

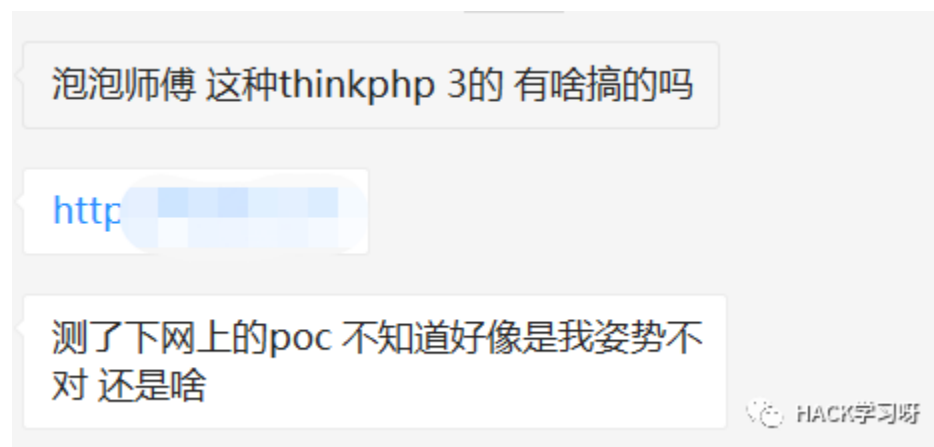
记一次渗透某XX站

原创 r00tuser HACK学习呀

2019-10-20原文

0X00 前言

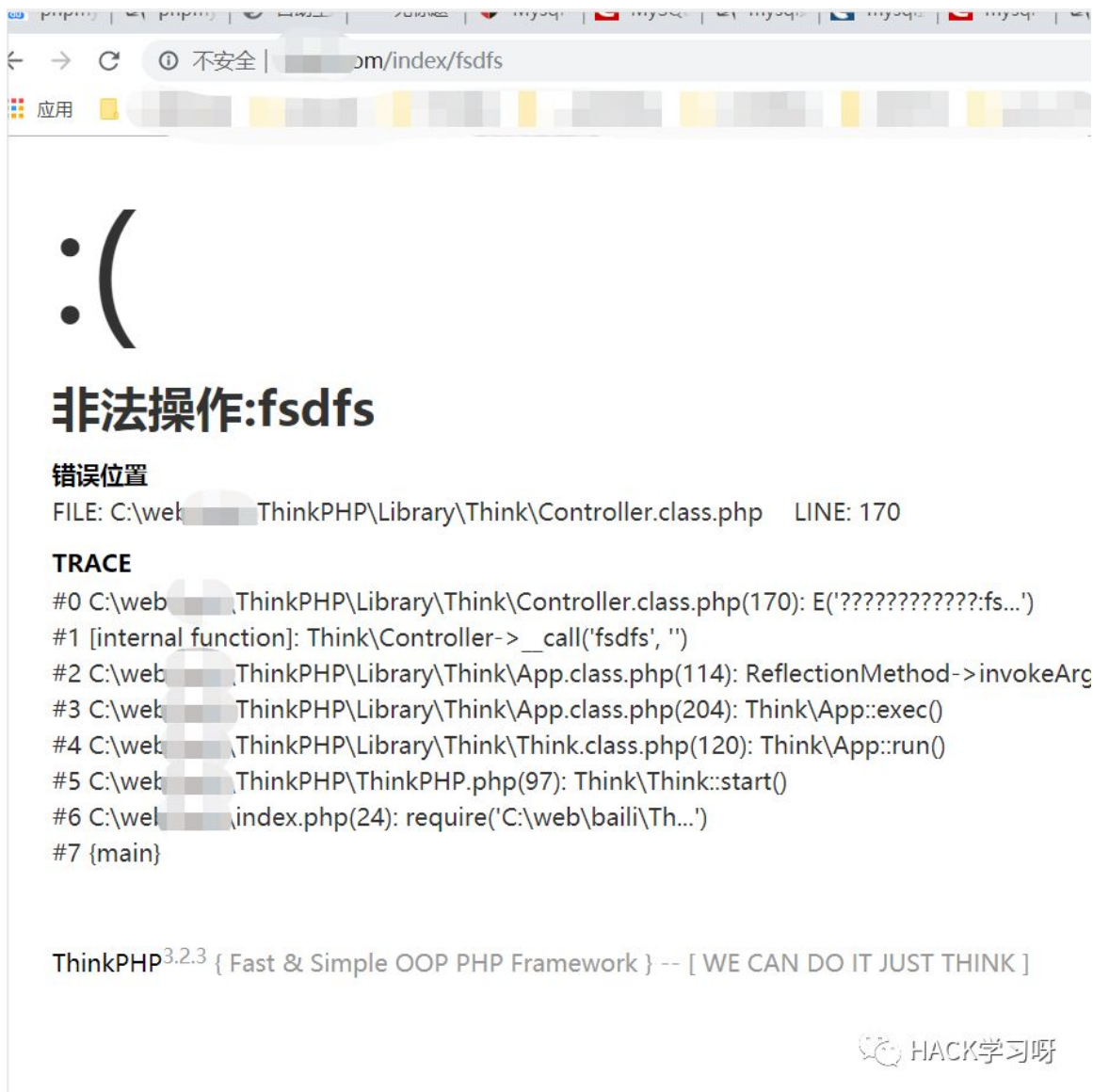
团队A师傅发来个站，问我有没有得搞



正好在搞其他的站，卡住了，开干换个思路。

0x01 信息收集

开burp抓了下包，目标设置了url重写，开了报错，我们随意输入一个控制器就直接报错。



获取到web绝对路径。

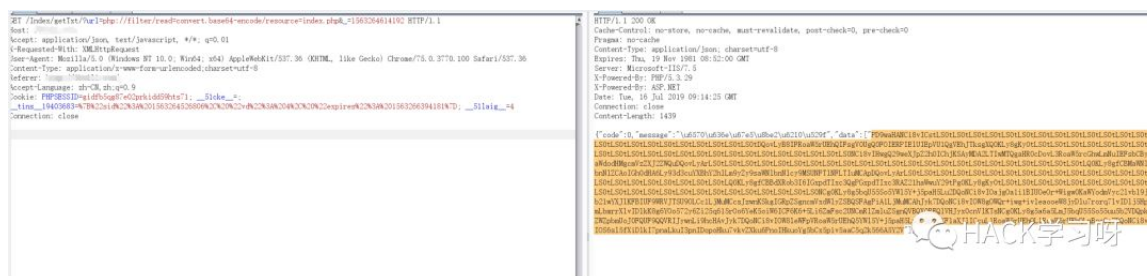
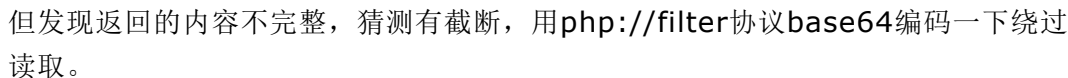
抓包发现这样的请求

```
GET /Index/getTxt?url=http://1563265097512 HTTP/1.1
Host: 1563265097512
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Referer: http://1563265097512/
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=gldfb5qg87e02prkidd59hts71; __51cke__=; pma_lang=zh_CN; pma_encrypt_iv=dTP1C4tb1WI%3D; pmaUser-1=a2IaJzHtwT8%3D; phpMyAdmin=zh5egqc31mm112ajkt9bgsInvgkoc; __tins__19403683=%7B%22sid%22%3A%201563264526806%2C%20%22vd%22%3A%206%2C%20%22expires%22%3A%201563266857501%7D; __51laig__=6
Connection: close
```

