

# week1

---

## Web

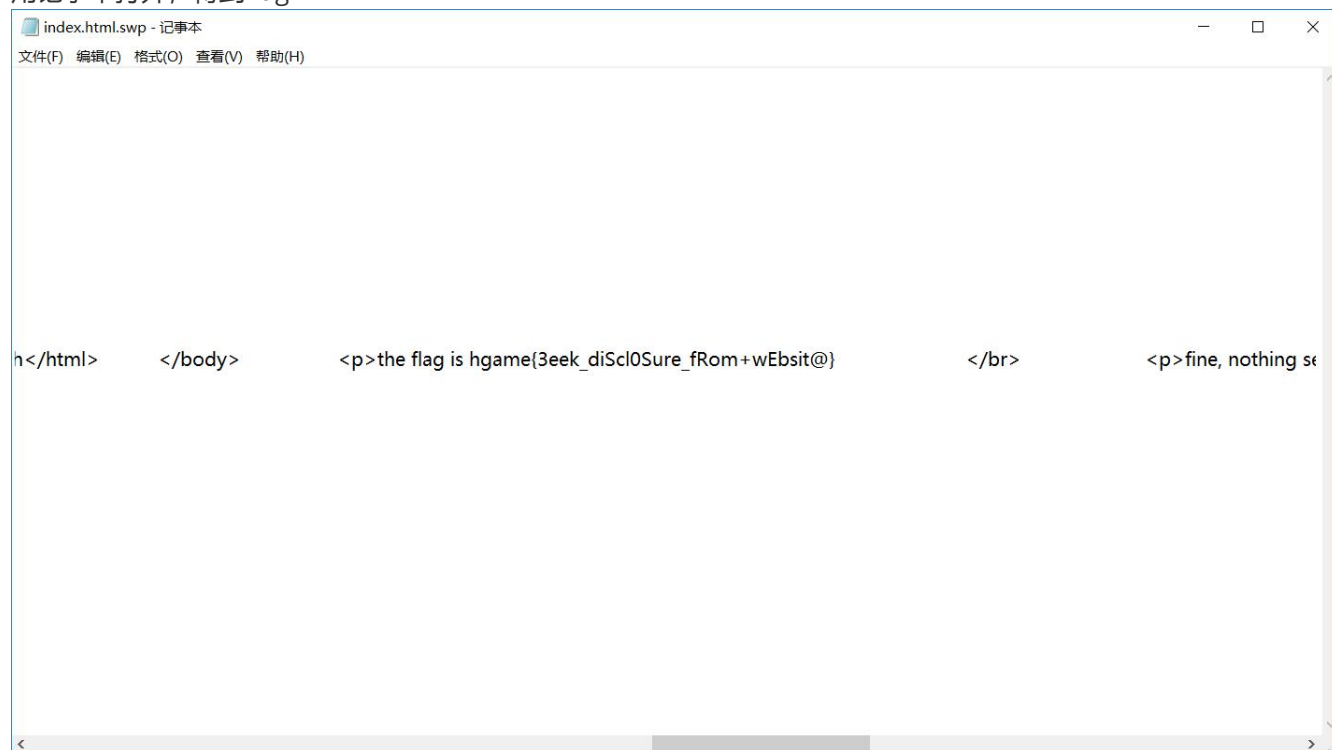
---

### 谁吃了我的flag

打开网址，发现hgame{3eek\_diScI0Sure，disclosure是泄露的意思，联系hint，是vim备份文件泄露，于是可以在网址后面尝试.index.php.swp，下载下来一个文件



