



ThinkPHP log information leak vulnerability exists

Backlog #13YNWY xrun Opened this issue 2021-07-01 14:02

Hello, after testing, I found that tpcms v3.2 has a vulnerability -- The CMS code does not restrict the visitor's access to ThinkPHP logs through the URL. Such logs contain the administrator's user name, password, etc. Sensitive information brings greater security risks to the system.

URL:

[http://domain\(or IP\)/Data/Runtime/Logs/Admin/21_07_01.log](http://domain(or IP)/Data/Runtime/Logs/Admin/21_07_01.log)

[http://domain\(or IP\)/Data/Runtime/Logs/Home/21_07_01.log](http://domain(or IP)/Data/Runtime/Logs/Home/21_07_01.log)

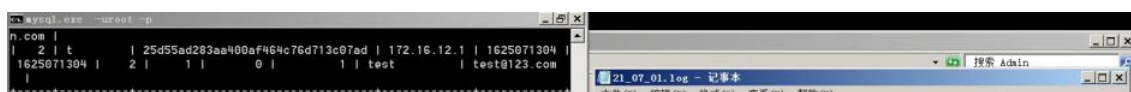
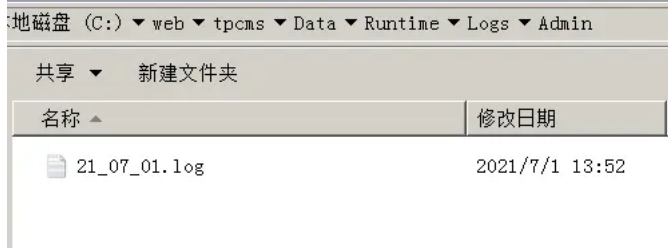
[http://domain\(or IP\)/Data/Runtime/Logs/Member/21_07_01.log](http://domain(or IP)/Data/Runtime/Logs/Member/21_07_01.log)

reference:

```
172.16.12.106/Data/Runtime/Lo X +
172.16.12.106/Data/Runtime/Logs/Admin/21_07_01.log
INFO: [ view_parse ] --END-- [ RunTime:0.000000s ]
INFO: [ view_filter ] --START--
INFO: Run Behavior\WriteHtmlCacheBehavior [ RunTime:0.000000s ]
INFO: [ view_filter ] --END-- [ RunTime:0.000000s ]
INFO: [ app_end ] --START--
INFO: Run Behavior\ShowPageTraceBehavior [ RunTime:0.000000s ]
INFO: [ app_end ] --END-- [ RunTime:0.000000s ]

[ 2021-07-01T01:23:30+08:00 ] 172.16.12.1 /index.php/Admin/User/change.html
INFO: [ app_init ] --START--
INFO: Run Behavior\BuildLiteBehavior [ RunTime:0.000000s ]
INFO: Run Common\Behavior\InitHookBehavior [ RunTime:0.000000s ]
INFO: [ app_init ] --END-- [ RunTime:0.000000s ]
INFO: [ app_begin ] --START--
INFO: Run Behavior\ReadHtmlCacheBehavior [ RunTime:0.000000s ]
INFO: [ app_begin ] --END-- [ RunTime:0.000000s ]
SQL: SHOW COLUMNS FROM `tpcms_user` [ RunTime:0.0000s ]
SQL: SELECT * FROM `tpcms_user` WHERE `username` = 'admin' LIMIT 1 [ RunTime:0.0000s ]
SQL: SELECT * FROM `tpcms_user` WHERE `uid` = 1 LIMIT 1 [ RunTime:0.0000s ]
SQL: UPDATE `tpcms_user` SET `password`='25d55ad283aa400af464c76d713c07ad' WHERE `uid` = 1 [ RunTime:0.0156s ]
NOTIC: [8] Undefined index: role C:\web\tpcms\Core\Frame\Common\Model\UserModel.class.php 405 0;E.

[ 2021-07-01T01:23:32+08:00 ] 172.16.12.1 /index.php/Admin/User/change.html
INFO: [ app_init ] --START--
INFO: Run Behavior\BuildLiteBehavior [ RunTime:0.000000s ]
INFO: Run Common\Behavior\InitHookBehavior [ RunTime:0.000000s ]
INFO: [ app_init ] --END-- [ RunTime:0.000000s ]
INFO: [ app_begin ] --START--
INFO: Run Behavior\ReadHtmlCacheBehavior [ RunTime:0.000000s ]
INFO: [ app_begin ] --END-- [ RunTime:0.000000s ]
SQL: SHOW COLUMNS FROM `tpcms_user` [ RunTime:0.0000s ]
SQL: SELECT * FROM `tpcms_user` WHERE `username` = 'admin' LIMIT 1 [ RunTime:0.0000s ]
INFO: [ view_parse ] --START--
NOTIC: [8] Undefined variable: php C:\web\tpcms\Core\ThinkPHP\Library\Think\Template\TagLib\Hd.class.php 300 0;E.
INFO: [ template_filter ] --START--
INFO: Run Behavior\ContentReplaceBehavior [ RunTime:0.000000s ]
INFO: [ template_filter ] --END-- [ RunTime:0.000000s ]
NOTIC: [8] Undefined variable: data C:\web\tpcms\Data\Runtime\Cache\Admin\8826f35f728fec4c310603fafb1388e.php 43 0;E.
NOTIC: [8] Undefined variable: data C:\web\tpcms\Data\Runtime\Cache\Admin\8826f35f728fec4c310603fafb1388e.php 48 0;E.
NOTIC: [8] Undefined variable: data C:\web\tpcms\Data\Runtime\Cache\Admin\8826f35f728fec4c310603fafb1388e.php 52 0;E.
INFO: Run Behavior\PageTemplateBehavior [ RunTime:0.000000s ]
```



