## huntr

# Reflect Cross Site Scripting when search in thorsten/phpmyfaq

1



✓ Valid ) 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**

Go to your web phpmyfaq and visit http://<ip>/phpmyfaq/index.php?search= inject payload to param search: 1af"+onclick='alert(1)' Click on field search, you will see the popup XSS (xss executed)

Image Poc Execute: https://drive.google.com/file/d/1VSAqG3MY7uyuXzl1OwrNac1q1A0iv2l/view?usp=sharing

## **Impact**

Attacker can execute javascript, steal the cookie.

### CVE

### Vulnerability Type

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

### Severity

### Registry

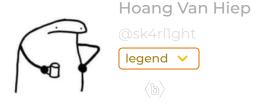
### Affected Version

Chat with us

## Status

Fixed

### Found by



Fixed by



Thorsten Rinne

unranked V

This report was seen 692 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

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 a month ago

Maintainer

I cannot reproduce this on my local machine or on the demo:

http://roy.demo.phpmyfaq.de/?search=laf%22+onload=%27alert(1)%27

Chat with us

Researcher

oh sorry, because my report, edit the payload: laf"+onload='alert(l)' --> laf"+onclick='alert(l)' Hoang Van Hiep modified the report a month ago Thorsten Rinne a month ago Maintainer I still cannot reproduce it. Which version do you use? Hoang Van Hiep a month ago Researcher i use version 3.1.7, do you click the field search after paste payload? Hoang Van Hiep a month ago Researcher you can watch this video poc: https://drive.google.com/file/d/17QaW1bBKVyvDqVEjesFBM9zvLBJbKZVI/view?usp=sharing Hoang Van Hiep a month ago Researcher (link above die) you can watch this video poc:https://drive.google.com/file/d/18HEsG7azToC1NMoRNWfvX8IMk2-Ycmld/view?usp=sharing Thorsten Rinne gave praise a month ago Okay, I can reproduce it, sorry!:-) The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1 Thorsten Rinne a month ago Maintainer Fix: https://github.com/thorsten/phpMyFAQ/commit/c7904f2236c6c0dd64c2226b90c30af0f7e5a72d

Thorsten Rinne validated this vulnerability a month ago

Chat with us

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 c7904f 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 @ 418sec

L		÷	÷	и		+	r
L	1	L	J	L	1	L	П

hama

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

## part of 418sec

company

about

team

Chat with us