用记事本打开，得到flag



### 换头大作战

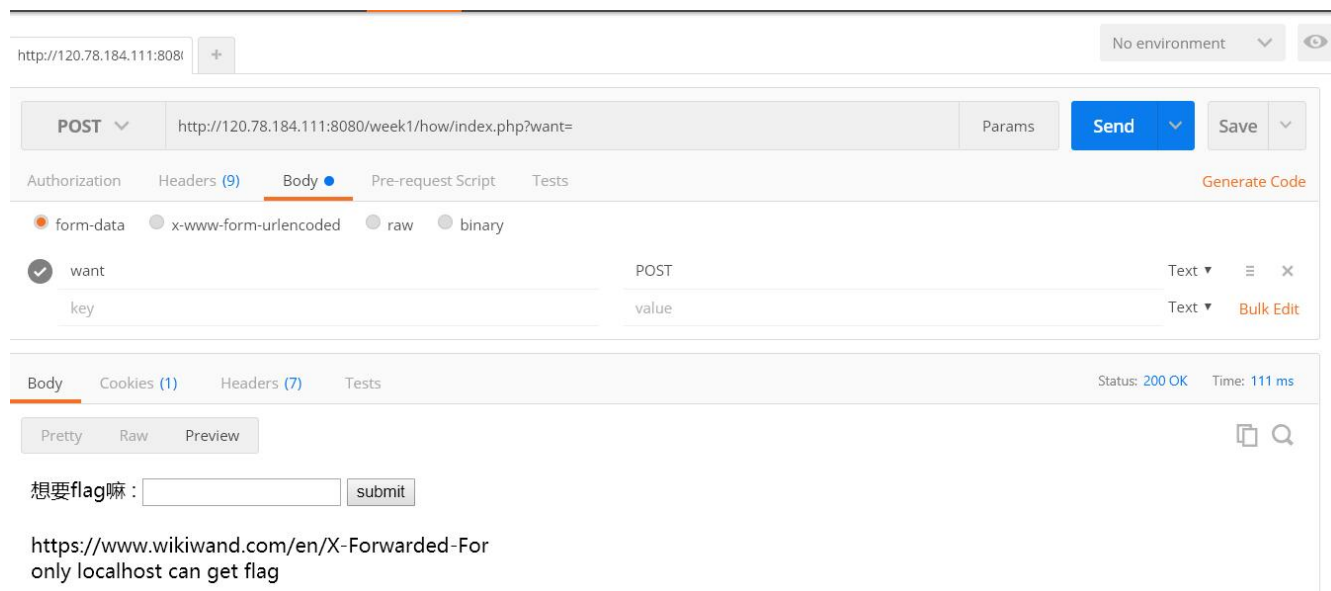
打开网址，随便输入一些什么东西

看到提示请求方法错误，用POST

想要flag嘛：

request method is error.I think POST is better

打开刚下好的postman发送post请求



发现提示 x-forwarded-for 还有只有localhost才能获得flag

于是。。换头！

✓ X-Forwarded-For 127.0.0.1

发现如下提示

想要flag嘛：

https://www.wikiwand.com/en/User\_agent  
please use Waterfox/50.0

于是只要把请求头中的用户代理中的浏览器版本信息改成和题中一样的就行了，换头！

✓ User-agent ; x64) AppleWebKit/537.36 (KHTML, like Gecko)Waterfox/50.0

然后又看到referer要换成从b站过来的

想要flag嘛:

https://www.wikiwand.com/en/HTTP\_referer  
the requests should referer from www.bilibili.com

于是再换头!

✓ Referrer

= =为什么还有 提示我不是admin

想要flag嘛:

https://www.wikiwand.com/en/HTTP\_cookie  
you are not admin

于是再将请求头里面的cookie改成admin=1, 最后一次换头!

✓ Cookie

于是flag就跳出来了

POST 

Params

Send

Authorization

Headers (8)

Body ☒

Pre-request Script

Tests

✓ Upgrade-Insecure-Requests	1	<input type="button" value="≡"/>	<input type="button" value="x"/>
✓ User-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.	<input type="button" value="≡"/>	<input type="button" value="x"/>
✓ Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image	<input type="button" value="≡"/>	<input type="button" value="x"/>
✓ Referrer	www.bilibili.com	<input type="button" value="≡"/>	<input type="button" value="x"/>
✓ Accept-Encoding	gzip, deflate	<input type="button" value="≡"/>	<input type="button" value="x"/>
✓ Accept-Language	zh-CN,zh;q=0.9	<input type="button" value="≡"/>	<input type="button" value="x"/>
✓ Cookie	admin=1	<input type="button" value="≡"/>	<input type="button" value="x"/>
✓ X-Forwarded-For	127.0.0.1	<input type="button" value="≡"/>	<input type="button" value="x"/>
key	value	<div>Bulk Edit</div>	

Body

Cookies (1)

Headers (7)

Tests

Status: 200 OK

Pretty

Raw

Preview

想要flag嘛:

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__);
?>
```

代码审计，程序的逻辑是id中找不到vidar，并且再一次解码后要 and vidar 相等

v的URL编码为：%76，二次编码为%25%37%36，绕过

[http://120.78.184.111:8080/week1/very\\_ez/index.php?id=%25%37%36idar](http://120.78.184.111:8080/week1/very_ez/index.php?id=%25%37%36idar)

```
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__);
?>
```

can u find me?



the gate has been hidden

can you find it? xixixi

右键查看网页源代码

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4   <title>can u find me?</title>
5 </head>
6 <body>
7   <p>the gate has been hidden</p>
8   <p>can you find it? xixixi</p>
9   <a href="f12.php"></a>
10 </body>
11 </html>
12
```

yeah!you find the gate

but can you find the password?

please post password to me! I will open the gate for you!

**connection** → keep-alive

**content-type** → text/html; charset=UTF-8

**date** → Sat, 02 Feb 2019 10:55:29 GMT

**password** → woyaoflag

**server** → nginx/1.15.8

**transfer-encoding** → chunked

**x-powered-by** → PHP/7.2.14

然后发现了password

用burpsuite

**Burp Suite Community Edition v1.7.33 - Temporary Project**

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title	Com
1	http://47.107.252.171:8080	GET	/f12.php			200	447	HTML	php	can u find me?	
2	http://47.107.252.171:8080	POST	/f12.php		✓			HTML	php		
3	http://47.107.252.171:8080		http://47.107.252.171:8080/f12.php		✓			HTML	php		

Request Response

Raw Headers Hex

GET /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,image/webp,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8  
Accept-Encoding: gzip, deflate  
Connection: close  
Upgrade-Insecure-Requests: 1

00101 Firefox/64.0  
=0.2

Send to Repeater

send to repeater



Raw Params Headers Hex		
Name	Value	
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; r...	Add
Accept	/*/*	Remove
Accept-Language	zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,e...	Up
Accept-Encoding	gzip, deflate	Down
content-type	application/x-www-form-urlencoded	
cache	no-cache	
origin	moz-extension://6210c8f8-e41b-43f9-9d97-9f...	
Content-Length	18	
Connection	close	
password	woyaoflag	

password=woyaoflag

发送! GO!

然后再一个get请求的response里面发现flag

GET request to http://47.107.252.171:8080/iamflag.php
Previous
Next
Action

Request
Response

Raw
Headers
Hex
HTML
Render

```

HTTP/1.1 302 Found
Server: nginx/1.15.8
Date: Sat, 02 Feb 2019 10:58:20 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>

```

?
<
+
>
0 matches

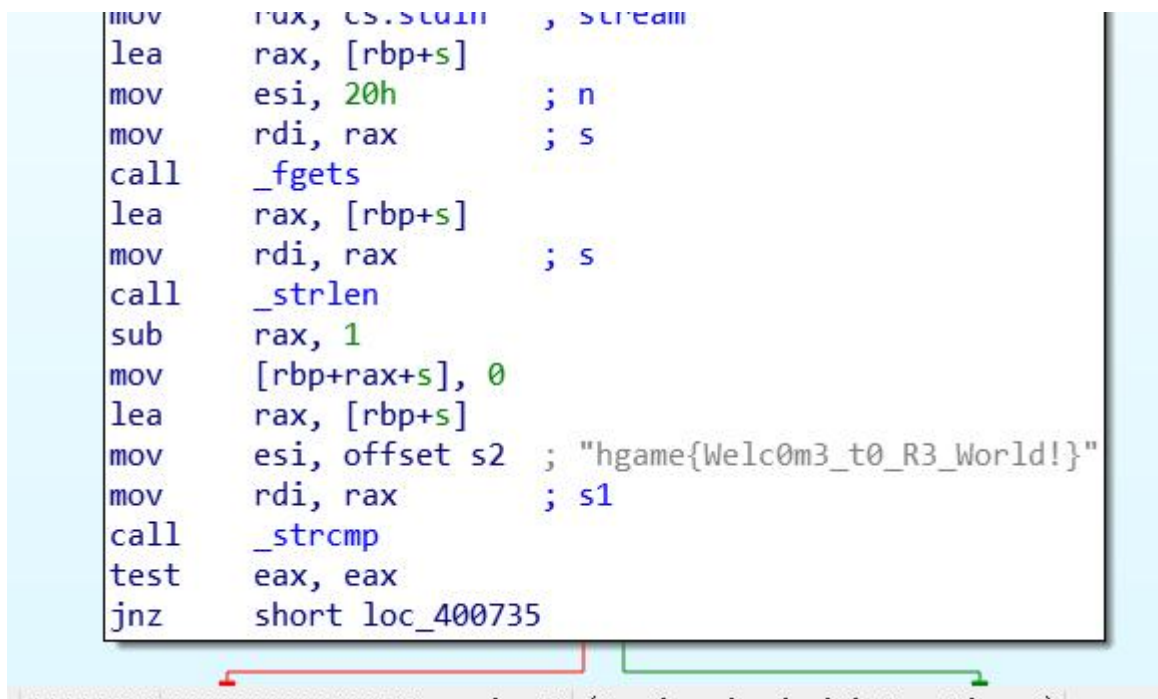


# Re

## HelloRe

直接拖入ida, 得到flag

```
mov     rax, cs:stream    , stream
lea     rax, [rbp+s]
mov     esi, 20h          ; n
mov     rdi, rax          ; s
call    _fgets
lea     rax, [rbp+s]
mov     rdi, rax          ; s
call    _strlen
sub     rax, 1
mov     [rbp+rax+s], 0
lea     rax, [rbp+s]
mov     esi, offset s2    ; "hgame{Welc0m3_t0_R3_World!}"
mov     rdi, rax          ; s1
call    _strcmp
test    eax, eax
jnz     short loc_400735
```



## Pro的Python教室(一)

把enc2用base64解码就行啦

```

import base64
import hashlib

enc1 = 'hgame{'
enc2 = 'SGVyZV8xc18zYXN5Xw=='
enc3 = 'Pyth0n}'

print 'Welcome to Processor\'s Python Classroom!\n'
print 'Here is Problem One.'
print 'There\'re three parts of the flag.'

print '-----'

print 'Plz input the first part:'
first = raw_input()
if first == enc1:
    pass
else:
    print 'Sorry , You\'re so vegatable!'
    exit()

print 'Plz input the secend part:'
secend = raw_input()
secend = base64.b64encode(secend)
if secend == enc2:
    pass
else:
    print 'Sorry , You\'re so vegatable!'
    exit()

print 'Plz input the third part:'
third = raw_input()
third = base64.b32decode(third)
if third == enc3:
    pass
else:
    print 'Sorry , You\'re so vegatable!'
    exit()

print 'Oh, You got it !'

```

[加密/解密](#)
[散列/哈希](#)
[BASE64](#)
[图片/BASE64转换](#)

明文:

Here 1s 3asy

BASE64编码 >

< BASE64解码

BASE64:

SGVyZV8xc18zYXN5Xw==

连起来就得到flag

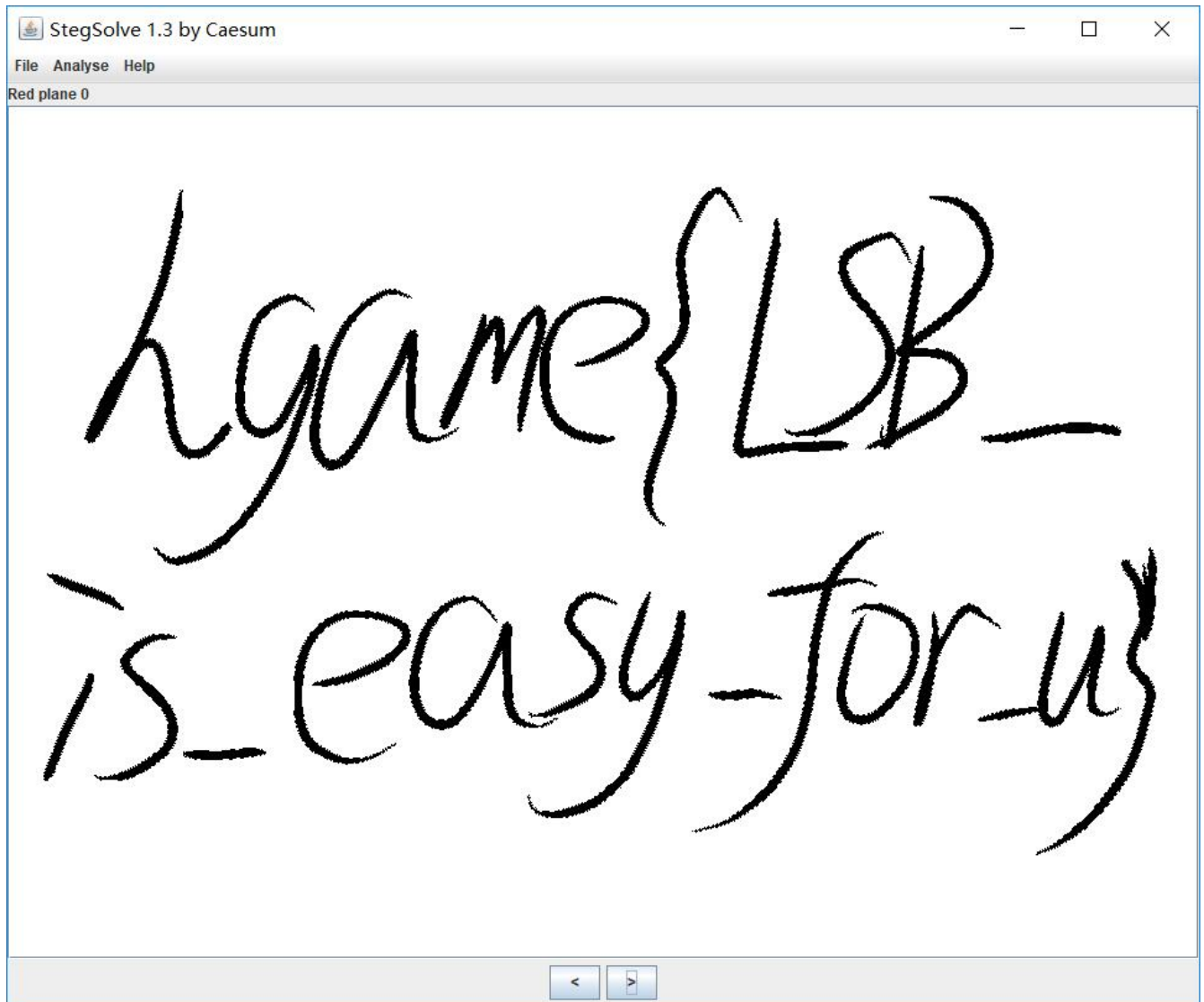
## Misc

### Hidden Image in LSB

百度一下。。嗯。。。LSB也就是最低有效位 (Least Significant Bit)。原理就是图片中的像数一般是由三种颜色组成，即三原色，由这三种原色可以组成其他各种颜色，例如在PNG图片的储存中，每个颜色会有 8bit，LSB隐写就是修改了像数中的最低的1bit，在人眼看来是看不出来区别的，也把信息隐藏起来了。

于是用神器stegsolve



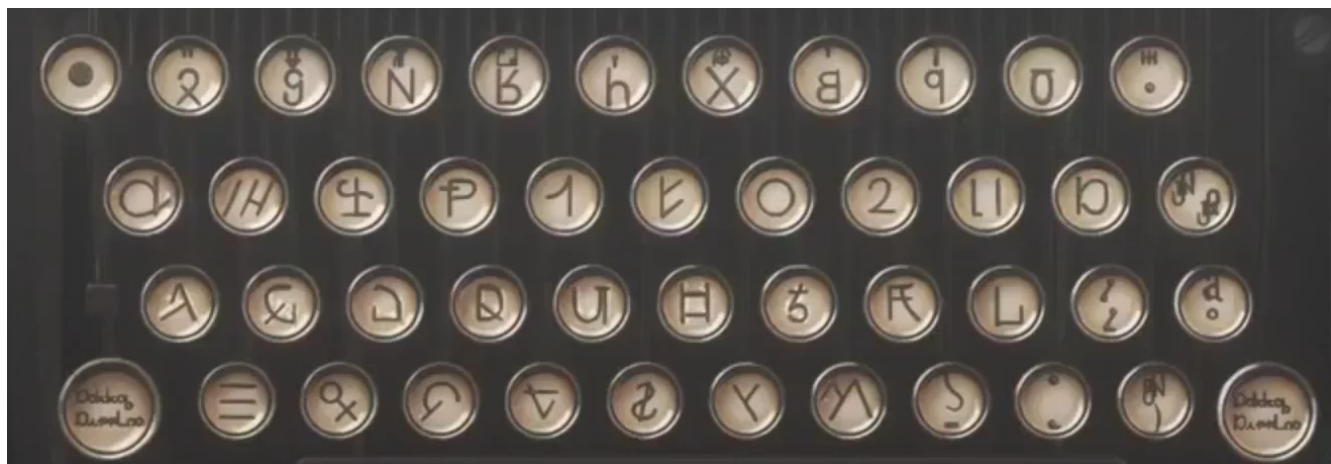


得到flag

## 打字机

嗯。。谷歌识图是个神器，发现这副图片是动漫紫罗兰永恒花园的截图





Πυλνα{Λr\_∀ι0Lαι\_ιr0αι//PιιαP}

于是利用强大的搜索引擎。。破解flag（一开始我把0和O搞错了，傻了好久



abcdefg hijkl mn

ιϕοδϕογ Πι κL ηχ

opqrst uvw xyz

νρ ϕ&ι οψ// ρr

然后其他题目都不怎么会了==慢慢学习ing。。。