Don't show this again

Status

Backlog

Assignees

Not set

Labels

Not set

Milestones

No related milestones

Pull Requests

None yet

Successfully merging a pull request issue.

Branches

No related branch

Planned to start - Planned to end

Unscheduled - Unschedule

Top level

Not Top

Priority

Not specified

参与者 (1)



[View Details](#)

```

INFO: [ view_filter ] --START--
INFO: Run Behavior\WriteHtmlCacheBehavior [ Runtime:0.000000s ]
INFO: [ view_filter ] --END-- [ Runtime:0.000000s ]
INFO: [ app_end ] --START--
INFO: Run Behavior\ShowPageTraceBehavior [ Runtime:0.000000s ]
INFO: [ app_end ] --END-- [ Runtime:0.000000s ]

[ 2021-07-0109:41:44+08:00 ] 172.16.12.1 /index.php/Member/Reg/index.html
INFO: [ app_init ] --START--
INFO: Run Behavior\BuildLiteBehavior [ Runtime:0.000000s ]
INFO: Run Common\Behavior\InitHookBehavior [ Runtime:0.000000s ]
INFO: [ app_init ] --END-- [ Runtime:0.000000s ]
INFO: [ app_begin ] --START--
INFO: Run Behavior\ReadHtmlCacheBehavior [ Runtime:0.000000s ]
INFO: [ app_begin ] --END-- [ Runtime:0.000000s ]
SQL: SHOW COLUMNS FROM `tpcms_user` [ Runtime:0.0000s ]
SQL: SELECT 'uid' FROM `tpcms_user` WHERE 'username' = '16250123.com' LIMIT 1 [ Runtime:0.0000s ]
SQL: SELECT 'uid' FROM `tpcms_user` WHERE 'email' = '16250123.com' LIMIT 1 [ Runtime:0.0000s ]
NOTICE: [2] Missing argument 1 for Member\Logic\UserLogic::__construct() C:\web\tpcms\Core\Tpcms\Member\Logic\UserLogic.class.php ↵ 54 &#x
NOTICE: [3] Undefined variable: C:\web\tpcms\Core\Tpcms\Member\Logic\UserLogic.class.php ↵ 56 &#x
SQL: INSERT INTO `tpcms_user` ('username','email','password','addtime','role','times','login_time','login_ip','nickname') VALUES
('1625', '16250123.com', 'e10ad33949ba59abbe56e057f20f883e', '1625071304', '2', '1', '1625071304', '172.16.12.1', '1625') [ Runtime:0.0000s ]
INFO: [ view_parse ] --START--
NOTICE: [8] Undefined variable: php C:\web\tpcms\Core\ThinkPHP\Library\Think\Template\TagLib\Rd.class.php ↵ 300 &#x
INFO: [ template_filter ] --START--
INFO: Run Behavior\ContentReplaceBehavior [ Runtime:0.000000s ]
INFO: [ template_filter ] --END-- [ Runtime:0.000000s ]
INFO: Run Behavior\ParseTemplateBehavior [ Runtime:0.015600s ]
INFO: [ view_parse ] --END-- [ Runtime:0.015600s ]
INFO: [ view_filter ] --START--
INFO: Run Behavior\WriteHtmlCacheBehavior [ Runtime:0.000000s ]
INFO: [ view_filter ] --END-- [ Runtime:0.000000s ]
INFO: [ app_end ] --START--
INFO: Run Behavior\ShowPageTraceBehavior [ Runtime:0.000000s ]
INFO: [ app_end ] --END-- [ Runtime:0.000000s ]

```



©OSCHINA. All rights reserved

[Git Resources](#)

[Learning Git](#)

[CopyCat](#)

[Downloads](#)

[Gitee Reward](#)

[Gitee Stars](#)

[Featured Projects](#)

[Blog](#)

[Nonprofit](#)

[Gitee Go](#)

[OpenAPI](#)

[Help Center](#)

[Self-services](#)

[Updates](#)



Gitee 已支持 CLA 协议签署

- 🔥 第一方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 👤 让开源贡献也能有据可依

[I know](#)

[View Details](#)

777320883

git@oschina.cn

Gitee

+86 400-606-0201



Mini Program

[OpenAtom Foundation](#) [Cooperative code hosting platform](#)



违

号

[简体](#)

