New issue

Jump to bottom

Bug:V2.0.0 File upload vulnerability #1

Open Richard1266 opened this issue on Apr 29, 2019 · 0 comments

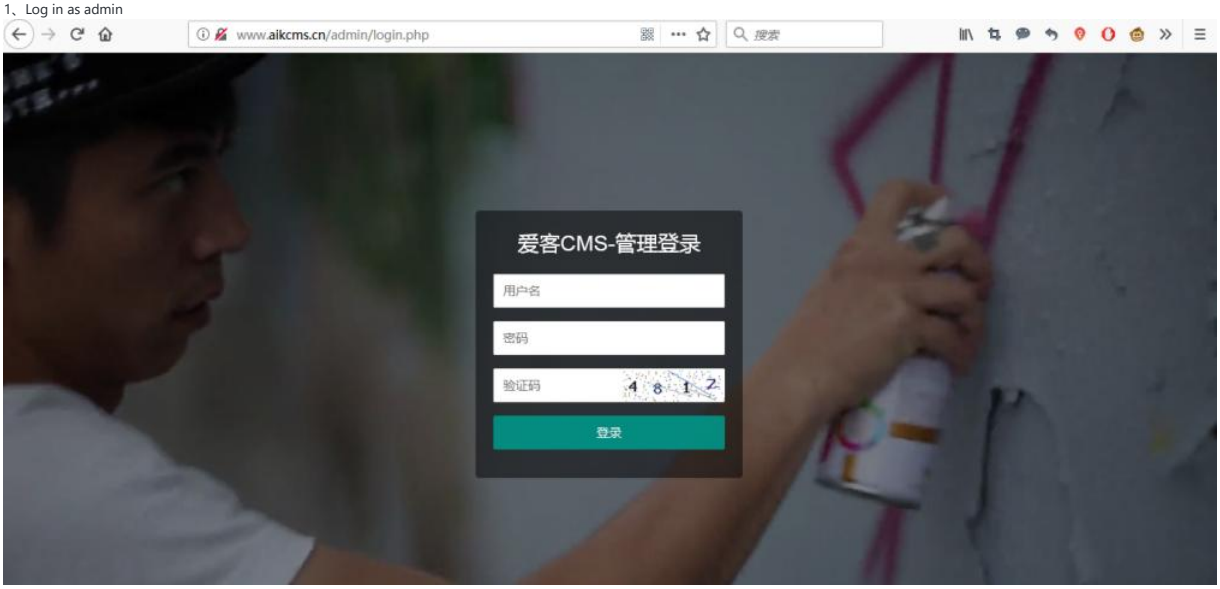
Richard1266 commented on Apr 29, 2019 Owner

There is an File upload vulnerability in your latest version of the CMS v2.0.0
Download link: "http://www.aikcms.com/download/%E7%88%B1%E5%AE%A2CMS2.0.zip"

