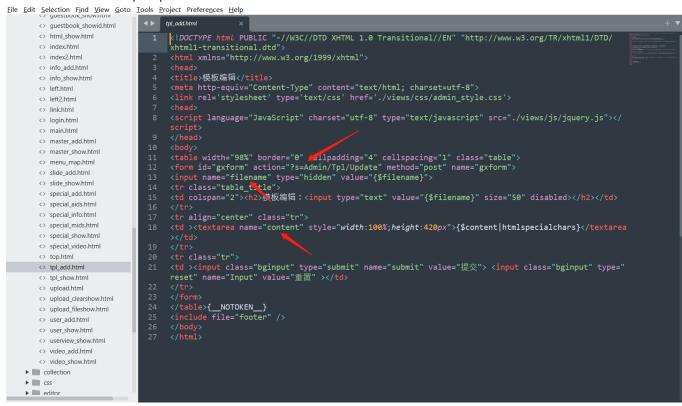


## 1、Vulnerability code Audit

The vulnerability appears in the template management page in the background:



/views/admin/tpl\_add. HTML file is received by filename, content is received by content, and then the data is sent to? S = Admin/Tpl/Update



Track? S = Admin/Tpl/Update page source/core/Lib/Action/Admin/TplAction class. PHP file, see the Update function to receive the filename and the content variables, only after receiving the two variables for judging whether it is empty, Data is written to the file directly using the write\_file function without dangerous

character detection for file names and contents, which means there is any file upload vulnerability.

```
<u>File Edit Selection Find View Goto Iools Project Preferences Help</u>

<u>Find View Goto Iools Project Preferences Help</u>
                                                        ▼ ► TplAction.class.php
       ▼ 🚞 Lib
         ▼ 🕋 Action
                                                                                        $this->error('模板名不能为空!');
           ▼ 🚞 Admin
                                                                                 $content = read_file($tpl);
$this->assign('filename',$tpl);
$this->assign('content',$content);
               AdsenseAction.class.php
                CacheAction.class.php
                ChannelAction.class.php
                                                                                 $this->display('./views/admin/tpl_add.html');
                CollectAction.class.php
               CommentAction.class.php
                ConfigAction.class.php
                                                                          public function update(){
    $filename = trim($_POST['filename']);
    $content = stripslashes($_POST['content']);
    if (|testwrite(substr($filename,0,strrpos($filename,'/')))){
        $this->error('在线编辑模板需要给'.TEMPLATE_PATH.'添加写入权限!');
}
                CustomcollectAction.class.php
                DataAction.class.php
               DatacheckAction.class.php
                GuestbookAction.class.php
                HtmlAction.class.php
                                                                                 }
if (empty($filename)) {
    $this->error('模板文件名不能为空!');
                IndexAction.class.php
               ☐ InfoAction.class.php
                InstallAction.class.php
                                                                                 if (empty($content)) {
    $this->error('模板内容不能为空!');
               ☐ LinkAction.class.php
               LoginAction.class.php
               MasterAction.class.php
                                                                                 $
$tpl = $filename;
$ile($tpl,$)
                ☐ SlideAction.class.php
                                                                                 write file($tpl,$content);
if (!empty($_SESSION['tpl_reurl'])) {
    $this->assign("jumpUrl",$_SESSION['tpl_reurl']);
                SpecialAction.class.php
               TplAction.class.php
               UploadAction.class.php
               ☐ UserAction.class.php
               UserviewAction.class.php
               ☐ VideoAction.class.php
           ▶ ■ Home
           ▶ ■ Plus
             AdminAction.class.php
                                                                          public function del(){
    $id = str_replace('*','/',str_replace('@','.',trim($_GET['id'])));
    if (!substr(sprintf("%o",fileperms($id)),-3)){
        $this->error('无删除权限!');
             CmsAction.class.php
             HomeAction.class.php

☐ VcodeAction.class.php

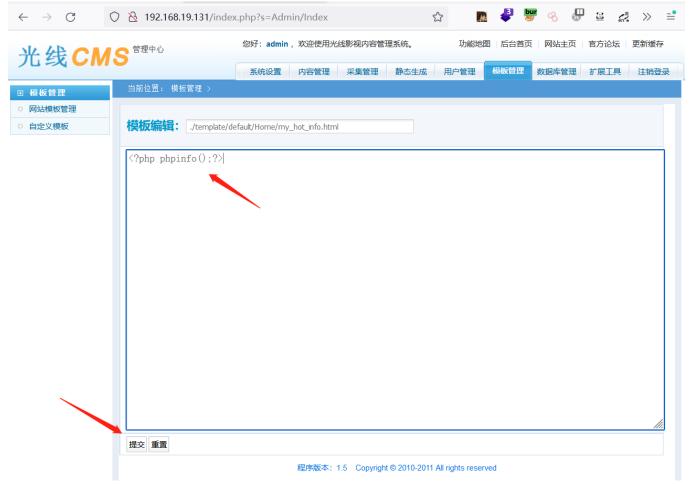
         ▶ ■ Model
      ► ThinkPHP
                                                                                 @unlink($id);
if (!empty($_SESSION['tpl_reurl'])) {
```