随手试了一下burpsuite的dnslog，发现请求过去并回显了，猜测后端使用file_get_contents来获取。

一个可回显ssrf，有什么用呢？

尝试file协议，尝试读取文件，发现可以读。



解码



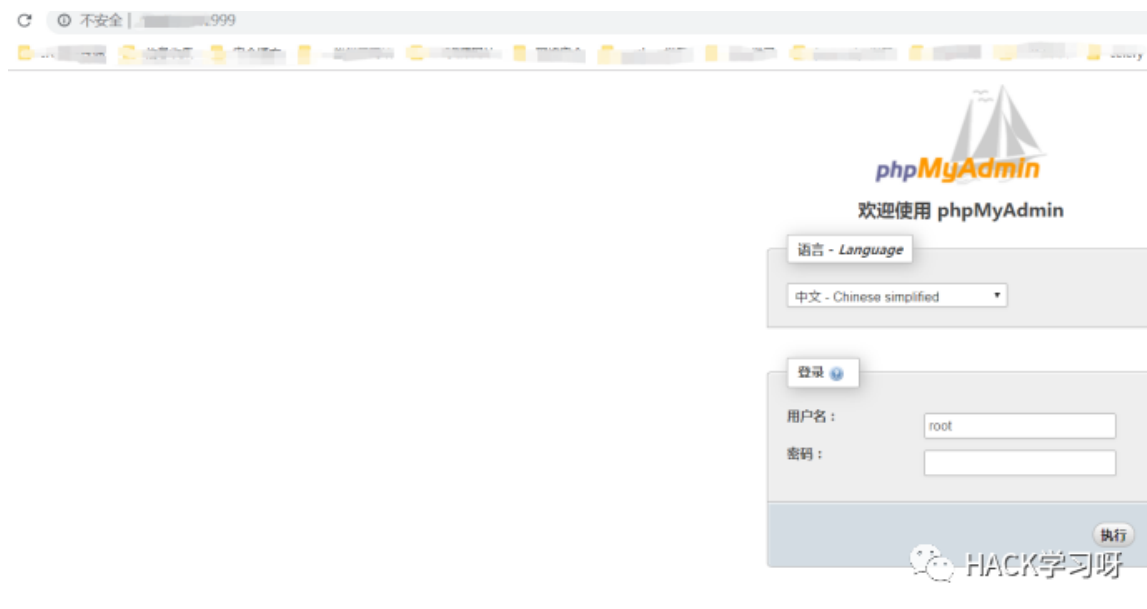
有一个任意文件读取有什么用呢？

在这之前，其实是有用nmap扫了一下其他端口

```
Starting Nmap 6.40 ( http://nmap.org ) at 2019-07-16 16:15 CST
Nmap scan report for 192.168.1.100
Host is up (0.011s latency).
Not shown: 984 closed ports
PORT      STATE      SERVICE
21/tcp    open      ftp
80/tcp    open      http
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
443/tcp   open      https
445/tcp   filtered  microsoft-ds
999/tcp   open      garcon
1010/tcp  open      surf
1723/tcp  filtered  pptp
3306/tcp  open      mysql
49152/tcp open      unknown
49153/tcp open      unknown
49154/tcp open      unknown
49155/tcp open      unknown
49156/tcp open      unknown
49158/tcp open      unknown

Nmap done: 1 IP address (1 host up) scanned in 9.08 seconds
```

开了挺多端口的，一个个测了一下发现999端口开着phpmyadmin。



结合任意文件读取，那么只要我们读取出mysql的账号密码即可进入phpmyadmin，之后的getshell方法就很多了。

thinkphp的目录结构根据官方文档一般都长这样。

接下来再看原来空的 `Application` 目录下面，已经自动生成了公共模

1.		<code>Application</code>	
2.		<code>Common</code>	应用公共模块
3.		<code>Common</code>	应用公共函数目录
4.		<code>Conf</code>	应用公共配置文件目录
5.		<code>Home</code>	默认生成的Home模块
6.		<code>Conf</code>	模块配置文件目录
7.		<code>Common</code>	模块函数公共目录
8.		<code>Controller</code>	模块控制器目录
9.		<code>Model</code>	模块模型目录
10.		<code>View</code>	模块视图文件目录
11.		<code>Runtime</code>	运行时目录
12.		<code>Cache</code>	模版缓存目录
13.		<code>Data</code>	数据目录
14.		<code>Logs</code>	日志目录
15.		<code>Temp</code>	缓存目录

