新生平台CTF

原创

paintShadow 于 2019-09-23 22:20:42 发布 548 收藏 1

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_44236278/article/details/101226949

get（Web）

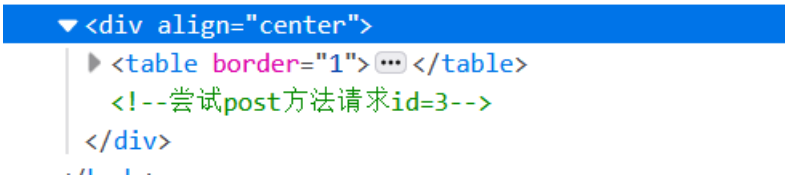
```
▶ <div style="color:aqua" align="center">…</div>
▼ <div align="center">
  ▶ <div style="color:red" align="center">…</div>
  ▶ <table border="1">…</table>
    <!--尝试get方法请求id=3-->
  </div>
```

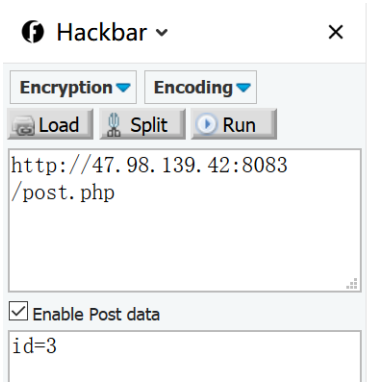
构造URL加上?id=3，然后就会获得flag

图书馆查询系统

id	书名	简介
3	《flag》	flag{congratulations_succeed}

post（Web）



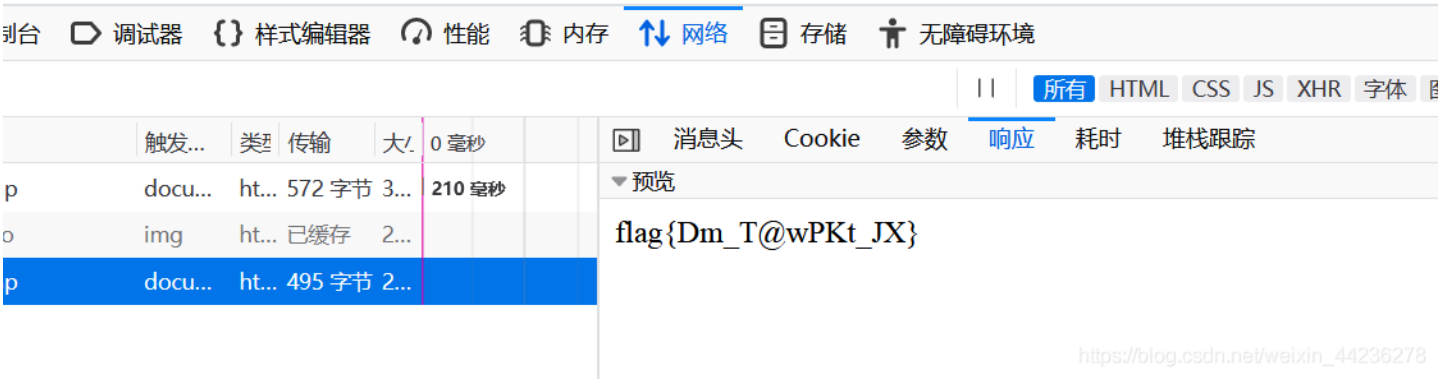


图书馆查询系统

id	书名	简介
3	《flag》	flag{eI_G65Dz8_hn}

ip欺骗（Web）

网络重新加载，编辑消息头添加X-Forwarded-For:127.0.0.1然后重新发送



cookies欺骗（Web）

修改cookies的值为admin，重新刷新网页即可

302跳转（Web）

打开页面点击flag会立即跳转到另一个界面，会显示已经错过了flag。
根据题目，这里是有关302重定向的解释：

> 302重定向又称之为暂时性转移(Temporarily Moved)，英文名称：302 redirect。
> 也被认为是暂时重定向（temporary
> redirect），一条对网站浏览器的指令来显示浏览器被要求显示的不同的URL，当一个网页经历过短期的URL的变化时使用。一个暂时重定向是一种服务器端的重定向，能够被搜索引擎蜘蛛正确地处理。

