Cross-Site Request Forgery (CSRF) in phoronix-test-suite/phoronix-test-suite

0

Valid Reported on Jan 9th 2022

Description

Hi there, I would like to report a Cross Site Request Forgery in phoronix source code. Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform. It allows an attacker to partly circumvent the same origin policy, which is designed to prevent different websites from interfering with each other.

Proof of Concept

Install a local instance of phoronix test suite
Create a schedule, note down the schedule id
Access this link `/?schedules/<schedule-id>/deactivate` and see that the schedule is deactivated
Access this link `/?schedules/<schedule-id>/activate` and see that the schedule is activated.
In real attack scenarios, the hacker would send the 2 above links to the victim and when they clicks it, their schedules are activated/deactivated without their consent.

Impact

This vulnerability is capable of CSRF.

Occurrences

phoromatic_schedules.php L135

References

- https://portswigger.net/web-security/csrf

CVE
CVE-2022-0197

(Published)

Vulnerability Type
CWE-352: Cross-Site Request Forgery (CSRF)

Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by

M0rphling
@ktg9
amateur

This report was seen 347 times.

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

A **phoronix-test-suite/phoronix-test-suite** maintainer validated this vulnerability 10 months ago

M0rphling has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

A **phoronix-test-suite/phoronix-test-suite** maintainer marked this as fixed in **10.8** with commit **4f1829** 10 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

phoromatic_schedules.php#L135 has been validated ✔

> Sign in to join this conversation