HACK学习呀

而数据库文件一般是放在`common/conf`下面的。

简单猜了会，尝试读取`index`控制器。

之前的报错其实已经放出了`index`控制器在那个模块下面了，就是默认的`home`模块

。



非法操作:fsdfs

错误位置

FILE: C:\web\ThinkPHP\Library\Think\Controller.class.php LINE: 170

TRACE

```
#0 C:\web\ThinkPHP\Library\Think\Controller.class.php(170): E('?????????fs...')
#1 [internal function]: Think\Controller->_call('fsdfs', '')
#2 C:\web\ThinkPHP\Library\Think\App.class.php(114): ReflectionMethod->invokeArgs(Object(Home\Controller\IndexController), Array)
#3 C:\web\ThinkPHP\Library\Think\App.class.php(204): Think\App::exec()
#4 C:\web\ThinkPHP\Library\Think\Think.class.php(120): Think\App::run()
#5 C:\web\ThinkPHP\ThinkPHP.php(97): Think\Think::start()
#6 C:\web\index.php(24): require('C:\web\bail\Th...')
#7 (main)
```

ThinkPHP 3.2.3 { Fast & Simple OOP PHP Framework } -- [WE CAN DO IT JUST THINK]

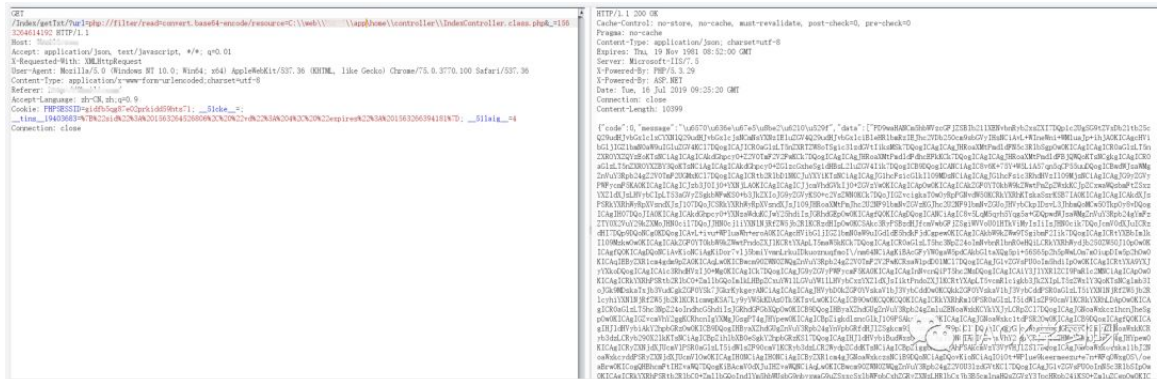


读取

