

Hgame_Week1_Writeup

Web

换头大作战

进入页面

想要flag嘛:

随便输入，出现提示我们用 POST 方法发送

想要flag嘛:

request method is error.I think POST is better

利用火狐自带的开发者工具查看页面代码，将方法改为 POST，并重新发送

```
<!DOCTYPE html>
<html>
  <head> ... </head>
  <body>
    <form action="index.php" method="post"> ... </form>
    <br>
    request method is error.I think POST is better
  </body>
</html>
```

提示只有本地服务器可以得到 FLAG，并给了提示 X-Forwarded-For

想要flag嘛:

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

重新在请求头中增加参数 X-Forwarded-For:127.0.0.1 并发送请求

Request URL: http://120.78.184.111:8080/week1/how/index.php
Request method: POST
Remote address: 120.78.184.111:8080
Status code: 200 OK ⓘ Edit and Resend Raw headers
Version: HTTP/1.1

Filter headers

Content-Type: application/x-www-form-urlencoded
Cookie: admin=0
Host: 120.78.184.111:8080
Pragma: no-cache
Referer: http://120.78.184.111:8080/week1/how/index.php?want=1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linu...) Gecko/20100101 Firefox/64.0
X-Forwarded-For: 127.0.0.1

返回页面中提示我们更改代理浏览器参数为 use Waterfox/50.0

submit

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

更改并发送得到返回页面

User-Agent: use Waterfox/50.0

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

提示更改参照页为 WWW。BILIBILI。COM，更改后重新发送，得到返回页面

Referer: www.bilibili.com

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

更改 cookie 为 admin=1

Cookie: admin=1

得到 FLAG

hgame{hTTp_HeaDeR_iS_Ez}