登录

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）

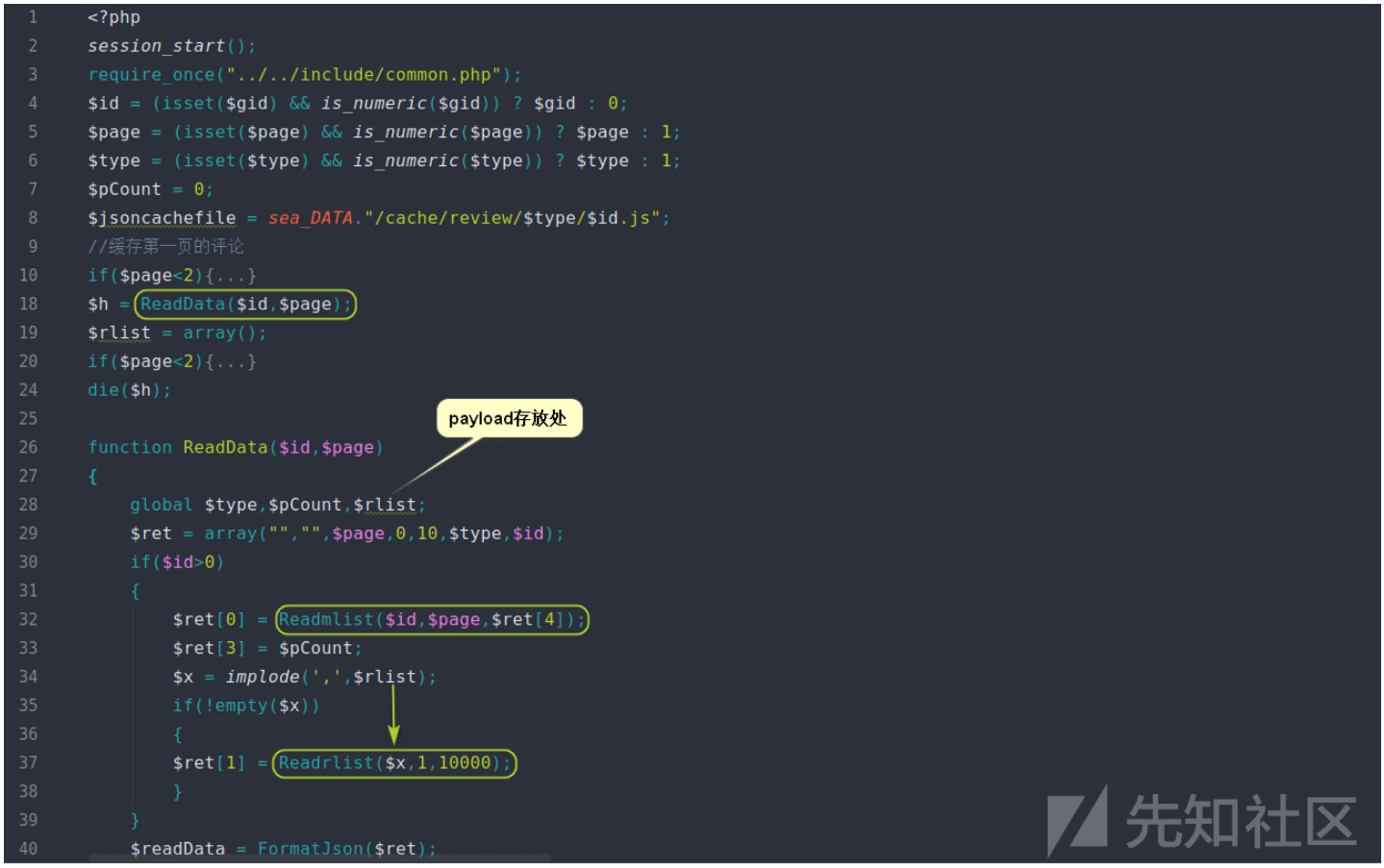
```php
<?php
if(!defined('sea_INC')){...}

$magic_quotes_gpc = ini_get('magic_quotes_gpc');  $magic_quotes_gpc: false
function _FilterAll($fk, &$svar){...}

/* 对 GET, POST, COOKIE进行过滤 */
foreach(Array('_GET','_POST','_COOKIE') as $_request)  $_request: "_GET"
{
    foreach($$_request as $_k => $_v)
    {
        ${$_k} = _FilterAll($_k,$_v);
    }
}

function _Replace_Badword(&$var){...}
/*...*/?>
```

