New issue

Jump to bottom

Session Fixation #605

Closed **PreethamBomma** opened this issue on Mar 20, 2020 · 1 comment

Milestone 1.4.3

PreethamBomma commented on Mar 20, 2020

PlaySMS is vulnerable to Session fixation (all versions, including the latest). Due to the lack of randomization of the sessionID and reuse of sessionID (prior login, after login). An attacker can set the user's session and can take control of the user's account.

Steps to reproduce:

1. Login to PlaySMS (Note down the value of cookie [PHPSESSID]).
2. Logout.
3. You can confirm the same session by checking prior login and after logging in.
4. You can observe that the value of PHPSESSID will be the same as in Step 1

antonraharja commented on Mar 20, 2020 Member

Please send email to my email araharja@protonmail.com for security related, thank you. Will open this issue again as soon as theres more feedback and solution.

antonraharja closed this as completed on Mar 20, 2020

antonraharja added the require feedback label on Mar 20, 2020

antonraharja added this to the **1.4.3** milestone on Mar 20, 2020

antonraharja reopened this on Apr 1, 2020

antonraharja added a commit that referenced this issue on Apr 1, 2020

`fix session fixation #605` b099f63

antonraharja removed the require feedback label on Apr 1, 2020

antonraharja added a commit that referenced this issue on Apr 3, 2020

`Merge pull request #606 from antonraharja/session_fixation_fix` ... 0c00f54

antonraharja closed this as completed on May 1, 2020

Assignees

No one assigned

Labels

None yet

Milestone

1.4.3

Development

No branches or pull requests

2 participants