想要获得flag，就必须让网页不能进行重定向，这里使用的是curl命令。
注意这里访问的网址是在控制台里获得提示的网址

```
C:\Users\24366>curl http://47.98.139.42:8083/redirect.php
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>redirect</title>
</head>
<body>
<!-- flag{m81_J2xK!_AC}-->
</body>
</html>
```

下面是有关HTTP状态码的汇总：

HTTP状态码 进入词条

- 100 Continue
- 101 Switching Protocols
- 102 Processing

2 成功

- 200 OK
- 201 Created
- 202 Accepted
- 203 Non-Authoritative Information
- 204 No Content
- 205 Reset Content
- 206 Partial Content
- 207 Multi-Status

3 重定向

- 300 Multiple Choices
- 301 Moved Permanently
- 302 Move Temporarily
- 304 Not Modified
- 305 Use Proxy
- 306 Switch Proxy
- 307 Temporary Redirect

4 请求错误

- 400 Bad Request
- 401 Unauthorized
- 402 Payment Required
- 403 Forbidden
- 404 Not Found
- 405 Method Not Allowed
- 406 Not Acceptable
- 407 Proxy Authentication Required
- 408 Request Timeout
- 409 Conflict
- 410 Gone
- 411 Length Required
- 413 Request Entity Too Large
- 414 Request-URI Too Long
- 415 Unsupported Media Type
- 416 Requested Range Not Satisfiable
- 417 Expectation Failed
- 418 I'm a teapot
- 421 Too Many Connections
- 422 Unprocessable Entity
- 423 Locked
- 424 Failed Dependency
- 425 Too Early
- 426 Upgrade Required
- 449 Retry With

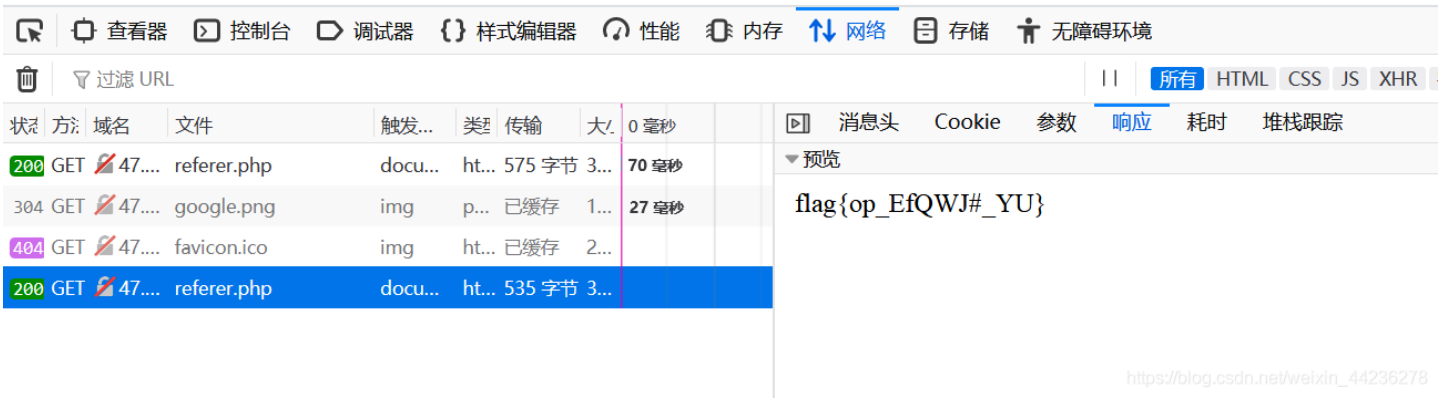
5 服务器错误

- 500 Internal Server Error
- 501 Not Implemented
- 502 Bad Gateway
- 503 Service Unavailable
- 504 Gateway Timeout
- 505 HTTP Version Not Supported
- 506 Variant Also Negotiates
- 507 Insufficient Storage
- 509 Bandwidth Limit Exceeded
- 510 Not Extended
- 600 Unparseable Response Headers

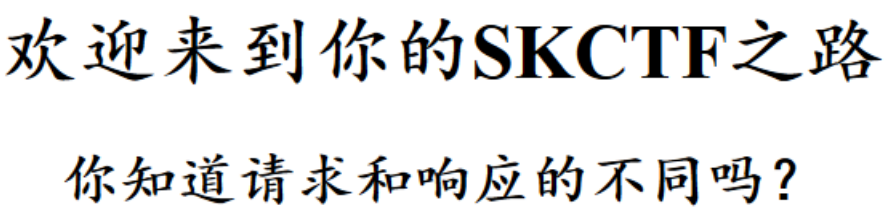
referer（Web）

编辑消息头添加`referer:https://www.google.com`，然后重新发送即可

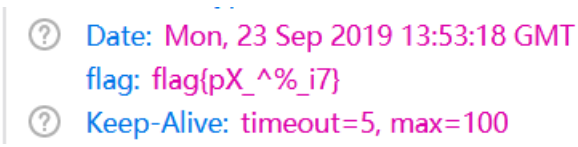
你知道谷歌搜索的网址吗？



HTTP Response头（Web）



控制台里消息头里直接查看到flag



签到（MISC）

直接base64解码拿到flag

Vegetable（MISC）

Vegetable

188

I good Vegetable a!!