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）

```php
<?php
error_reporting(0);
require_once('webscan/webscan.php');
define('sea_INC', preg_replace("|[/\\\]{1,}|",'/',dirname(__FILE__) ) );
define('sea_ROOT', preg_replace("|[/\\\]{1,}|",'/',substr(sea_INC,0,-8) ) );
define('sea_DATA', sea_ROOT.'/data');
require_once(sea_INC.'/inc/mysql.php' );
require_once(sea_INC."/filter.inc.php");
if(PHP_VERSION < '4.1.0') {...}
$starttime = microtime();
require_once(sea_INC.'/common.func.php');
//检查和注册外部提交的变量
foreach($_REQUEST as $_k=>$_v)  $_k: "kd35xb_admin_username"  $_v: "admin"
{
    if( strlen($_k)>0 && m_eregi('^(cfg_|GLOBALS|_GET|_POST|_COOKIE|_REQUEST|_SERVER)',$_k) && !isset($_COOKIE[$_k]) )
    {
        exit('Request var not allow!');
    }
}
```


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）



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 ）

```php
function Readmlist($id,$page,$size)
{
    global $dsql,$type,$pCount,$rlist;
    $rlist = str_ireplace('@', "", $rlist);
    $rlist = str_ireplace('/*', "", $rlist);
    $rlist = str_ireplace('*/', "", $rlist);
    $rlist = str_ireplace('*!', "", $rlist);
    $rlist = str_ireplace('%00', "", $rlist);
    $rlist = str_ireplace('0x', "", $rlist);
    $rlist = str_ireplace('%0b', "", $rlist);
    $rlist = str_ireplace('%23', "", $rlist);
    $rlist = str_ireplace('hex', "", $rlist);
    $rlist = str_ireplace('updatexml', "update", $rlist);
    $rlist = str_ireplace('extractvalue', "extract", $rlist);
    $rlist = str_ireplace('union', "unio", $rlist);
    $rlist = str_ireplace('benchmark', "bench", $rlist);
    $rlist = str_ireplace('sleep', "slee", $rlist);
    $rlist = str_ireplace('load_file', "", $rlist);
    $rlist = str_ireplace('outfile', "out", $rlist);
    $rlist = str_ireplace('ascii', "asc", $rlist);
    $rlist = str_ireplace('char(', "cha", $rlist);
    $rlist = str_ireplace('substr', "sub", $rlist);
    $rlist = str_ireplace('substring', "sub", $rlist);
    $rlist = str_ireplace('script', "scri", $rlist);
    $rlist = str_ireplace('frame', "", $rlist);
    $rlist = str_ireplace('%26', "", $rlist);
    $rlist = str_ireplace('%7c', "", $rlist);
    $rlist = str_ireplace('file_', "fil", $rlist);
    $rlist = str_ireplace('information_schema', "infor", $rlist);
    $rlist = str_ireplace('exp', "ex", $rlist);
    $rlist = str_ireplace('information_schema', "infor", $rlist);
    $rlist = str_ireplace('GeometryCollection', "Geomet", $rlist);
    $rlist = str_ireplace('polygon', "poly", $rlist);
    $rlist = str_ireplace('multipoint', "multi", $rlist);
    $rlist = str_ireplace('multilinestring', "multi", $rlist);
    $rlist = str_ireplace('linestring', "lines", $rlist);
    $rlist = str_ireplace('multipolygon', "multi", $rlist);
    $ml=array();
    if($id>0){...}
    $readmlist=join($ml,",");
    return $readmlist;
}
```

