

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[CTF 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

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

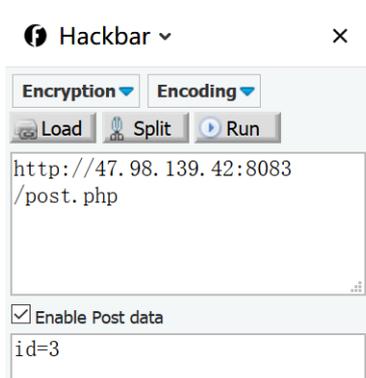
图书馆查询系统

id	书名	简介
3	《flag》	flag{congratulations_succeed}

https://blog.csdn.net/weixin_44236278

post (Web)

```
<div align="center">
  <table border="1">
    <!--尝试post方法请求id=3-->
  </div>
```



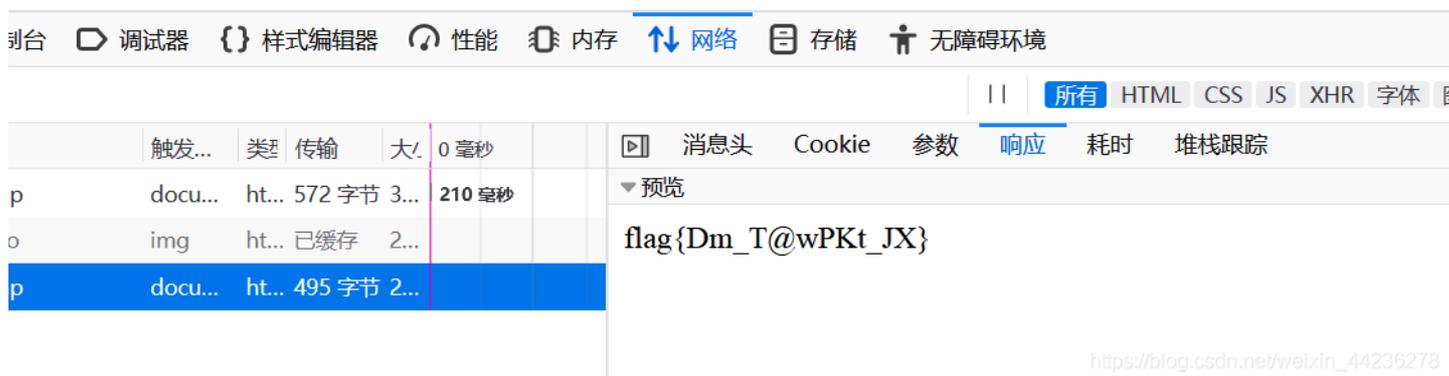
图书馆查询系统

id	书名	简介
3	《flag》	flag{eI_G65Dz8_lm}

https://blog.csdn.net/weixin_44236278

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



https://blog.csdn.net/weixin_44236278

cookies欺骗 (Web)

修改cookies的值为admin，重新刷新网页即可



名称	域名	路径	过期时间	最后访问	值	Http
username	47.98.139.42	/	会话	Mon, 23 Sep 2019 13:34:40 GMT	admin	false

