

A file upload vulnerability exists in the background

1.Environment construction

Built with PHPStudy2014 (Nginx+PHP5.3) and Ray CMS1.5.

Download from <http://www.gxcms.org/>



Put the website source code into the website root directory, access the address installation:

光线影视内容管理系统1.5 安装向导

1. 许可协议 2. 环境检测 3. 数据库设置 4. 安装完成

安装设置:

安装目录 自动检测一般不需要修改,结尾必需加斜杆 '/'	<input type="text" value="/"/>
服务器地址 一般为localhost	<input type="text" value="localhost"/>
数据库端口 请填写MYSQL数据库使用的端口	<input type="text" value="3306"/>
数据库用户名 一般为root	<input type="text" value="root"/>
数据库密码 密码尽量不要设为空	<input type="password" value="...."/>
数据库名称 请填写已存在的数据库名	<input type="text" value="gxcms"/>
数据库表前缀 一般不用修改	<input type="text" value="gx_"/>

<< 上一步 下一步 >>

Powered By 光线影视内容管理系统 1.5

192.168.19.131

光线影视 www.gxcms.com

登录 | 注册

RSS订阅 | 收藏本站 | 留言反馈 | 播放记录

首页 电影 电视剧 动漫 综艺 体育 纪录片 资讯 | 排行 专题

请输入关键字 视频 搜索 热门关键词: 热门标签1 热门标签2 热门标签3 热门标签4

最近更新 今日更新: [0] 总电影数量: [0]

近期热片推荐 热片排行榜>>

首页通栏广告1

电视剧热播榜 更多>> 电视剧 国产剧 台湾剧 香港剧 韩国剧 日本剧 欧美剧 海外剧 全部>>

2.Vulnerability code audit

File Edit Selection Find View Goto Tools Project Preferences Help

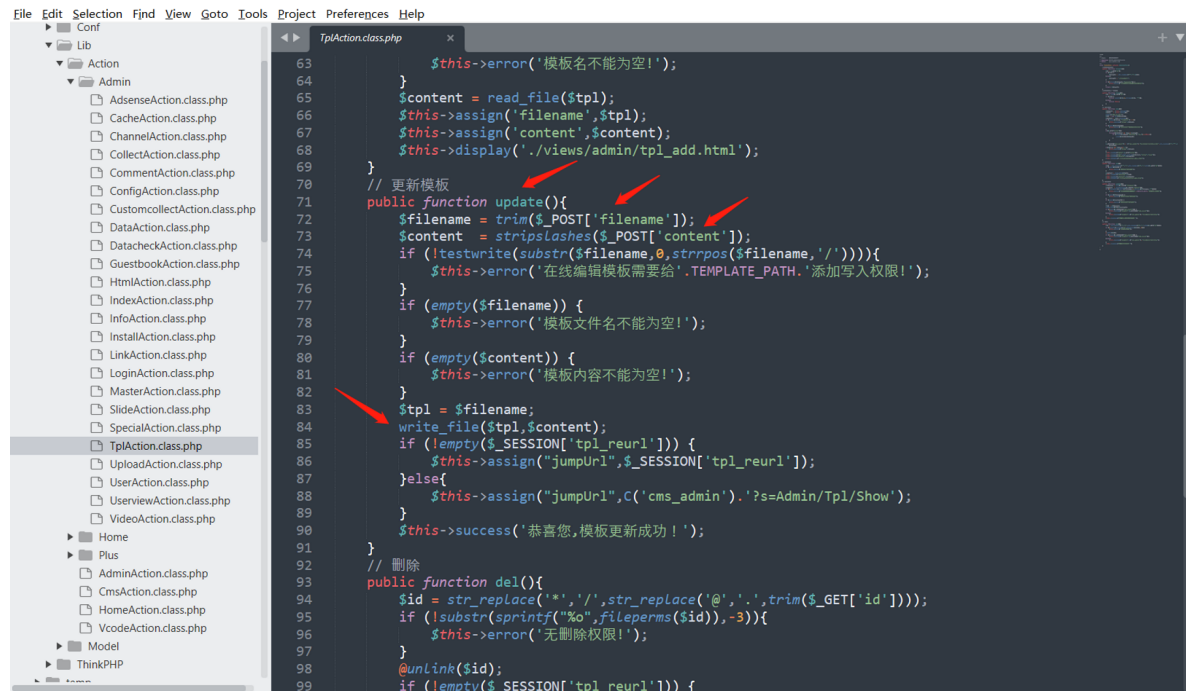
guestbook_showid.html
html_show.html
index.html
index2.html
info_add.html
info_show.html
left.html
left2.html
link.html
login.html
main.html
master_add.html
master_show.html
menu_map.html
slide_add.html
slide_show.html
special_add.html
special_aids.html
special_info.html
special_mids.html
special_show.html
special_video.html
top.html
tpl_add.html
tpl_show.html
upload.html
upload_clearshow.html
upload_fileshtml.html
user_add.html
user_show.html
userview_show.html
video_add.html
video_show.html