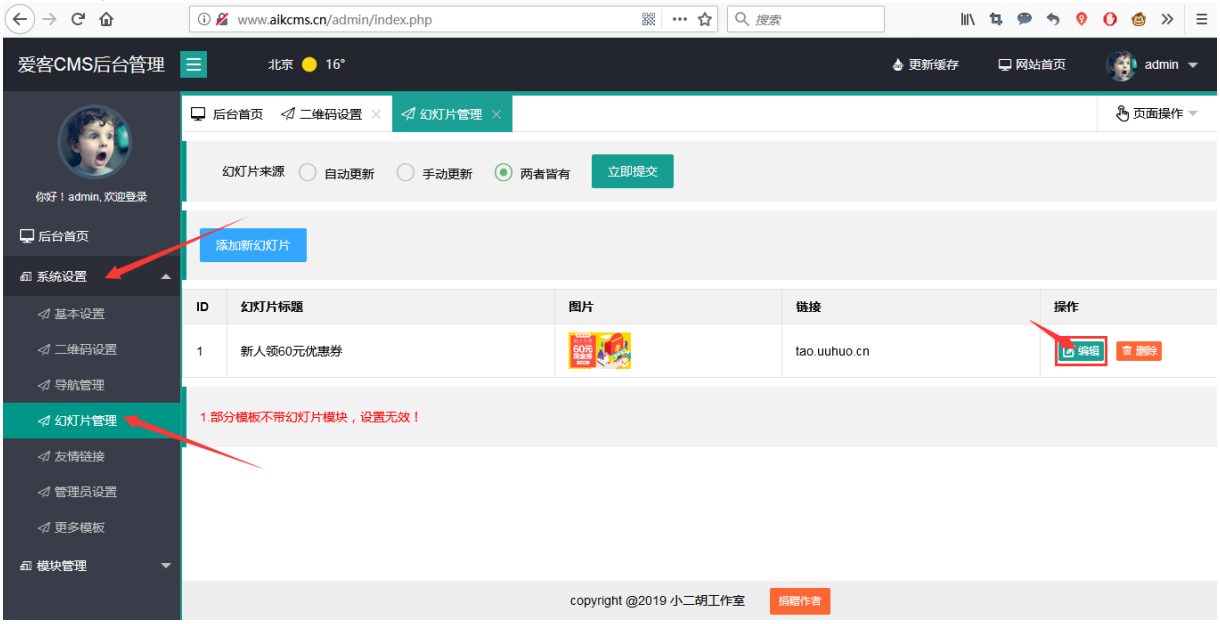
In the AIKCMSv2.0.0\admin\page\admincore\poster_edit.php，No checksum filtering of file extensions of uploaded files：

```php
<?php
if (isset($_POST['update'])) {
    $_data['aik_hd_name'] = $_POST['aik_hd_name'];
    $_data['aik_hd_img'] = $_POST['aik_hd_img'];
    $_data['aik_hd_link'] = $_POST['aik_hd_link'];
    if(move_uploaded_file($_FILES['aik_hd_img']['tmp_name'],'../../../upload/'.$_FILES['aik_hd_img']['name'])){
    $_data['aik_hd_img']='/upload/'.$_FILES['aik_hd_img']['name'];}
    null_back($_data['aik_hd_link'], '请输入或上传图片');
    $sql = 'update aikcms_poster  set ' . arrtoupdate($_data) . ' where id = ' . $_GET['id'] . '';
    if (mysql_query($sql)) {
        alert_href('幻灯片修改成功!', 'poster.php');
    } else {
        alert_back('修改失败!');
    }
}
```