## 2. The exploit

Log in to the background of the target website by admin default password admin888 or password blasting or even phishing, click Template Management to enter the /template/default/Home directory, select any file and click Edit:



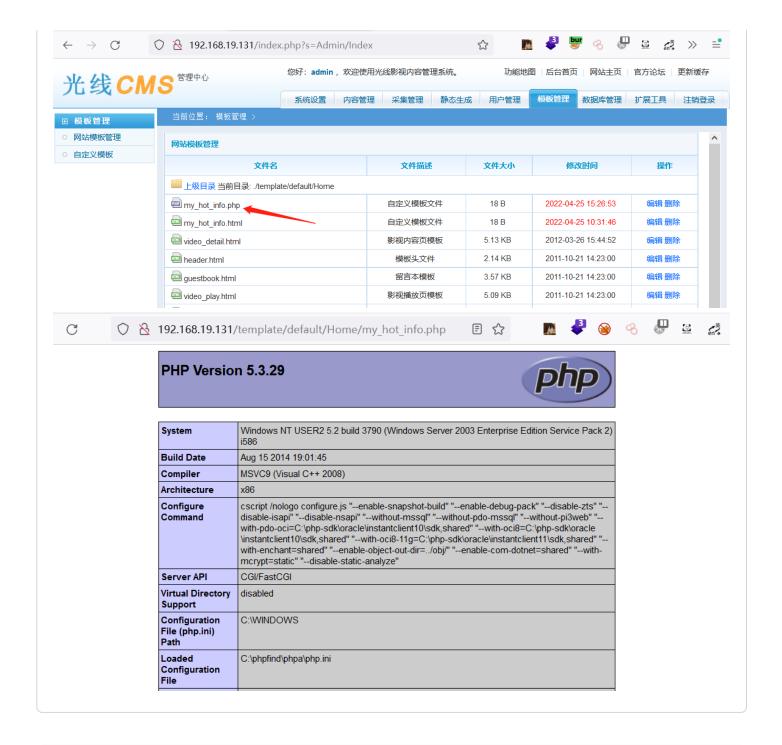
Enter the EDIT page, enter the PHP test code in the file content form, start the BurpSuite tool to capture packages, and click Submit:



After BurpSuite catches the package, change the filename suffix to PHP and click "Put the package" :



My\_hot\_info.php file was created successfully, and the PHP test code was successfully executed.



## Zack-Huang commented on May 17

Author

This vulnerability has been fixed in the new version, please visit the link to download the latest version of V1.7: http://www.gxcms.org/

**Assignees** 

No one assigned

Labels

None yet

Projects	
None yet	
Milestone No milestone	
Development  No branches or pull requests	

1 participant

