New issue

Jump to bottom

Username and password recheck bypassed #658

Open **peng-hui** opened this issue on May 26, 2020 · 0 comments

peng-hui commented on May 26, 2020

Hi,

I just find that, in many places of oscommerce v2.3.4.1, the username and password recheck during registration and other processes can be bypassed easily through the `magic string` in loose comparison, for example `"0e11111" == "0e22222"` returns `Bool(True)`. If the user sets the username or password to such magic strings, the recheck process using loose comparison (==) does not work at all.
Affected code locations

- /catalog/admin/administrators.php:66
- /catalog/admin/administrators.php#L109
- /catalog/admin/administrators.php#L132
- /catalog/admin/administrators.php#L148

and some other files in `catalog/password_reset.php`, `catalog/create_account.php` and `catalog/ext/modules/content/account/set_password.php`

ruden added a commit to ruden/vanilla-oscommerce that referenced this issue on Aug 29, 2020

`strict verification osCommerce#658` b258880

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant