Frost HGAME 2019 week_1 web write up

（实在太菜，只做出来 1 道题。另外几道都做了一半,卡住做不下去了，很难受。不过我一定会继续努力的！）

换头大作战

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

打开网页，看到如下输入框：

尝试输入 flag 并提交，得到如下提示：

于是用 burpsuite 截包并修改 get 为 post，得到如下提示：

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

于是添加头信息 X-Forwarded-For: 127.0.0.1 并发送， 又得到如下提示：

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

于是添加在 User_agent 添加 Waterfox/50.0 并发送，又得到如下提示：

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

于是添加头信息 Referer: www.bilibili.com，又得到如下提示：

想要flag嘛： submit

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

于是修改头信息 cookie: admin=1 并发送，得到 flag：

想要flag嘛： submit

hgame{hTTp_HeaDeR_iS_Ez}

以下为最终头部：

Raw | Params | Headers | Hex

```
POST /week1/how/index.php HTTP/1.1
Host: 120.78.184.111:8080
Content-Length: 9
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.67 Safari/537.36Waterfox/50.0
Origin: http://120.78.184.111:8080
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://120.78.184.111:8080/week1/how/index.php?want=
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: admin=1
Connection: close
X-Forwarded-For: 127.0.0.1
Referer: www.bilibili.com

want=flag
```