tpl_add.html

```
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 </script>
10 </head>
11 <body>
12 <table width="98%" border="0" cellpadding="4" cellspacing="1" class="table">
13 <form id="gxform" action="?s=Admin/Tpl/Update" method="post" name="gxform">
14 <input name="filename" type="hidden" value="{ $filename }">
15 <tr class="table_title">
16 <td colspan="2"><h2>模板编辑 : <input type="text" value="{ $filename }" size="50" disabled></h2></td>
17 </tr>
18 <tr align="center" class="tr">
19 <td ><textarea name="content" style="width:100%;height:420px">{ $content|htmlspecialchars}</textarea>
20 </td>
21 </tr>
22 <tr class="tr">
23 <td ><input class="bginput" type="submit" name="submit" value="提交"> <input class="bginput" type="
24 reset" name="Input" value="重置" ></td>
25 </tr>
26 </form>
27 </table>{ _NOTOKEN_ }
28 <include file="footer" />
29 </body>
30 </html>
```

Track them down? 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, The file name and file contents are not
detected with dangerous characters, and data is directly written to the file using the write_file

function, which means that there is any file upload vulnerability.



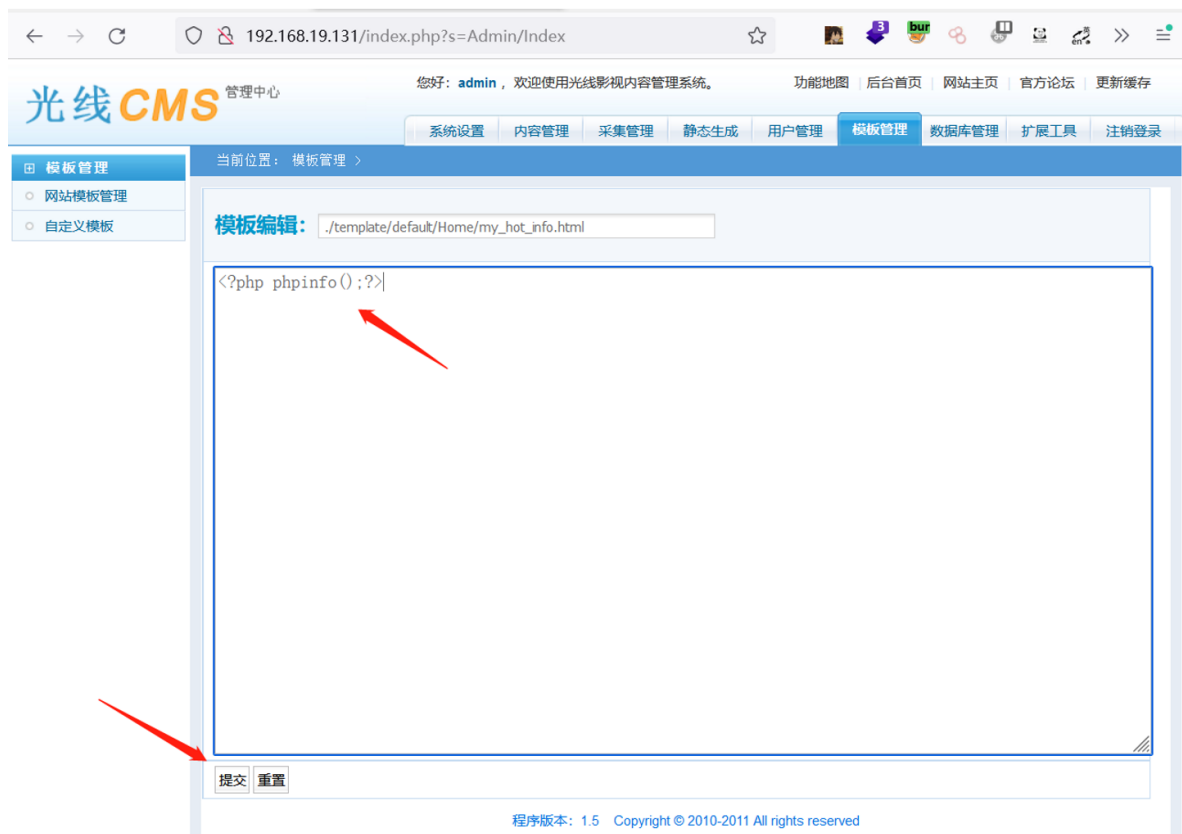
```
63 $this->error('模板名不能为空!');
64 }
65 $content = read_file($tpl);
66 $this->assign('filename',$tpl);
67 $this->assign('content',$content);
68 $this->display('./views/admin/tpl_add.html');
69 }
70 // 更新模板
71 public function update(){
72     $filename = trim($_POST['filename']);
73     $content = stripslashes($_POST['content']);
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('恭喜你,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'])) {
```

3. Exploit the vulnerability

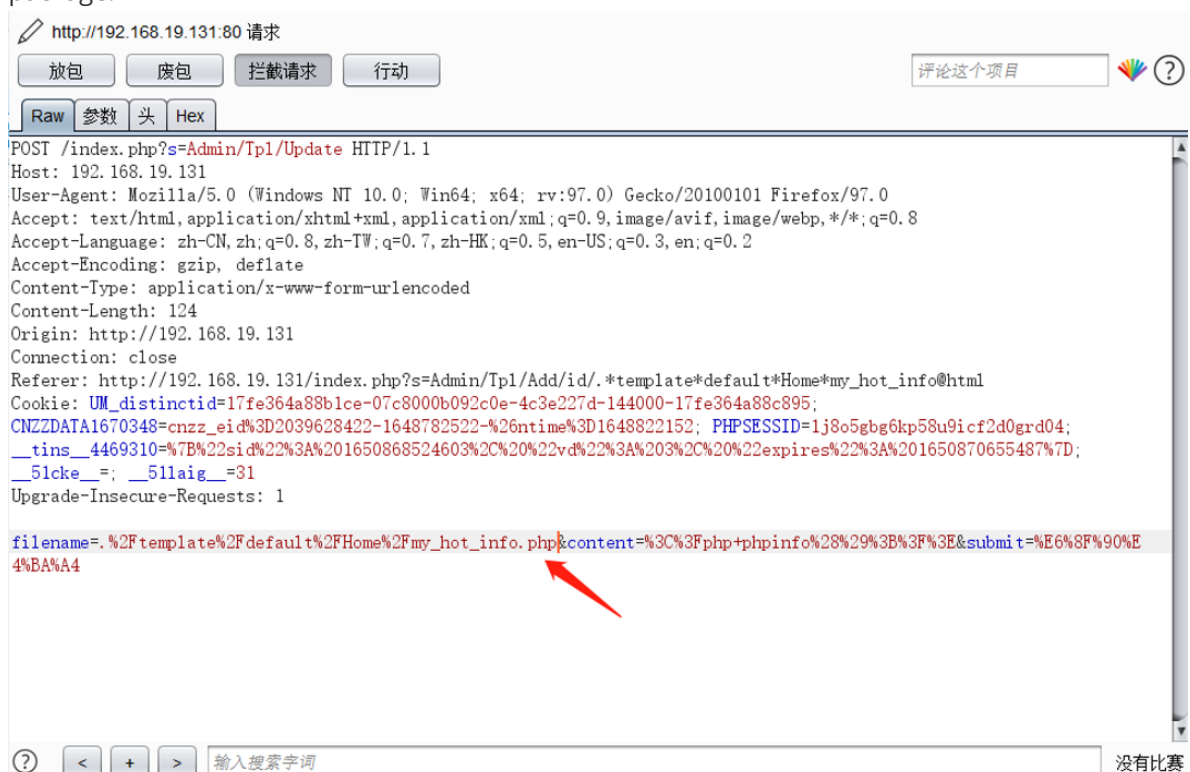
Log in to the background of the target website through admin default password admin888 or password blasting or even phishing, click template management to enter the /template/default/Home directory, select any file and click edit:



Enter the editing page, enter the php test code in the file content form, start BurpSuite tool to capture the package, and click Submit:



BurpSuite after catching the package, change the filename suffix to php, and then click Put package:



Back to the background website template management, see the successful creation of my_hot_info.php file, visit the file page to see the successful execution of php test code:

← → ↺

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

当前位置: 模板管理 >

网站模板管理

自定义模板

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	留言板模板	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

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	cscript /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