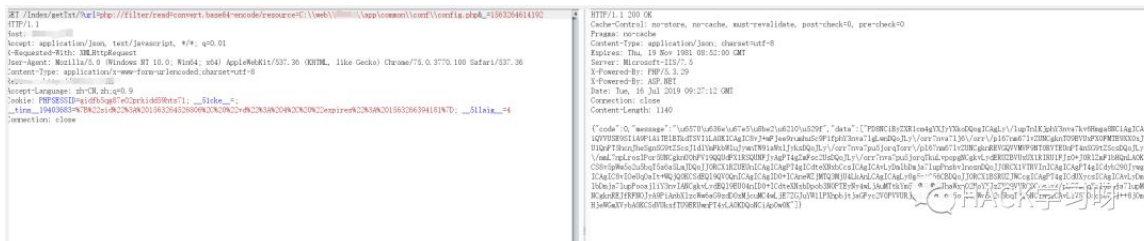


没有返回, 猜测是application目录改名了, 结合之前的审计经验, 一般会改为app

再读取, 成功。



一般会存放在common模块下面的config.php或者db.php，尝试了一下config.php，命中。

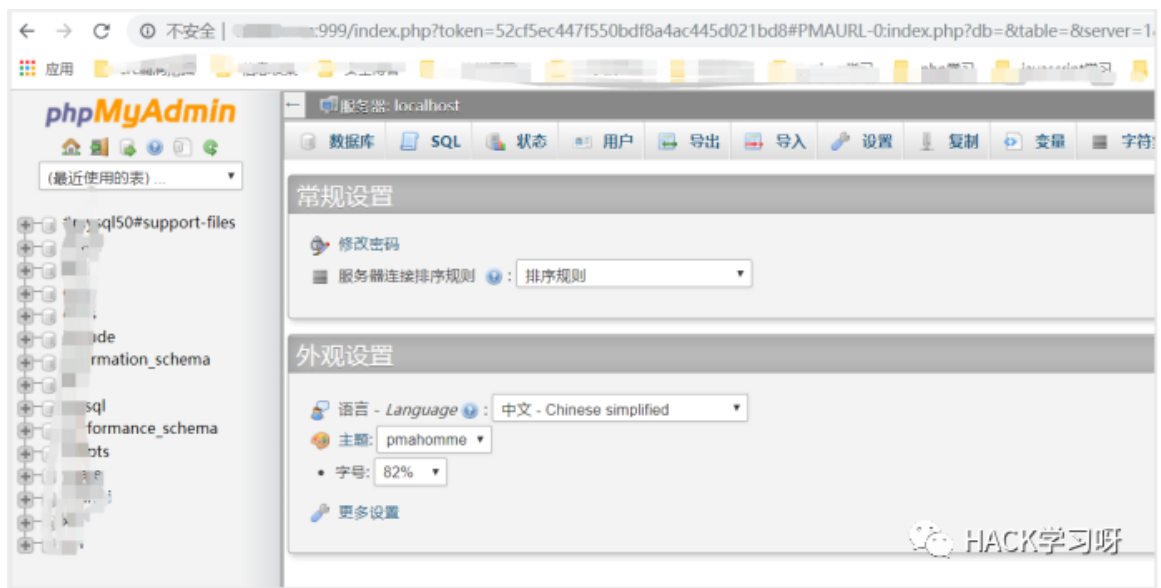


```
<?
return array(
    //应用配置信息
    "AUTHOR" => "LIANGSIR",
    //'配置项'=>'配置值'
    //设置可访问目录
    'MODULE_ALLOW_LIST'=>array('Home','Webadmin','Mobile'),
    //设置默认访问目录
    'DEFAULT_MODULE'=>'Home',
    //显示调试
    'SHOW_PAGE_TRACE' => false,
    //设置默认主题
    //'DEFAULT_THEME'=>'Default',
    //数据库定义
    'DB_TYPE'          => 'mysql',          // 数据库类型'
    'DB_USER'          => 'root',           // 用户名
    'DB_PWD'           => '1234567890.0',    // 密码
    'DB_PREFIX'        => 'T_',             // 数据库表前缀
    //'DB_DSN' => 'mysql:host=127.0.0.1;[redacted] charset=UTF8',//链接数据库
    'DB_DSN' => 'mysql:host=127.0.0.1;dbname=[redacted] set=UTF8',//链接数据库

    //URL模式，重写url
    'URL_MODEL'=>2,

);
```

输入账号密码，回车，登陆成功。



后面拿shell就给A师傅去弄了。

0x02 URL Rewrite的一些疑惑

题外话：因为之前帮朋友搞了一些站也是这样的，有文件上传直接拿shell，但是没有办法访问，访问提示：



无法加载控制器:Uploads/2019-97-16/test

错误位置

FILE: D:\...Core\Library\Think\App.class.php LINE: 101

TRACE

```
#0 D:\...Core\Library\Think\App.class.php(101): E('\xE6\x97\xA0\xE6\xB3\x9!')
#1 D:\...Core\Library\Think\App.class.php(204): Think\App::exec()
#2 D:\...Core\Library\Think\Think.class.php(120): Think\App::run()
#3 D:\...Core\core.php(97): Think\Think::start()
#4 D:\...start.php(30): require('D:\...')
#5 {main}
```



有拿到源码，.htaccess里面有对url重写，比如长这样的。

```
<IfModule mod_rewrite.c>

DirectoryIndex start.php index.php
RewriteEngine on
RewriteCond %{REQUEST_FILENAME} !-d
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule ^(.*)$ start.php?s=/$1 [QSA,PT,L]
</IfModule>
```



之前上传没法访问一直以为是重写的问题。

但其实也可能不是，有可能是马儿被杀了缘故，当文件不存在的时候才会提示这样。

在本地测试，拉了个thinkphp 3.2.3的项目，htaccess一样配置。

```
<IfModule mod_rewrite.c>
    Options +FollowSymlinks
    RewriteEngine On

    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteRule ^(.*)$ index.php/$1 [QSA,PT,L]
</IfModule>
```

 HACK学习呀

在根目录下写入个test.php，内容为phpinfo。可以直接访问。

删掉test.php, 报错



无法加载模块:Test

错误位置

FILE: F:\Downloads\thinkphp-3.2.5\thinkphp-3.2.5\ThinkPHP\Library\Think\Dispatcher.class.php

TRACE

```
#0 F:\Downloads\thinkphp-3.2.5\thinkphp-3.2.5\ThinkPHP\Library\Think\Dispatcher.class.php(1:
#1 F:\Downloads\thinkphp-3.2.5\thinkphp-3.2.5\ThinkPHP\Library\Think\App.class.php(39): Thir
#2 F:\Downloads\thinkphp-3.2.5\thinkphp-3.2.5\ThinkPHP\Library\Think\App.class.php(204): Th
#3 F:\Downloads\thinkphp-3.2.5\thinkphp-3.2.5\ThinkPHP\Library\Think\Think.class.php(136): T
#4 F:\Downloads\thinkphp-3.2.5\thinkphp-3.2.5\ThinkPHP\ThinkPHP.php(100): Think\Think::star
#5 F:\Downloads\thinkphp-3.2.5\thinkphp-3.2.5\index.php(26): require('F:\\Downloads\\th...')
#6 {main}
```

ThinkPHP^{3.2.5} { Fast & Simple OOP PHP Framework } -- [WE CAN DO IT JUST THINK!]  HACK学习呀

换到二级目录下继续测试:



PHP Version 5.4.45

System	Windows NT KXING 6.2 build 9200 (Windows 8 Enterprise Edition) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--with-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pdo-web" "pdo-oci=C:\php-sdk\oracle\instantclient10\sdk\shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk\shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk\shared" "--enable-object-out-dir=../obj/" "--com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--w
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows

不存在文件的时候同样提示:



无法加载模块:Public

错误位置

FILE: F:\Downloads\thinkphp-3.2.5\thinkphp-3.2.5\ThinkPHP\Library\Think\Dispatcher.class.php

TRACE

```
#0 F:\Downloads\thinkphp-3.2.5\thinkphp-3.2.5\ThinkPHP\Library\Think\Dispatcher.class.php(192)
#1 F:\Downloads\thinkphp-3.2.5\thinkphp-3.2.5\ThinkPHP\Library\Think\App.class.php(39): Think
#2 F:\Downloads\thinkphp-3.2.5\thinkphp-3.2.5\ThinkPHP\Library\Think\App.class.php(204): Thin
#3 F:\Downloads\thinkphp-3.2.5\thinkphp-3.2.5\ThinkPHP\Library\Think\Think.class.php(136): Thi
#4 F:\Downloads\thinkphp-3.2.5\thinkphp-3.2.5\ThinkPHP\ThinkPHP.php(100): Think\Think::start(
#5 F:\Downloads\thinkphp-3.2.5\thinkphp-3.2.5\index.php(26): require('F:\Downloads\th...')
#6 {main}
```

