New issue

Jump to bottom

Session fixation vulnerability in /verify #147

Closed **Arinerron** opened this issue on Mar 29, 2020 · 0 comments · Fixed by #156

Assignees

Labels bug

Projects Backend Frontend

Milestone Initial Release

Arinerron commented on Mar 29, 2020 • edited Member

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.

Arinerron added the bug label on Mar 29, 2020

Arinerron added this to the **Initial Release** milestone on Mar 29, 2020

Arinerron assigned **ethanwu10** on Mar 29, 2020

Arinerron added this to **To do** in **Backend** via automation on Mar 29, 2020

Arinerron assigned **chen-robert** and **ginkoid** on Mar 29, 2020

Arinerron added this to **to-do** in **Frontend** via automation on Mar 29, 2020

chen-robert mentioned this issue on Mar 30, 2020

Remove session fixiation vulnerability #156

Merged

chen-robert closed this as completed in #156 on Apr 1, 2020

ethanwu10 moved this from **To do** to **Done** in **Backend** on Apr 15, 2020

chen-robert moved this from **to-do** to **done** in **Frontend** on Apr 23, 2020

Assignees

ethanwu10

chen-robert

ginkoid

Labels

bug

Projects

Backend

Done

Frontend

done

Milestone

Initial Release

Development

Successfully merging a pull request may close this issue.

Remove session fixiation vulnerability
redpwn/rctf

4 participants