Unlock Hint for 50 points

Vegetable.jpg

Flag

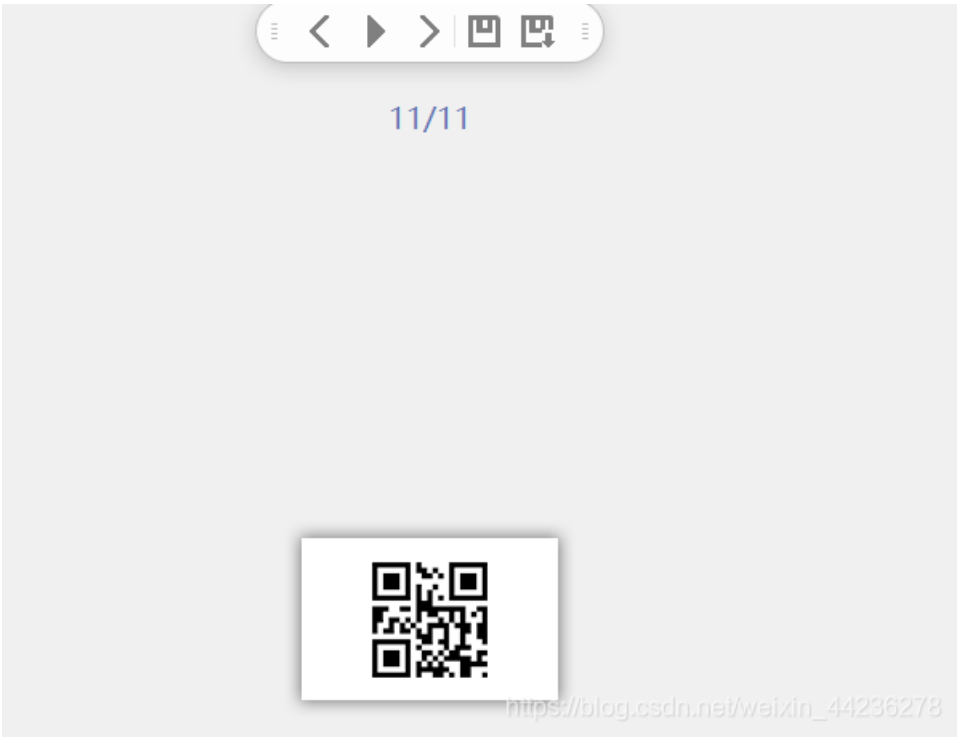
Submit

拿到一张图片

用记事本格式打开最后可以发现flag

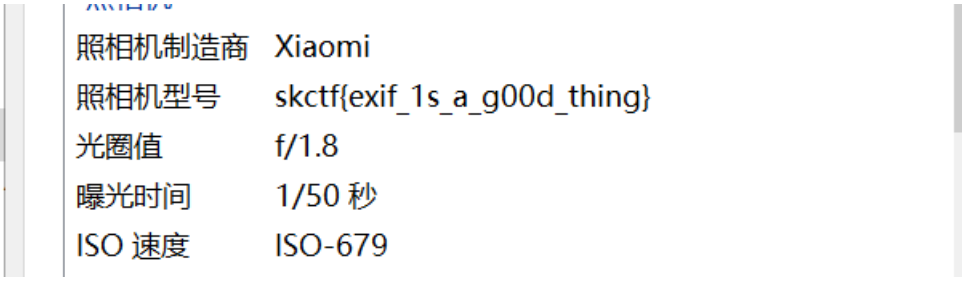
一脸懵逼（MISC）

下载附件拿到一张gif图片，得到最后一帧会有一张二维码，扫码即得flag



黄岛落日（MISC）

下载附件拿到一张图片，属性查看详细信息发现flag



不幸的江文表姐（MISC）

下载附件会有一个.swp备份文件，用记事本打开会发现一串base64编码，解码即得flag

蛤蛤（MISC）

下载附件是一张没有青蛙手的图片，所以首先想到的就是修改图片高度，使用winhex打开图片，第二行的前四组数代表图片宽度，第五组到第八组数代表图片高度，所以修改高度和宽度一样保存文件即可

无字天书（MISC）

下载附件是一个docx文档，打开以后什么文字都没有，然后用记事本打开，发现有很多.xml提示，然后尝试把.docx后缀修改成.zip文件，然后再打开会发现很多文件夹，依次查找会发现flag

```
:w15:chartTrackingRefBased/>
:w15:docId w15:val="{507DABFB-D787-4167-B5CD-7B151B3BA2B3}"/>
settings>
```

Vigenère（Crypto）

Vigenère

188

- ksoiqwmtruly
- skctf
- flag格式:flag{xxxxxxx}

Flag

Submit

根据提示是维吉尼亚编码，密钥是skctf

ksoiqwmtruly

密钥 skctf 加密 解密

simplecrypto

I love bacon！（Crypto）

I love bacon!

194

Bacon： feefe efffe eeeff eefee efeff efeee eeefe efeee efffe fefee feefe

flag格式: flag{xxxxx}

Flag

Submit

根据培根密码的加密规则，e对应a，f对应b解码即可

A/a	aaaaa	H/h	aabbb	O/o	abbba	V/v	babab
B/b	aaaab	I/i	abaaa	P/p	abbbb	W/w	babba
C/c	aaaba	J/j	abaab	Q/q	baaaa	X/x	babbb
D/d	aaabb	K/k	ababa	R/r	baaab	Y/y	bbaaa
E/e	aabaa	L/l	ababb	S/s	baaba	Z/z	bbaab
F/f	aabab	M/m	abbaa	T/t	baabb		
G/g	aabba	N/n	abbab	U/u	babaa		

情报（Crypto）

情报

300

一位知名的博士被黑帮组织抓住了。警方全力营救，还派遣了卧底打入黑帮内部。就在卧底刚获取到情报后，他被人发现了，他冒死传递出一份情报（见附件）和一张纸条，纸条被血浸湿，隐约可见“4”，“2”，“2”，“4”，几个数字，这是什么意思呢？警长看着纸条陷入沉思.... 提示：flag格式：flag{}

code.txt

Flag

Submit

下载附件得到一串编码 `SlZERUlWU05MSktFRVRDQ0pCRFUyV1NETEJEVk1WU1dLVkxVR1MyTkxKSlVLVFpTSVJHVVlRSzJJVktUTVRDQ0pNMlVVUlpVSzVKVkVTQ1ZHWklUMlBKNUhVPT09PT09`

根据题目的提示，其实就是base64解密一次，base32解密两次,base64再解密一次就可以拿到flag

编码 base64　　字符集 utf8(unicode编码)

编 码　　解

he_is_under_the_bridge