ThinkPHP^{3.2.5} (Fast & Simple OOP PHP Framework) -- [WE CAN DO IT JUST THINK]

 HACK学习呀

后面深入研究了一下那份源码发现也不是马儿被杀了的原因，应该由于它的分割符问题。

不是传统的/，而是点号，传统的文件路径访问与路由冲突了，最终也就没办法访问到uploads目录下的shell。

没想出对于这种路由有啥办法可以解决的，如果有知道的师傅欢迎评论交流。

更新：那个有问题的站也拿下了，原因确实是没有文件导致的，至于为什么没有写入成功又是另外一回事了。

更新2：感谢love17师傅的评论，关于htaccess的理解之前确实不对，删掉了，不误人子弟。

0x03 拿shell

由于上面的疑惑，生成了我错误的认知，导致我以为拿shell会比较麻烦，我的思路是phpmyadmin

日志方式导出一个符合thinkphp路由的shell到相应的控制器下，以绕过路由的检测。

但A师傅说直接into outfile

到images目录就可以了，那就是mysql版本不高也没有secure_file_priv的问题，直接导出shell了。

搞定了

into outfile都是开的

直接一条语句就shell了 😂

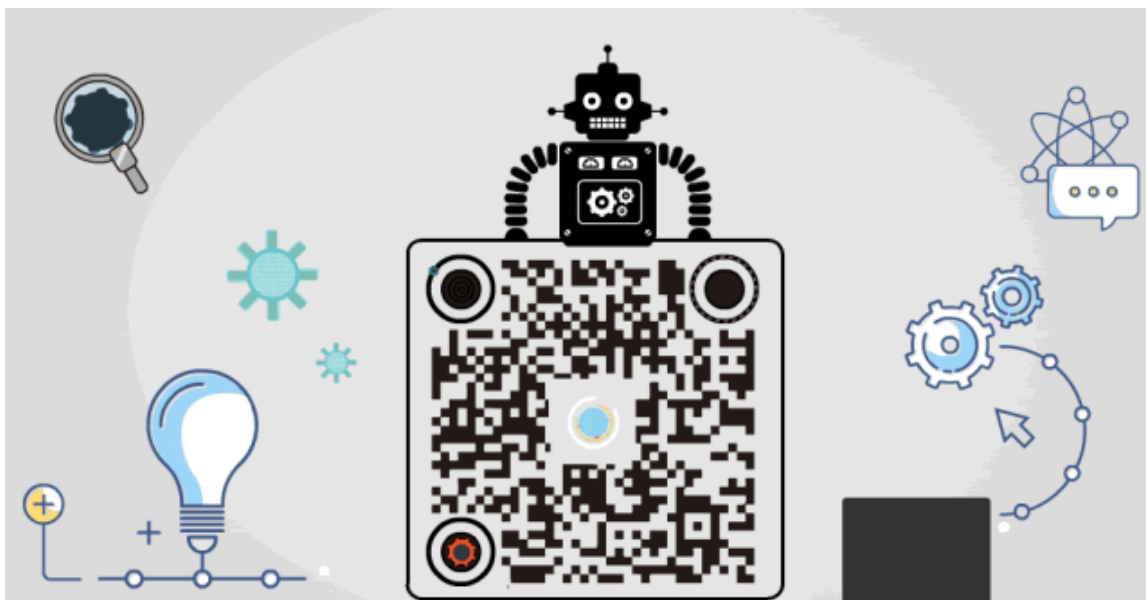
HACK学习呀

我：emmmmm

END

原创投稿作者：r00tuser

博客地址：<https://www.cnblogs.com/r00tuser/p/11197671.html>



精选留言

用户设置不下载评论