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>
```

https://blog.csdn.net/weixin_44236278

下面是有关HTTP状态码的汇总：

HTTP状态码

[进入词条](#)

<ul style="list-style-type: none">100 Continue101 Switching Protocols102 Processing <h3>2 成功</h3> <ul style="list-style-type: none">200 OK201 Created202 Accepted203 Non-Authoritative Information204 No Content205 Reset Content206 Partial Content207 Multi-Status <h3>3 重定向</h3> <ul style="list-style-type: none">300 Multiple Choices301 Moved Permanently302 Move Temporarily	<ul style="list-style-type: none">304 Not Modified305 Use Proxy306 Switch Proxy307 Temporary Redirect <h3>4 请求错误</h3> <ul style="list-style-type: none">400 Bad Request401 Unauthorized402 Payment Required403 Forbidden404 Not Found405 Method Not Allowed406 Not Acceptable407 Proxy Authentication Required408 Request Timeout409 Conflict410 Gone411 Length Required	<ul style="list-style-type: none">413 Request Entity Too Large414 Request-URI Too Long415 Unsupported Media Type416 Requested Range Not Satisfiable417 Expectation Failed418 I'm a teapot421 Too Many Connections422 Unprocessable Entity423 Locked424 Failed Dependency425 Too Early426 Upgrade Required449 Retry With	<h3>5 服务器错误</h3> <ul style="list-style-type: none">500 Internal Server Error501 Not Implemented502 Bad Gateway503 Service Unavailable504 Gateway Timeout505 HTTP Version Not Supported506 Variant Also Negotiates507 Insufficient Storage509 Bandwidth Limit Exceeded510 Not Extended600 Unparseable Response Headers
--	--	---	---

https://blog.csdn.net/weixin_44236278

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？

查看器 控制台 调试器 样式编辑器 性能 内存 网络 存储 无障碍环境

过滤 URL

状态	方法	域名	文件	触发...	类型	传输	大小	耗时
200	GET	47...	referer.php	docu...	ht...	575 字节	3...	70 毫秒
304	GET	47...	google.png	img	p...	已缓存	1...	27 毫秒
404	GET	47...	favicon.ico	img	ht...	已缓存	2...	
200	GET	47...	referer.php	docu...	ht...	535 字节	3...	

消息头 Cookie 参数 响应 耗时 堆栈跟踪

预览

```
flag{op_EfQWJ#_YU}
```

https://blog.csdn.net/weixin_44236278

欢迎来到你的SKCTF之路

你知道请求和响应的不同吗?

控制台里消息头里直接查看到flag

- ① Date: Mon, 23 Sep 2019 13:53:18 GMT
- flag: flag{pX_^%_i7}
- ① Keep-Alive: timeout=5, max=100

签到 (MISC)

Challenge

24 Solves



签到

100

c2tjdGZ7YmFzZTY0X2lzX3BvcHVzYXlhfQ== 解出这段代码，这将是你的入坑的第一步。提示：是网络上最常见的用于传输8Bit字节码的编码方式之一，一种基于64个可打印字符来表示二进制数据的方法。

Flag

Submit

https://blog.csdn.net/weixin_44236278

直接base64解码拿到flag

Vegetable (MISC)

Challenge

6 Solves



Vegetable

188

I good Vegetable a!!

Unlock Hint for 50 points

📄 Vegetable.jpg

Flag

Submit

https://blog.csdn.net/weixin_44236278

拿到一张图片



我好菜啊

SVIP 高清3D重置版

https://blog.csdn.net/weixin_44236278

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

照相机制造商	Xiaomi
照相机型号	skctf{exif_1s_a_g00d_thing}
光圈值	f/1.8
曝光时间	1/50 秒
ISO 速度	ISO-679

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

Vigenère (Crypto)

Vigenère

188

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

Flag

Submit

https://blog.csdn.net/weixin_44236278

根据提示是维吉尼亚编码，密钥是skctf

ksoiqwmtruly

密钥

simplecrypto

https://blog.csdn.net/weixin_44236278

I love bacon! (Crypto)

I love bacon!

194

Bacon: feefe effe eeef eefee eeff efee eeefe efee effe
feefe feefe

flag格式: flag{xxxxx}

Flag

Submit

https://blog.csdn.net/weixin_44236278

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		

https://blog.csdn.net/weixin_44236278

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

https://blog.csdn.net/weixin_44236278

下载附件得到一串编

码 `S1ZERU1WU05MSktFRVRDQ0pCRFUyV1NETEJEVklWU1dLVkxVR1MyTkxKS1VLVFPtSVJHVW1RSzJJVktUTVRDQ0pNM1VVU1pVSzVKVkvTQ1ZHWkLUM1BKNUhVPT09PT09`

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

https://blog.csdn.net/weixin_44236278