huntr

Cross-site Scripting (XSS) - Reflected in beancount/fava

0

✓ Valid Reported on Jun 9th 2022

Description

The time parameter in `fava` is vulnerable to reflected XSS

Proof of Concept

1.Open the web browser to access the fava webpage.
2.Access the url: `https://fava.pythonanywhere.com/example-beancount-file/income_statement/?time=%22%3E%3Cbutton+onclick%3Dalert%281%29%3EClICK+ME%3C%2Fbutton%3E` Script will be reflected in on clicking the button.
3.when the victim clicks on the button -> Alert box will pop up

Image

https://drive.google.com/file/d/1PJ_kKyn5KrHbzplApD-rfhuwSbtsCTvS/view?usp=sharing

Impact

If an attacker can control a script that is executed in the victim's browser, then they can typically fully compromise that user. Amongst other things, the attacker can:
+Perform any action within the application that the user can perform.
+View any information that the user is able to view.
+Modify any information that the user is able to modify.
Initiate interactions with other application users, including malicious attacks, that will appear to originate from the initial victim user. There are various means by which an attacker might induce a victim user to make a request that they control, to deliver a reflected XSS attack. These include placing links on a website controlled by the attacker, or on another website that allows content to be generated, or by sending a link in an email, tweet or other message

References

- huntr.dev

- https://owasp.org/www-project-top-ten/2017/A7_2017-Cross-Site_Scripting_(XSS)

CVE
CVE-2022-2514
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Reflected

Severity
High (8)

Registry
Pypi

Affected Version
v1.21

Visibility
Public

Status
Fixed

Found by

saharshtapi
@saharshtapi
master ⌄

This report was seen 504 times.

We are processing your report and will contact the **beancount/fava** team within 24 hours.
6 months ago

saharshtapi modified the report 6 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 6 months ago

saharshtapi 5 months ago Researcher

@admin can you please sent the magic link to the maintainers at this emails
mail@jakobschnitzer.de
mail@jakobschnitzer.de

Chat with us

PS: This email were provided by them in one of the GitHub issues and I has also contacted them via mail and they requested to access the reports without signing up
Thanks

Jamie Slome 5 months ago Admin

Sorting this for you now 👍

Jamie Slome 5 months ago Admin

I've dropped a comment on the GitHub Issue here. I do need to get authorised confirmation from the maintainers before sending any e-mails out with magic URLs.

saharshtapi 5 months ago Researcher

Understood. Appreciate it!!

We have opened a **pull request** with a `SECURITY.md` for **beancount/fava** to merge. 5 months ago

We have contacted a member of the **beancount/fava** team and are waiting to hear back 5 months ago

Jamie Slome 5 months ago Admin

E-mail sent 👍

We have sent a follow up to the **beancount/fava** team. We will try again in 7 days. 5 months ago

A **beancount/fava** maintainer has acknowledged this report 5 months ago

A **beancount/fava** maintainer modified the Severity from Critical (9.6) to High (8) 4 months ago

A **beancount/fava** maintainer modified the Severity from High to Low 4 months ago

A **beancount/fava** maintainer 4 months ago Maintainer

Since Fava URLs are dependent on the name of the underlying Beancount jo URLs, which should be private and require a previous attach to be determined by the attacker, I've marked the attack complexity as "high"

I've marked the attack complexity as "High"

A **beancount/fava** maintainer modified the Severity from Low to High (8.2) 4 months ago

A **beancount/fava** maintainer modified the Severity from High (8.2) to High (8) 4 months ago

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

A **beancount/fava** maintainer validated this vulnerability 4 months ago

saharshtapi has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

A **beancount/fava** maintainer marked this as fixed in **1.22** with commit **ca9e38** 4 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

♥ A **beancount/fava** maintainer gave praise 4 months ago

Thank you for the report :)

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

Sign in to join this conversation