

Web

0x01 谁吃了我的 flag

根据 hint, vim 在非正常退出时, 临时文件 swap 不会被删除, 访问 .xxx.swp 可以下载源码。

wget <http://118.25.111.31:10086/.index.html.swp>

```
kirino@kirino-virtual-machine:~$ wget http://118.25.111.31:10086/.index.html.swp
--2019-01-28 21:24:03-- http://118.25.111.31:10086/.index.html.swp
正在连接 118.25.111.31:10086... 已连接。
已发出 HTTP 请求, 正在等待回应... 200 OK
长度: 12288 (12K) [application/octet-stream]
正在保存至: ".index.html.swp"
```

cat index.html.swp, 得到 flag:

```
kirino@kirino-virtual-machine:~/download$ cat index.html.swp
b0VIM 8.0[PE]
000000E=000000</h</html>arrival~</body>mki/hgame<p>the flag is hgame{3eek diSc10Sure_fRo
m+wEbsit@}          </br>          <p>fine, nothing serious, just give you flag thi
s time...</p>          </br>          <p>damn...hgame2019 is coming soon, but the stu
```

0x02 换头大作战

打开网站, 随意输入, 提示要 POST 数据

Firefox hackbar:

Load URL:

Split URL: ☐

Execute:

Post data: ☐ Enable Post data ☐ Enable Referrer

Post data:

想要flag嘛:

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

提示要修改 X-Forwarded-For, 上 Burp Suite:

```
POST /week1/how/index.php? HTTP/1.1
Host: 120.78.184.111:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; 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
Accept-Encoding: gzip, deflate
Cookie: admin=0
Referer: http://120.78.184.111:8080/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 6
X-Forwarded-For: 127.0.0.1

want=1
```

提示 use Waterfox/50.0:

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

修改 User-Agent:

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:49.0)
Gecko/20100101 Waterfox/50.0
```

提示 referer from www.bilibili.com:

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

修改 referer:

```
Referer: www.bilibili.com
```

提示 you are not, 此时 Cookie 的 admin=0:

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

修改 Cookie:

```
Cookie: admin=1
```

得到 flag:

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

0x03 very easy Web

打开网站, 是段 php 代码, 大意是, 输入 id=vidar 的话直接终止, 但是只有 id=vidar 才能得到 flag, 这里要利用代码中的 urlencode, 只要把 vidar urlencode 就可以, v 的 ASCII 是%76, 但是还要注意%的 ASCII 是%25。

Payload: http://120.78.184.111:8080/week1/very_ez/index.php?id=%2576idar

```
hgame{urlDecode_Is_GoOd} <?php
error_reporting(0);
include("flag.php");
```

0x04 Can u find me?

根据 hint, 十二姑娘指 F12, 直接 F12, 在 body 里发现提示。

```
<body>
  <p>the gate has been hidden</p>
  <p>can you find it? xixixi</p>
  <a href="f12.php"></a>
</body>
```

访问 <http://47.107.252.171:8080/f12.php>, 页面提示要 POST password, F12, 发现响应头中的 password: wayaoflag。

响应头信息	原始头信息
Connection	keep-alive
Content-Length	242
Content-Type	text/html; charset=UTF-8
Date	Mon, 28 Jan 2019 14:41:21 GMT
Server	nginx/1.15.8
X-Powered-By	PHP/7.2.14
password	woyaoflag

Hackbar:

☒ Enable Post data ☐ Enable Referrer

访问连接:

```

yeah!you find the gate
but can you find the password?
please post password to me! I will open the gate for you!
right!
click me to get flag

```

提示 flag left in somewhere, 接着 F12

URL	Method	Status
GET iamflag.php	GET	302 Found
GET toofast.php	GET	200 OK

有个 302 跳转, flag 应该在 iamflag.php 里, 但是在 F12 中没有找到, 上 BurpSuit 拦截看看, 在 response 里发现 flag:

64	http://47.107.252.171:8080	GET	/iamflag.php	<input type="checkbox"/>	<input type="checkbox"/>	302
65	http://47.107.252.171:8080	GET	/toofast.php	<input type="checkbox"/>	<input type="checkbox"/>	200

RequestResponse

RawHeadersHexHTMLRender

```

Connection: keep-alive
X-Powered-By: PHP/7.2.14
location: toofast.php
Content-Length: 132

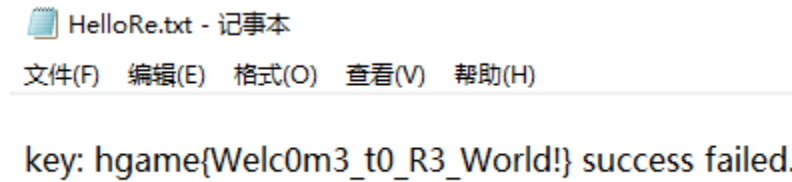
<html>
  <head>
    <title>can you find me?</title>
  </head>
  <body>
    <p>flag:hgame{f12_is_aMazIng111}</p>
  </body>
</html>

```

RE

0x01 HelloRe

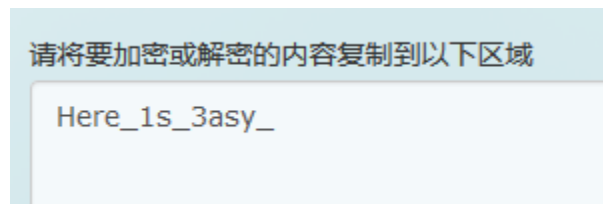
下载文件，用 TXT 打开，再 CTRL+F 搜索 hgame，得到 flag。



0x02 Pro 的 Python 教室（一）

打开链接是一段 python 代码，但是给出了 flag，直接 base64。

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



MISC

0x01 Hidden Image in LSB

用 StegSolve 打开，切换通道可以直接获得 flag。

