easily controlled by malicous user.

We have sent a third and final follow up to the **go-gitea/gitea** team. This rep considered stale. 6 months ago

Chat with us

Lauris BH 6 months ago

Maintainer

https://github.com/mozilla/pdf.js/blob/master/examples/learning/helloworld.pdf

when clicking on this on `Raw` it will open:
https://raw.githubusercontent.com/mozilla/pdf.js/master/examples/learning/helloworld.pdf

With headers:

```
Content-Security-Policy: default-src 'none'; style-src 'unsafe-inline'; sandbox
Content-Type: application/octet-stream
```

cokebeer 6 months ago

Researcher

On my Chrome, the PDF is downloaded directly via your link. Whatever, I just advice the bug. Whether to fix it is up to yours.

Lauris BH modified the Severity from High to Low 6 months ago

Lauris BH 6 months ago

Maintainer

Imho CVSS is `AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:N` - 4.4

Lauris BH modified the Severity from Low to Medium (4.4) 6 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

Lauris BH validated this vulnerability 6 months ago

cokebeer has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Lauris BH 6 months ago

Chat with us

I have submitted PR to fix this issue: https://github.com/go-gitea/gitea/pull/19825

Lauris BH marked this as fixed in **1.16.9** with commit **65e068** 6 months ago

Lauris BH has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation