

# CTF基础题

原创

[Mars\\_boom](#) 于 2020-10-21 11:26:32 发布 2613 收藏 30

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/Mars\\_boom/article/details/109133100](https://blog.csdn.net/Mars_boom/article/details/109133100)

版权

## web基础题

攻防世界

bugku-CTF

### 攻防世界

1、题目描述：X老师让小宁同学查看一个网页的源代码，但小宁同学发现鼠标右键好像不管用了。

题目场景：<http://220.249.52.133:48687/>

答案：按F12/fn+F12打开源代码，查看到flag

2、题目描述：X老师告诉小宁同学HTTP通常使用两种请求方法，你知道是哪两种吗？

题目场景：<http://220.249.52.133:48092>

请用GET方式提交一个名为a,值为1的变量

请再以POST方式随便提交一个名为b,值为2的变量

cyberpeace{14a25599fdc184f1b0f845e924c84ce9}

get方式可以在网页直接加上?a=1。

post需要用ackbar将b=2传到网页。

3、题目描述：X老师上课讲了Robots协议，小宁同学却上课打了瞌睡，赶紧来教教小宁Robots协议是什么吧。

题目场景： <http://220.249.52.133:36226>

答案：robots协议，即爬虫协议，网站可以防止爬虫爬取不愿意被爬取内容。

robots.txt是网站根目录下的文本文，robots.txt必须放置在一个站点的根目录下，而且文件名必须全部小写。如果搜索引擎爬虫要访问的网站地址是<http://www.w3.org/>，那么robots.txt文件必须能够通过<http://www.w3.org/robots.txt>打开并看到里面的内容。(1)User-agent:用于描述搜索引擎爬虫的名字。在Robots.txt文件中，如果有多条User-agent记录，说明有多个搜索引擎爬虫会受到该协议的限制，对该文件来说，至少要有一条User-agent记录。如果该项的值设为木，则该协议对任何搜索引擎爬虫均有效，在Robots.txt文件中，“User-agent:”这样的记录只能有一条。(2)Disallow:用于描述不希望被访问到的一个URL。这个URL可以是一条完整的路径，也可以是部分路径，任何以Disallow开头的URL均不会被Robot访问到。

url末尾加上/robots.txt可查看不能访问的爬虫以及网页。

```
User-agent: *
Disallow:
Disallow: flag_1s_h3re.php
```

将Disallow的网页 `flag_1s_h3re.php` 输入在url末尾（进行文件访问）得到flag

`cyberpeace{39d2d1bcd23444c4c7ae24ea405b1dae}`

4、题目描述：X老师今天上课讲了前端知识，然后给大家一个不能按的按钮，小宁惊奇地发现这个按钮按不下去，到底怎么才能按下去呢？

题目场景： <http://220.249.52.133:57420>

分析一下源代码，我们看到下面的按钮是一个disabled的，将disabled删掉后，按钮可以按下并且得到flag

`cyberpeace{9bbd7d73e73ca9c01cf029d4450e5e29}`

5、题目描述：X老师告诉小宁他在cookie里放了东西，小宁疑惑地想：‘这是夹心饼干的意思吗？’

题目场景： <http://220.249.52.133:52616>

Cookie是由服务器端生成，发送给User-Agent,浏览器会将Cookie的key/value保存到某个目录下的文本文件内，下次请求同一网站时就发送该Cookie给服务器。

打开看到，你知道什么是cookie吗？

指引我们从fn/f12中找到cookie，从network的Doc中可以看到cookie，得到

Request Cookies  show filtered out request cookies

Name	Value	D...	Path	Ex...	Size	Ht...	Se...	Sa...
look-here	cookie.php	22...	/	Se...	19			

将cookie.php放入url中（进行文件访问）得到新页面

See the http response

从Doc中可以找到response，里面出现了flag

`cyberpeace{ce7d0987eb76d6c33127f64b47ed1662}`

6、题目描述：X老师忘记删除备份文件，他派小宁同学去把备份文件找出来,一起来帮小宁同学吧！

题目场景： <http://220.249.52.133:30627>

在考察对index.php文件的备份文件名怎么显示。即index.php.bak加在末尾得到一个下载包，用记事本打开得到源代码以及flag

`Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}`

7、题目描述：小宁写了一个登陆验证页面，随手就设了一个密码。

题目场景： <http://220.249.52.133:46768>

孩子尽力了，只能猜到username写admin

密码可能要爆破吧，bp还不太会。。。

8、题目描述：小宁听说php是最好的语言,于是她简单学习之后写了几行php代码。

题目场景： <http://220.249.52.133:41029>

分析PHP代码可知需要`a==0`又要`a!=0`

那么就需要`a`是一个字符串`admin`,

`is_number`只要数字后面加上`%00`就可以当作空格,成为字符串。

得到

`Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}`

9、题目描述：小宁发现了一个网页,但却一直输不对密码。(Flag格式为 `Cyberpeace{xxxxxxxx}`)

题目场景： <http://220.249.52.133:52432>

**bugku-CTF**

### 1、GET

http://123.206.87.240:8002/get/


网页内容:

```
what= _GET['what'];  
echo what;if(what=='flag')  
echo 'flag{****}';
```

答案:

url中，有get/分析只要what=flag就能得到flag。那么在url/get/后面加上参数，注意参数？开头&连接。

flag{bugku\_get\_su8kej2en}

 不安全 | 123.206.87.240:8002/get/?what=flag

### 2、POST

http://123.206.87.240:8002/post/

网页内容:

```
what= _POST['what'];  
echo what;if(what=='flag')  
echo 'flag{****}';
```

答案: hacker bar或者burp可以得到接收的请求，加入条件what=flag可得答案。

flag{bugku\_get\_ssseint67se}



The screenshot shows a web proxy tool interface. On the left, there are three buttons: 'Load URL', 'Split URL', and 'Execute'. The main area contains a text input field with the URL 'http://123.206.87.240:8002/post/'. Below the URL field, there are four checkboxes: 'Post data' (checked), 'Referer', 'User Agent', and 'Cookies'. To the right of these checkboxes is a 'Clear All' button. At the bottom, there is a large text area containing the text 'what=flag'. In the bottom right corner, there is a small URL: 'https://blog.csdn.net/Mars\_brother'.

### 3、web2

http://123.206.87.240:8002/web2/

flag就在源码中。

#### 4、计算

http://123.206.87.240:8002/yanzhengma/

**34+14=?**

计算后输入发现只能输入一位数，打开源码看看，

```
▼<body>  
  <span id="code" class="code" style="background: rgb(38, 82, 163); color: rgb(249, 176, 225);">34+14=?</span>  
  ... <input type="text" class="input" maxlength="1" > == $0
```

发现这个框设置最长为1，修改为2试试。

可以输入两位数字了，验证得到flag

flag{CTF-bugku-0032}

#### 5、http://123.206.87.240:8002/baopo/?yes

答案：

爆破问题用burp进行密码的试验，从10000-99999。

未完待续。。。