Session Fixation in rCTF <2.3

Low **Arinerron** published **GHSA-p5fh-2vhw-fvpq** on Mar 30, 2020

Package

rctf (yarn)

Affected versions	Patched versions
<2.3	2.3

Description

Description

There is a session fixation vulnerability in rCTF exploitable through the `#token=$ssid` hash when making a request to the `/verify` endpoint.

Vulnerable code

```
document.title = 'Verify' + config.ctfTitle

   const prefix = '#token='
   if (document.location.hash.startsWith(prefix)) {
     route('/verify', true)

     const verifyToken = document.location.hash.substring(prefix.length)

     verify({ verifyToken })
       .then(errors => {
         this.setState({
           errors
         })
       })
   }
```

Exploitation Scenario

An attacker team could potentially steal flags by, for example, exploiting a stored XSS payload in a CTF challenge so that victim teams who solve the challenge are unknowingly (and against their will) signed into the attacker team's account. Then, the attacker can gain points / value off the backs of the victims.

Reproduction Steps

1. Create two teams: an attacker, and a victim. Sign into the victim's account.
2. Make an HTTP request to `/verify#hash=$ssid` where `$ssid` is the attacker's team code.
3. Observe that you have been logged in as the attacker.

Extra Details

Commit that introduced the vulnerability

`1f91230` #diff-95a87eb07806dffb6d81c2ffdd27f8f5R16-R32

Potential solution

Instead of having the verification email link immediately sign users in, have it be purely for confirmation purposes. After opening the verification link and verifying the email address, the original registration page--which is polling the server for updates--would receive word that the email is verified. It would then log in without requiring a session ID from user input.

Issue

A copy of this report is in issue #147.

Severity

Low

CVE ID

CVE-2020-5290

Weaknesses

No CWEs