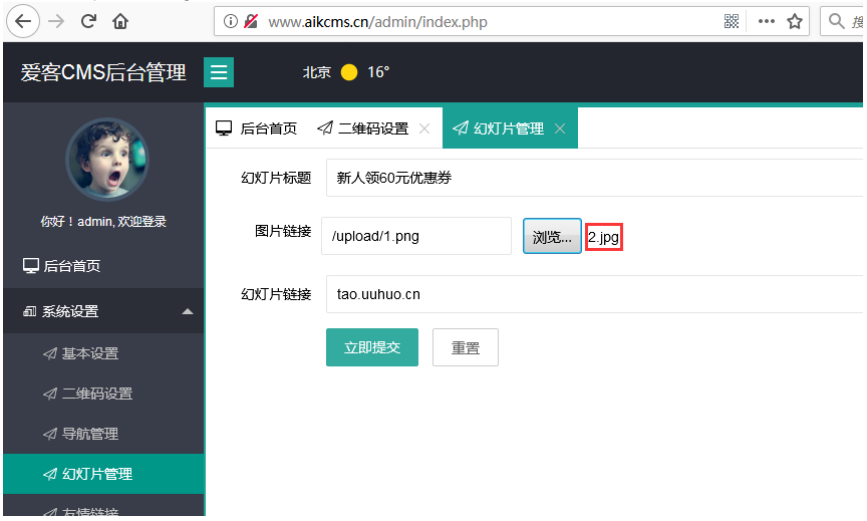
1、Log in as admin

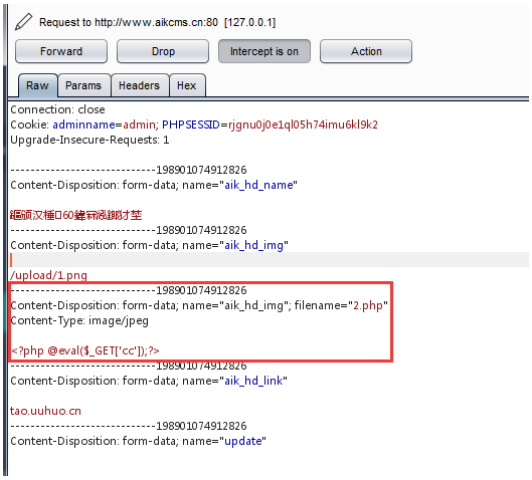


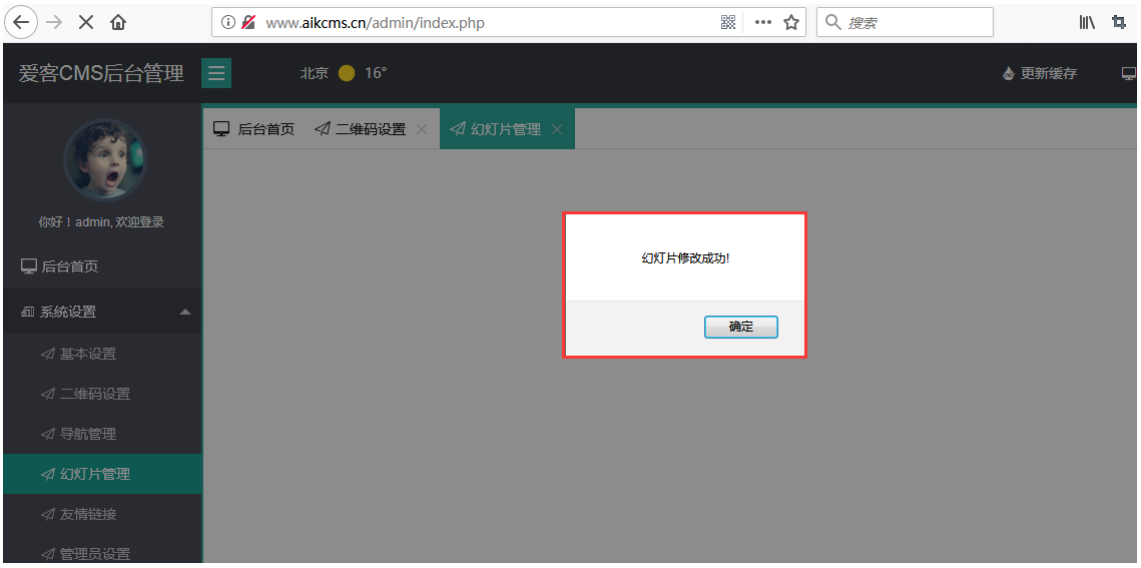
2、Choose this part



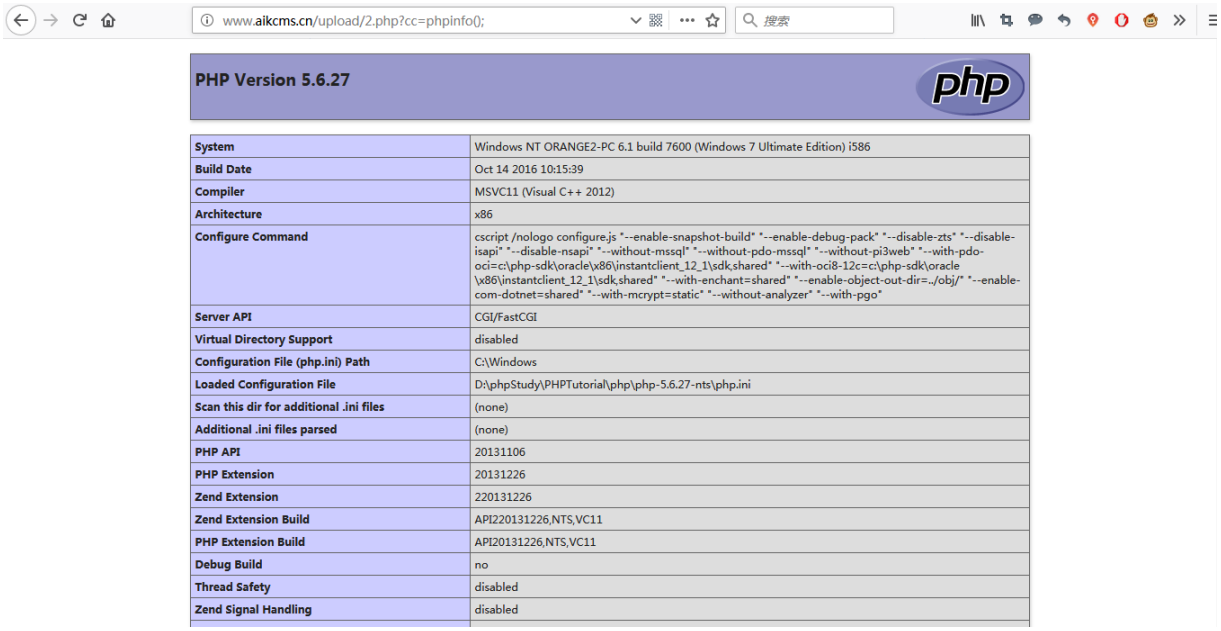
3、Edit and capture the change suffix name







4、Getshell



System	Windows NT ORANGE2-PC 6.1 build 7600 (Windows 7 Ultimate Edition) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
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\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	D:\phpStudy\PHPTutorial\php\php-5.6.27-nts\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,NTS,VC11
PHP Extension Build	API20131226,NTS,VC11
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant