huntr

Open Redirect in star7th/showdoc

✓ Valid Reported on Nov 20th 2021

0

Description

I found a new way to exploit Open Redirect at the "**redirect**" parameter on the login page by using the Chinese dot (`%E3%80%82`) to bypass the dot (.) filter.

Vulnerable parameter

```
redirect
```

Payload

```
/%09/google%E3%80%82com
```

Proof of Concept

Send users the following login link `https://www.showdoc.com.cn/user/login?redirect=/%09/google%E3%80%82com`
After users use their registered accounts to login, they will be redirected to `google.com`

Impact

By modifying the URL value to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials.

References

- Open Redirect

CVE
CVE-2021-4000
(Published)

Vulnerability Type
CWE-601: Open Redirect

Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by

KhanhCM
@khanhchauminh
pro

Fixed by

star7th
@star7th
unranked

This report was seen 443 times.

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

This problem is very similar to that one. https://huntr.dev/bounties/ffc61eff-efea-42c5-92c2-e043fdf904d5/ Can you provide some repair suggestions under the comment? If I need to enumerate various escape situations, maybe showdoc's reward will be consumed on the same kind of problems. This will lead to no one else to help me find other types of vulnerabilities

KhanhCM a year ago Researcher

Hi @star7th,

Chat with us

Surely, I am glad to help you with the repair suggestions for this problem. Since I am not good at validation, but I think you can try this regex for validating the value of the `redirect` parameter: `![^A-Za-z0-9/:\?\._\*\+\-]+.*!` .

Moreover, after you fix this problem, I can help you to retest the problem and if it is still vulnerable, I will put a comment here for you to improve it without submit a new report.

star7th validated this vulnerability a year ago

KhanhCM has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Jamie Slome a year ago Admin

Just a reminder to mark a fix against this report, so that we can go ahead and publish the CVE! ♥

star7th a year ago Maintainer

@Chau Minh Khanh

I have released a version that fixes this problem. You can test it

KhanhCM a year ago Researcher

Hi @star7th,

In your new version, I am still able to bypass your fix by using this payload: `///google.com/`

You can check it via this PoC link: `https://www.showdoc.com.cn/user/login?redirect=///google.com/`

star7th a year ago Maintainer

OK, I fixed this problem just now. You can try again

KhanhCM a year ago Researcher

Hi @star7th,

Since you fixed the problem by filtering the dot, I can still bypass this by not using the dot with this payload: `///3627734862/`

You can check it via this PoC link: `https://www.showdoc.com.cn/user/login?redirect=///3627734862/`

star7th a year ago Maintainer

I've fixed the problem by filtering the '//'

KhanhCM a year ago Researcher

Hi @star7th,

It looks like your newest fix is good, I have tried many test cases and no longer bypass.
In the future, if I know any new bypass techniques, I will come back here and put a comment for you to fix it.

Nice to work with you. Now you can submit the fix against this report. Thank you!

star7th marked this as fixed in 2.9.13 with commit c7f100 a year ago

star7th has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation