Cross-site Scripting (XSS) - Reflected in icecoder/icecoder

0

Valid Reported on Jan 14th 2022

Description

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into websites. An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. `https://github.com/icecoder/ICEcoder/` is vulnerable to XSS as shown below:

Proof of concept

Vuln variable: `$_POST['username']`
Snippet:

```
if ($ICEcoder["multiUser"]) {
    $_SESSION['username'] = $_POST['username'];
}
```

Payload

Login as an admin and enable multiuser and registration. Now register a new user with the following username:

```
admon<img src="x" onerror=alert`XSS`>
```

Set any password , for example:

```
P@55worD123.
```

Clic login observe the XSS....

Impact

Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

References

https://portswigger.net/web-security/cross-site-scripting https://owasp.org/www-community/attacks/xss/

References

- https://owasp.org/www-community/attacks/xss/
- https://portswigger.net/web-security/cross-site-scripting

CVE
CVE-2021-3862
(Published)

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

Severity
Medium (5.4)

Visibility
Public

Status
Fixed

Found by

hitisec
@hitisec
pro

This report was seen 401 times.

We are processing your report and will contact the **icecoder** team within 24 hours. a year ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` a year ago

We have opened a **pull request** with a `SECURITY.md` for **icecoder** to merge. a year ago

We have contacted a member of the **icecoder** team and are waiting to hear back a year ago

A **icecoder/icecoder** maintainer validated this vulnerability a year ago

hitisec has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

A **icecoder/icecoder** maintainer marked this as fixed in **8.1** with commit **51cf24** a year ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

A **icecoder/icecoder** maintainer a year ago — Maintainer

Many thanks for the excellent report here, it allowed me to find & resolve the issue quickly.

I can confirm the input field "username" under multi-user mode indeed had an rXSS vuln (reflection within the editor.php file - within data seen after login).

While every security issue should be looked into and resolved, thankfully it's only exploitable if a user were to set the editor to multi-user mode and leave open so anyone could register. (In that case someone could register under a standard name and create new files using ICEcoder, for example - xss.js, rce.php, sqli.sql etc etc. So thankfully not exploitable unless someone had really bad "open to all" security practices in the first place).

Even so... it's technically a vulnerable point, needed patching and has been patched quickly. As ICEcoder follows the practice of "clean on output, not input" - the reflection on editor.php L153 is where I've fixed things, rather than input point settings.php L238.

Thanks again - it's fantastic researchers like yourself that make the web more secure. Kudos!

hitisec a year ago — Researcher

Thanks!

Sign in to join this conversation