huntr

Cross-site Scripting (XSS) - Stored in livehelperchat/livehelperchat
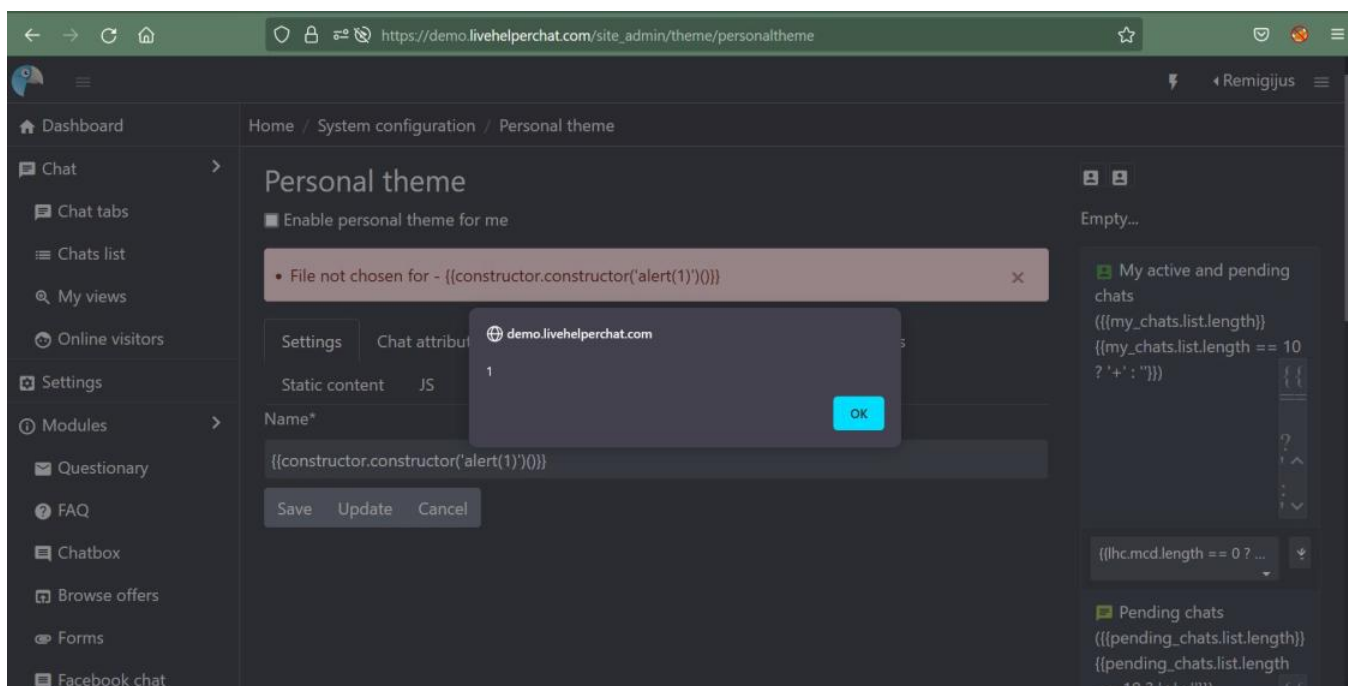
0

✔ **Valid** Reported on Jan 25th 2022

Description

Stored XSS is found in Settings>Live help configuration>Personal Theme>static content. Under the NAME field put a payload {{constructor.constructor('alert(1)')()}} while creating content, and you will see that the input gets stored, and every time the user visits, the payload gets executed.

Proof of Concept

Impact

Through this vulnerability, an attacker is capable to execute malicious scripts.

Chat with us

(Published)

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

Severity
High (7.1)

Visibility
Public

Status
Fixed

Found by

shubh123-tri
@shubh123-tri

unranked ⌄

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

We have contacted a member of the **livehelperchat** team and are waiting to hear back
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 **3.93v** with commit **9f5bc3** 10 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us