Reflected XSS in fava application in beancount/fava

0

Valid Reported on Jul 22nd 2022

Description

The "query_string" parameter of fava application is vulnerable to reflected XSS for which a attacker can modify any information that the user is able to modify.

Proof of Concept

1.Open the url: `https://fava.pythonanywhere.com/example-with-budgets/query/?filter=payee%3A%22Chichipotle%22&query_string=%3Cimg+src%3D1+onerror%3Dalert%28document.location%29%3E`
2.Now XSS will popup.

Image

`https://drive.google.com/file/d/1N7XGqTg4J5rPdDzFQ4TgEtwE9v2LXDlL/view?usp=`

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 ot

References

- owasp.org
- huntr.dev

CVE
CVE-2022-2523
(Published)

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

Severity
High (8)

Registry
Pypi

Affected Version
v1.22.1

Visibility
Public

Status
Fixed

Found by

SAMPRIT DAS
@sampritdas8
pro

This report was seen 593 times.

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

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

A **beancount/fava** maintainer modified the Severity from Critical (9.6) to Hi

A beancount/fava maintainer 4 months ago Maintainer

A beancount/fava maintainer 4 months ago Maintainer

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

A **beancount/fava** maintainer has acknowledged this report 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

SAMPRIT DAS 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 **1.22.2** with commit **dccfb6** 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

SAMPRIT DAS 4 months ago Researcher

You are welcome :) @maintainer

SAMPRIT DAS 4 months ago Researcher

@admin Can you please update the CVE description in nvd/mitre

Chat with us

Jamie Slome 4 months ago Admin

Jamie Slome 4 months ago Admin

We are currently waiting for MITRE to accept our contribution here. Once they do, the CVE will go live 👍

Sign in to join this conversation