huntr

Stored Cross-site scripting in thorsten/phpmyfaq

1



Reported on Oct 20th 2022

Description

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.

Proof of Concept

Visit: http://<ip>/phpmyfaq/admin/?action=meta Click button Add template meta data Inject payload in field Page type: "><script>alert("XSS")</script> and Save Every time you go to http://<ip>/phpmyfaq/admin/?action=meta, payload XSS will execute Image POC: https://drive.google.com/file/d/1iezIdmxcCBY8G714AUFGIm3fl145yiC1/view?usp=sharing

Impact

Attacker can inject Javascript steal cookie, deface website

CVE

CVE-2022-3765 (Published)

Vulnerability Type

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

Severity

High (8.2)

Registry

Other

Affected Version

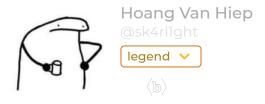
317

Visibility

Public

Chat with us

Found by



Fixed by



Thorsten Rinne
@thorsten
unranked v

This report was seen 718 times.

We are processing your report and will contact the **thorsten/phpmyfaq** team within 24 hours. a month ago

Hoang Van Hiep modified the report a month ago

We have contacted a member of the **thorsten/phpmyfaq** team and are waiting to hear back a month ago

A thorsten/phpmyfaq maintainer has acknowledged this report a month ago

♥ Thorsten Rinne gave praise a month ago

Thank you, here's the fix:

https://github.com/thorsten/phpMyFAQ/commit/372428d02a08e90b3a253ba5c506cda84581a5af

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

Hoang Van Hiep a month ago

Researcher

can we assign cve?

Chat with us

Hi @maintainer @admin if possible can we assign CVE id for this vulnerability?

Pavlos a month ago Admin

@maintainer can you please mark this report as valid, fixed and then publish it? Also at the request of the researcher, can we assign a CVE?

Thorsten Rinne validated this vulnerability a month ago

Hoang Van Hiep has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Thorsten Rinne marked this as fixed in 3.1.8 with commit 372428 a month ago

Thorsten Rinne has been awarded the fix bounty ✓

This vulnerability has been assigned a CVE 🗸

Thorsten Rinne published this vulnerability a month ago

Sign in to join this conversation

2022 © 418sed

huntr

home

part of 418sec

company

Chat with us

_ |_ _ . . .

leaderboard team

FAQ

contact us

terms