过滤

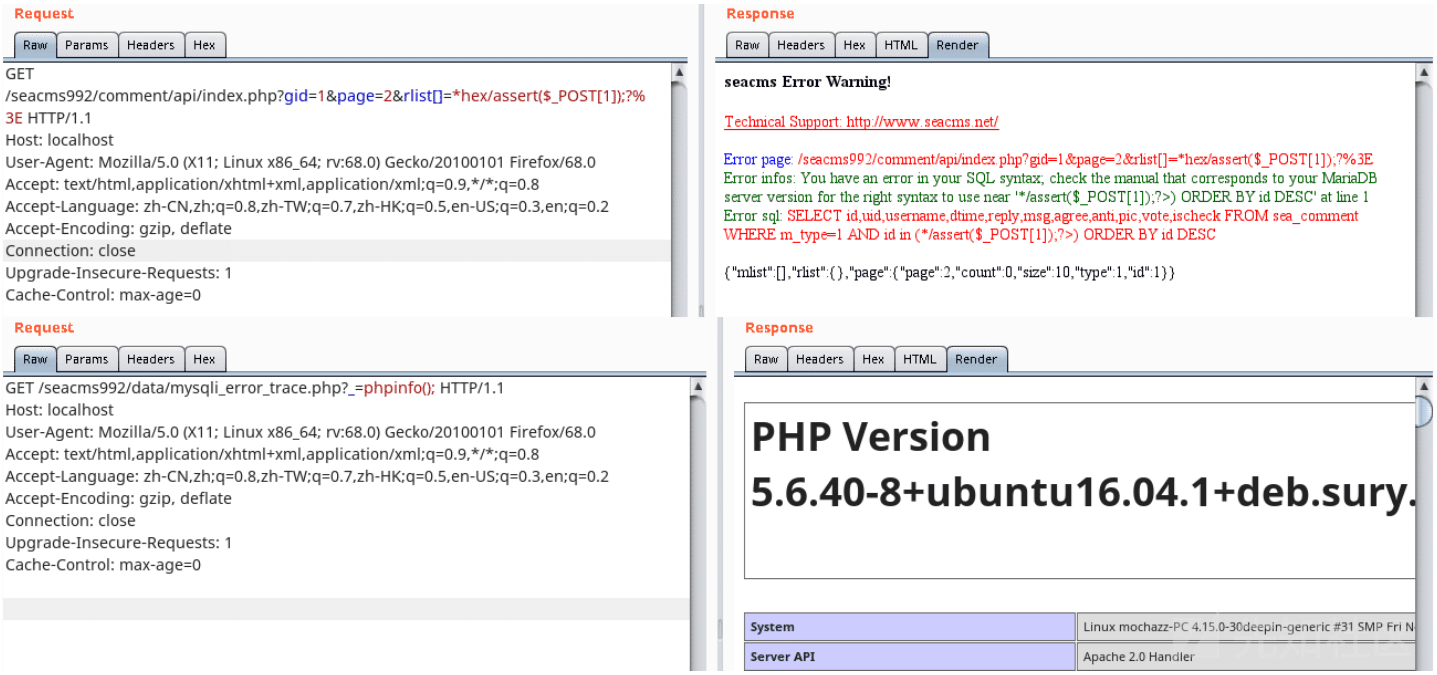
然后再看 Readrlist 函数。这里的 $ids 其实就是刚才可控的 $rlist 变量，有没发现这里直接拼接在 SQL 语句中，而且没有引号包裹。而 getshell 也是发生在SQL语句执行这里。（下图对应文件位置：comment/api/index.php）

```php
function Readrlist($ids,$page,$size)
{
    global $dsql,$type;
    $rl=array();
    $sql = "SELECT id,uid,username,dtime,reply,msg,agree,anti,pic,vote,ischeck FROM sea_comment WHERE m_type=$type AND id in ($ids) ORDER
    $dsql->setQuery($sql);
    $dsql->Execute('commentrlist');
    while($row=$dsql->GetArray('commentrlist'))
    {
        $rl[]="\"".$row['id']."\":{\"uid\":".$row['uid'].",\"tmp\":\"\",\"nick\":\"".$row['username']."\",\"face\":\"\",\"star\":\"\",\"ar
    }
    $readrlist=join($rl,",");
    return $readrlist;
}
```


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）

```php
    function Execute($id="me", $sql='')
    {
        //SQL语句安全检查
        if($this->safeCheck)  safeCheck: true
        {
            CheckSql($this->queryString);
        }
        $this->result[$id] = mysqli_query($this->linkID,$this->queryString);
        if($this->result[$id]===false)
        {
            $this->DisplayError(mysqli_error($this->linkID)." <br />Error sql: <font color='red'>".$this->queryString."</font>"
        }
    }
    function DisplayError($msg)
    {
        $errorTrackFile = dirname(__FILE__).'/../data/mysqli_error_trace.php';
        $emsg = '';
        $emsg .= "<div><h3>seacms Error Warning!</h3>\r\n";
        $emsg .= "<div><a href='http://www.seacms.net/
' target='_blank' style='...'>Technical Support: http://www.seacms.net/</a></div>";
        $emsg .= "<div style='line-helght:160%;font-size:14px;color:green'>\r\n";
        $emsg .= "<div style='color:blue'><br />Error page: <font color='red'>".$this->GetCurUrl()."</font></div>\r\n";
        $emsg .= "<div>Error infos: {$msg}</div>\r\n";
        $emsg .= "<br /></div></div>\r\n";
        $savemsg = 'Page: '.$this->GetCurUrl()."\r\nError: ".$msg;
        //保存MySql错误日志
        $fp = @fopen($errorTrackFile, 'a');
        @fwrite($fp, "\r\n<?php /*\r\n {$savemsg} \r\n*/  ?>\r\n\r\n");
        @fclose($fp);
    }
```


getshell 结果如下：



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