

攻防世界web新手练习区writeup（上）

原创

守护者  于 2019-11-26 20:13:34 发布  332  收藏

分类专栏: [CTF](#) 文章标签: [XCTF Writeup](#)

守护者安全 (www.zhaosimeng.cn)

本文链接: https://blog.csdn.net/weixin_42721957/article/details/103263479

版权



[CTF 专栏收录该内容](#)

5 篇文章 0 订阅

订阅专栏

第一题: view_source

view_source

 27 最佳Writeup由 [Healer_aptx](#) • [Anchorite](#) 提供

难度系数:  1.0

题目来源: [Cyberpeace-n3k0](#)

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: [点击获取在线场景](#)

题目附件: 暂无

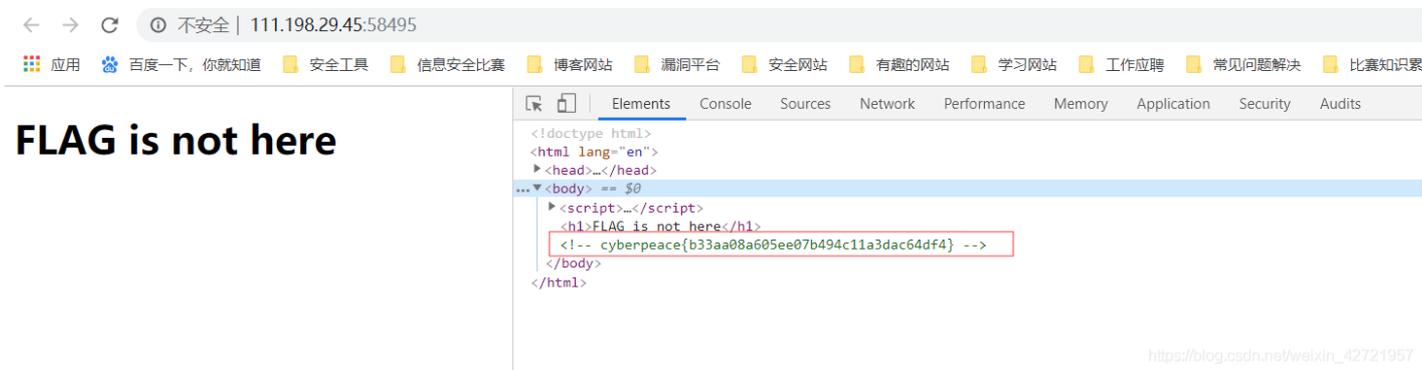
https://blog.csdn.net/weixin_42721957

顾名思义就是查看源码

FLAG is not here

https://blog.csdn.net/weixin_42721957

打开链接发现确实如题目描述那样鼠标右键不能用了。所以通过快捷键Ctrl +shift + i 查看源代码。发现flag。



https://blog.csdn.net/weixin_42721957

第二题: get_post

get_post

👍 16 最佳Writeup由神秘人·孔雀翎提供

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

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?

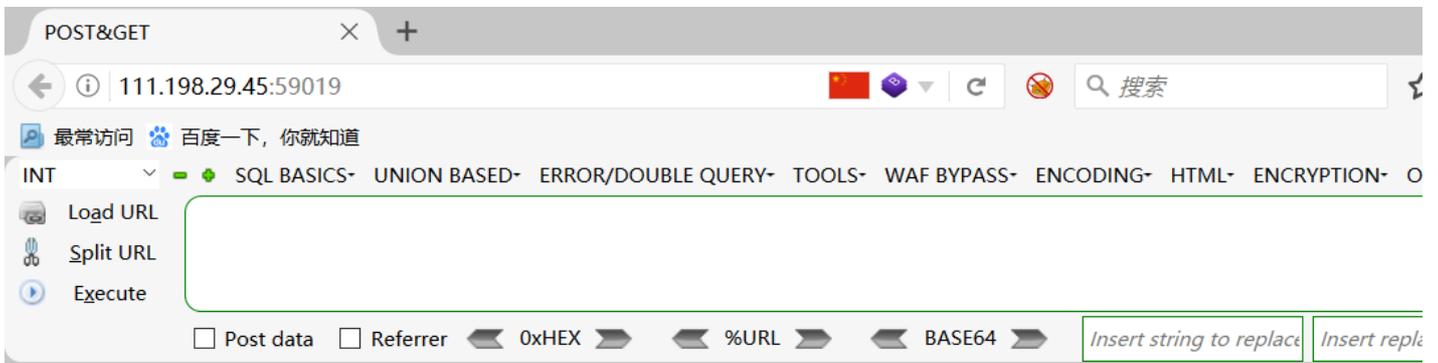
题目场景: [点击获取在线场景](#)

题目附件: 暂无

https://blog.csdn.net/weixin_42721957

HTTP通常使用的两种请求方式就是get和post

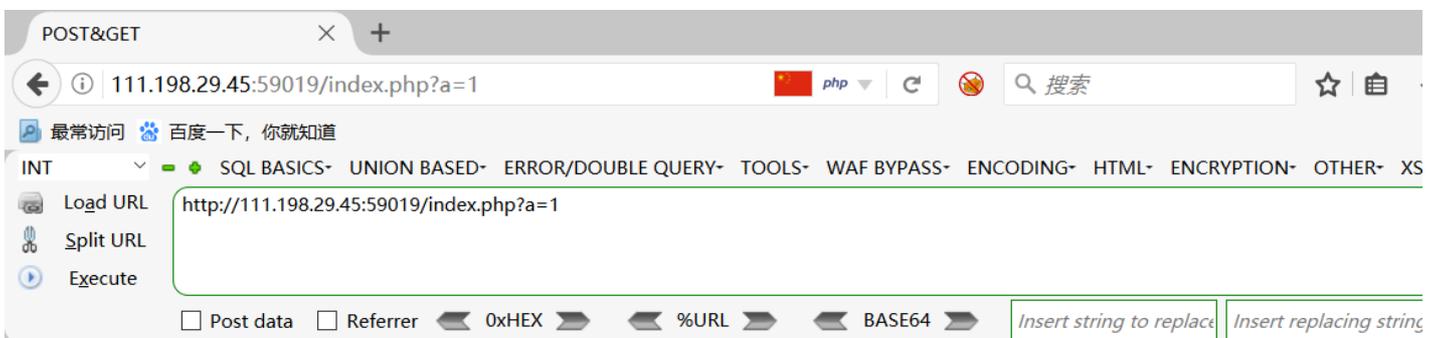
打开链接果然跟这个有关



请用GET方式提交一个名为a,值为1的变量

https://blog.csdn.net/weixin_42721957

既然要用GET方式，就在url后面构造参数a并赋值为1试试吧

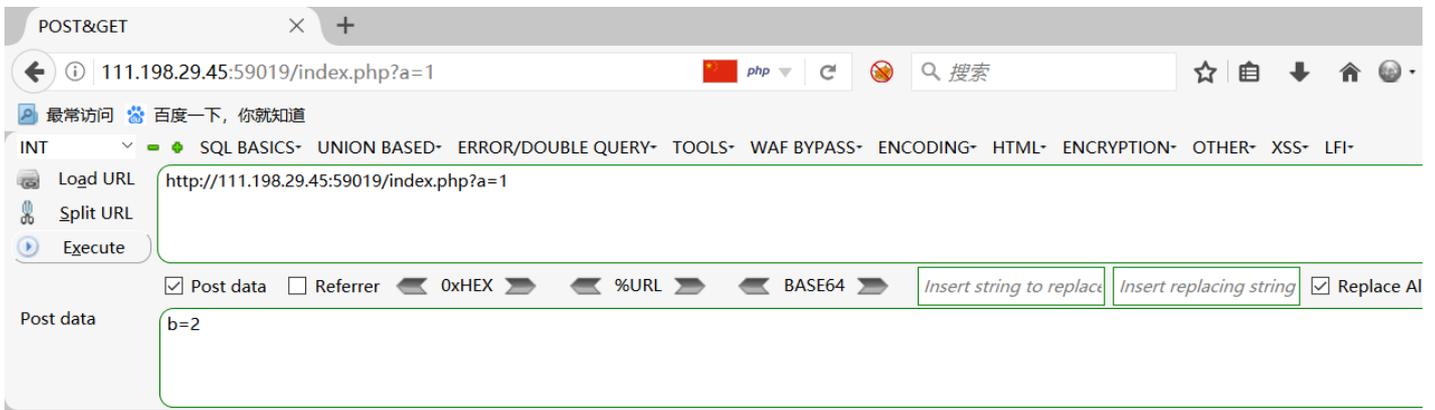


请用GET方式提交一个名为a,值为1的变量

请再以POST方式随便提交一个名为b,值为2的变量

https://blog.csdn.net/weixin_42721957

就知道套路没这么简单，这里要求还要post一个值为2的b参数。那么就直接用hackbar插件吧。



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{23a992726cda197f7a3cb6c4632d27b9}

https://blog.csdn.net/weixin_42721957

第三题：robots

robots 👍 21 最佳Writeup由MOLLMY提供

难度系数: ★ 1.0

题目来源: [Cyberpeace-n3k0](#)

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: [点击获取在线场景](#)

题目附件: 暂无

https://blog.csdn.net/weixin_42721957

题目既然提到了robots协议,那么就让我们百度一下吧

robots协议

 编辑

📖 本词条由“科普中国”科学百科词条编写与应用工作项目 审核。

robots协议也叫**robots.txt**（统一小写）是一种存放于**网站根目录**下的**ASCII编码的文本文件**，它通常告诉**网络搜索引擎**的**漫游器**（又称**网络蜘蛛**），此网站中的哪些内容是不应被搜索引擎的漫游器获取的，哪些是可以被漫游器获取的。因为一些系统中的URL是大小写敏感的，所以robots.txt的文件名应统一为小写。robots.txt应放置于网站的根目录下。如果想单独定义搜索引擎的漫游器访问子目录时的行为，那么可以将自定的设置合并到根目录下的robots.txt，或者使用**robots元数据**（Metadata，又称元数据）。

robots协议并不是一个规范，而只是约定俗成的，所以并不能保证网站的隐私。

中文名 robots协议

外文名 robots.txt

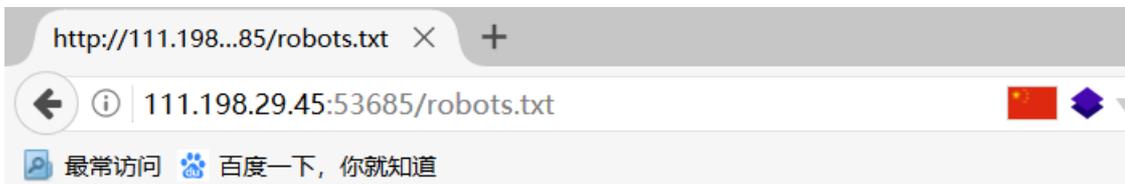
https://blog.csdn.net/weixin_42721957

既然有了初步的了解，就先打开链接看看吧



https://blog.csdn.net/weixin_42721957

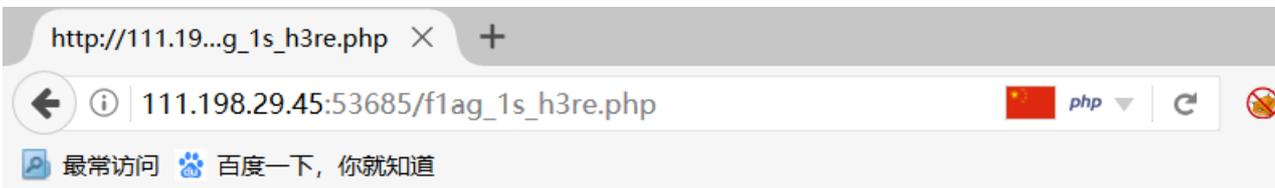
什么也没有。考虑到题目刚才说的robots协议，我们知道网站根目录下还有一个robotx.txt文件记录着某些信息，让我们看看



```
User-agent: *  
Disallow:  
Disallow: flag_ls_h3re.php
```

https://blog.csdn.net/weixin_42721957

果然，这里记录了一个可以的php文件，我们访问一下试试能不能看到flag



cyberpeace{19599b58cc1adb25bae8b841b12fd571}

https://blog.csdn.net/weixin_42721957

第四题: backup

backup 11 最佳Writeup由话求·樱宁提供

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

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: [点击获取在线场景](#)

题目附件: 暂无

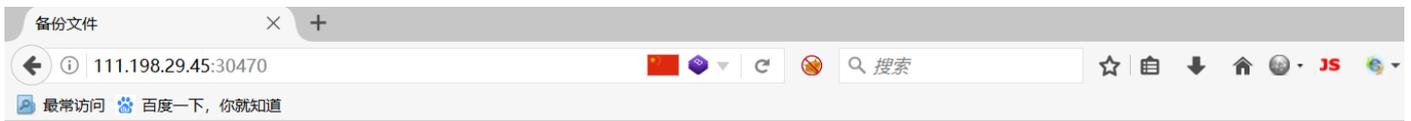
https://blog.csdn.net/weixin_42721957

这里就要知道一下常见的备份文件知识啦。

常见的备份文件后缀名有:

```
.git  
.svn  
.swp  
.svn  
.  
.  
.bak  
.bash_history
```

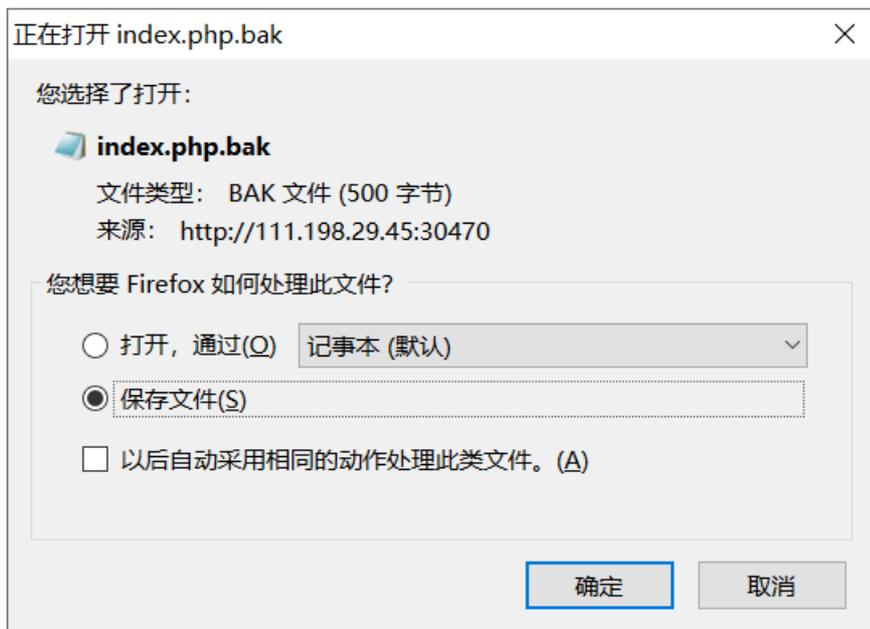
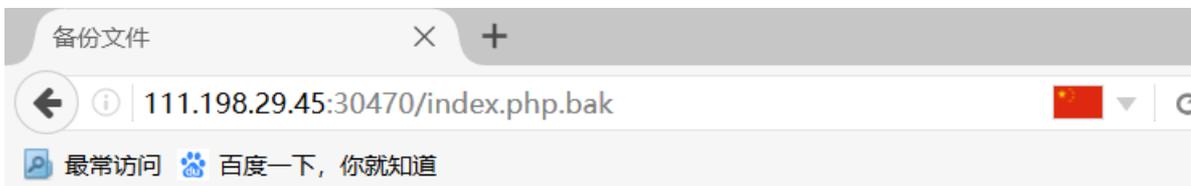
打开链接看看题目



你知道index.php的备份文件名吗？

https://blog.csdn.net/weixin_42721957

根据提示知道，应该是index.php有备份文件，那么根据上面的小常识我们试一试，最后得知.bak是正确的文件名，如下：



https://blog.csdn.net/weixin_42721957

保存文件并打开查看得到flag

```
index.php.bak - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
<html>
<head>
  <meta charset="UTF-8">
  <title>备份文件</title>
  <link
href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css"
rel="stylesheet" />
  <style>
    body{
      margin-left:auto;
      margin-right:auto;
      margin-top:200px;
      width:20em;
    }
  </style>
</head>
<body>
<h3>你知道index.php的备份文件名吗? </h3>
<?php
$flag="Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}"
?>
</body>
</html>
```

第 1 行, 第 1 列 100% Windows (CRLF) UTF-8 42721957

第五题: cookie

cookie

最佳Writeup由神秘人·孔雀翎提供

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

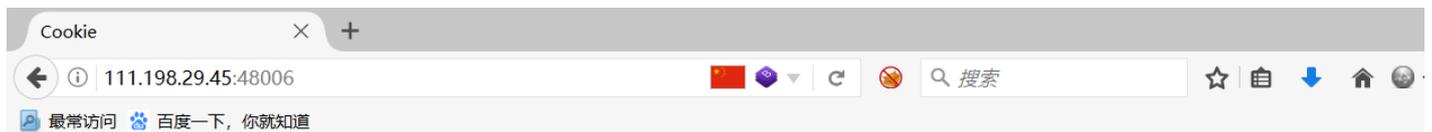
题目描述: X老师告诉小宁他在cookie里放了东西,小宁疑惑地想:‘这是夹心饼干的意思吗?’

题目场景: [点击获取在线场景](#)

题目附件: 暂无

https://blog.csdn.net/weixin_42721957

从提示看应该是关于cookie的考察,那么打开链接看看



你知道什么是cookie吗?

https://blog.csdn.net/weixin_42721957

问我们知不知道cookie,管他呐,不会做的题一律直接上BP抓包先看看再说

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://111.198.29.45:48006

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
GET / HTTP/1.1
Host: 111.198.29.45:48006
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
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: look-here=cookie.php
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

https://blog.csdn.net/weixin_42721957

先放到repeater里面看看反应

Go Cancel < >

Target: http://111.198.29.45:48006

Request

Raw Params Headers Hex

```
SET /cookie.php HTTP/1.1
Host: 111.198.29.45:48006
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
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: look-here=cookie.php
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

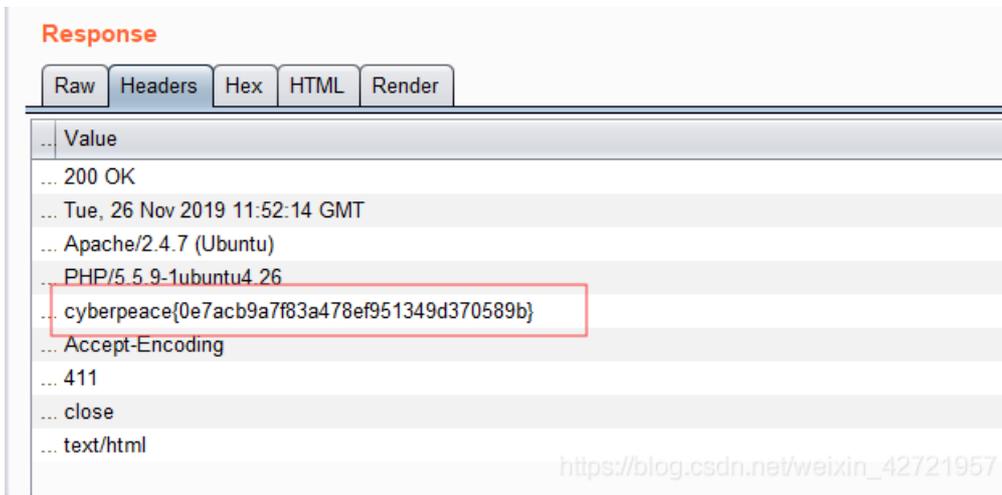
Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Tue, 26 Nov 2019 11:52:14 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
flag: cyberpeace[0e7acb9a7f33a478ef951349d370589b]
Vary: Accept-Encoding
Content-Length: 411
Connection: close
Content-Type: text/html

<html>
<head>
  <meta charset="UTF-8">
  <title>Cookie</title>
  <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />
  <style>
    body{
      margin-left:auto;
      margin-right:auto;
      margin-TOP:200PX;
      width:20em;
    }
  </style>
</head>
<body>
  <h3>See the http response</h3>
</body>
</html>
```

https://blog.csdn.net/weixin_42721957

返回页面说看看http的response



so easy 。X老师的饼干果然是夹心的。

第六题：disabled_button

disabled_button 👍 8 最佳Writeup由沐一清提供

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

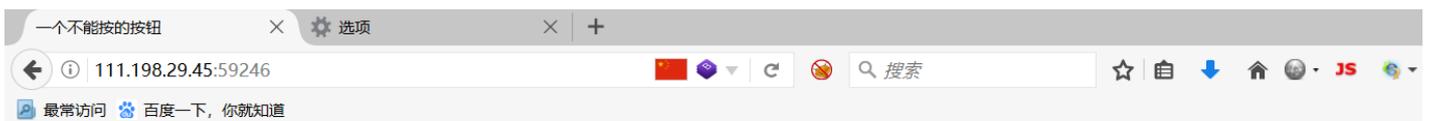
题目描述: X老师今天上课讲了前端知识, 然后给大家一个不能按的按钮, 小宁惊奇地发现这个按钮按不下去, 到底怎么才能按下去呢?

题目场景: 点击获取在线场景

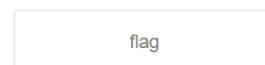
题目附件: 暂无

https://blog.csdn.net/weixin_42721957

打开链接发现按钮果然不能按



一个不能按的按钮



https://blog.csdn.net/weixin_42721957

既然说是涉及到前端知识, 那我们先看看源码吧

```
<html>
<head>
<meta charset="UTF-8">
<title>一个不能按的按钮</title>
<link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet">
<style>
body{ margin-left:auto; margin-right:auto; margin-TOP:200PX; width:20em; }
</style>
<style></style>
</head>
<body>
<h3>一个不能按的按钮</h3>
<form action="" method="post">
<input class="btn btn-default" disabled="" style="height:50px;width:200px;" value="flag" name="auth" type="submit">
</form>
</body>
</html>
```

https://blog.csdn.net/weixin_42721957

我说怎么按钮按不下去，原来是disabled在捣乱啊。那就把它踢出去看看

一个不能按的按钮

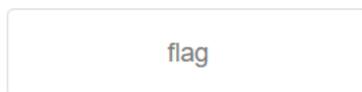


```
<html>
<head>
<meta charset="UTF-8">
<title>一个不能按的按钮</title>
<link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet">
<style>
body{ margin-left:auto; margin-right:auto; margin-TOP:200PX; width:20em; }
</style>
<style></style>
</head>
<body>
<h3>一个不能按的按钮</h3>
<form action="" method="post">
<input class="btn btn-default" style="height:50px;width:200px;" value="flag" name="auth" type="submit">
</form>
</body>
</html>
```

https://blog.csdn.net/weixin_42721957

哈哈，立竿见影。按钮能用啦。点击即可获得flag一枚。

一个不能按的按钮



cyberpeace{062dc99dbffaf3ef46b82e49651a1749}

https://blog.csdn.net/weixin_42721957

剩余writeup请看攻防世界web新手练习区writeup（下）

