

New issue Jump to bottom

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

 \bigcirc **Open** \bigcirc **zhendezuile** opened this issue on Apr 1 \cdot 0 comments

Vulnerability to reproduce:

- 1. First log in to the backend of the website
- 2、Visit url: http://www.xxx.com/admin/index.php?

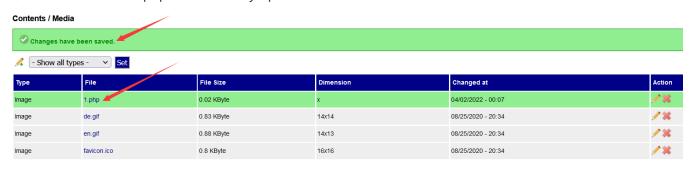
mode=content&page=media&action=edit&file=de.gif&type=1.

Then operate as shown below:

bloofoxCMS Admincenter



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



4. Visit http://www.xxx.com/media/images/1.pm	p and execute the code to get pripring information
PHP Versi	on 5.2.17
	W. L. MTWACON DO AND TLOOPS
System Build Date	Windows NT XIAOBIN-PC 6.2 build 9200 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
Server API	\sdk,shared" "with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "without-pi3web" Apache 2.4 Handler - Apache Lounge
Virtual Director Support	
Configuration F (php.ini) Path	File C:\windows
Loaded Configuration F	D:\phpstudy2018\PHPTutorial\php\php-5.2.17\php.ini
Scan this dir for additional .ini fi	(none)
additional .ini fi parsed	iles (none)
PHP API	20041225
Repair suggestion: Set the upload whitelist and limit the suffixes of u	uploaded files to gif, jpg, and png
ssignees	
o one assigned	
bels	
one yet	
ojects	
one yet	
ilestone	
o milestone	
evelopment	

No branches or pull requests

1 participant

