攻防世界web新手练习区writeup（上）

原创

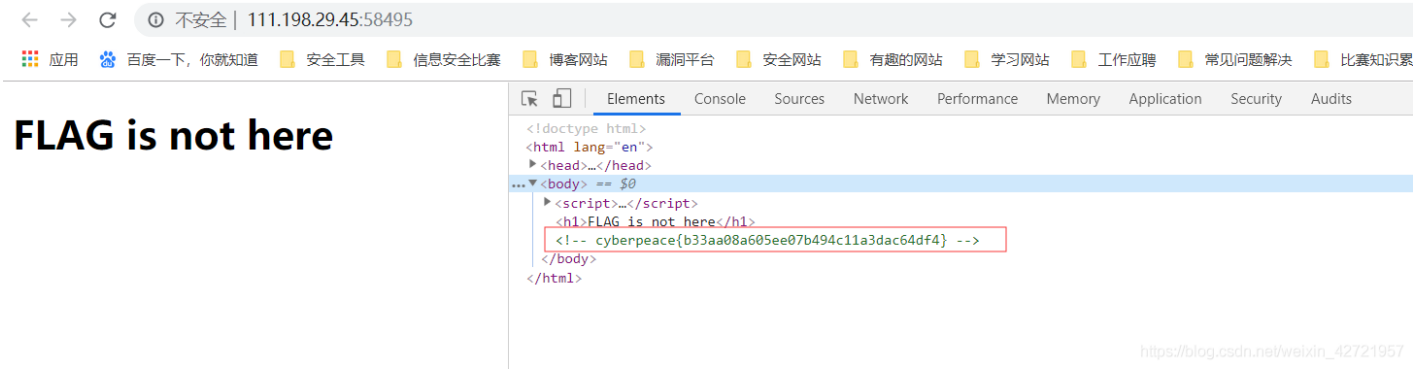
守卫者 于 2019-11-26 20:13:34 发布 332 收藏
分类专栏： CTF 文章标签： XCTF Writeup
守卫者安全（www.zhaosimeng.cn）
本文链接：https://blog.csdn.net/weixin_42721957/article/details/103263479

第一题：view_source

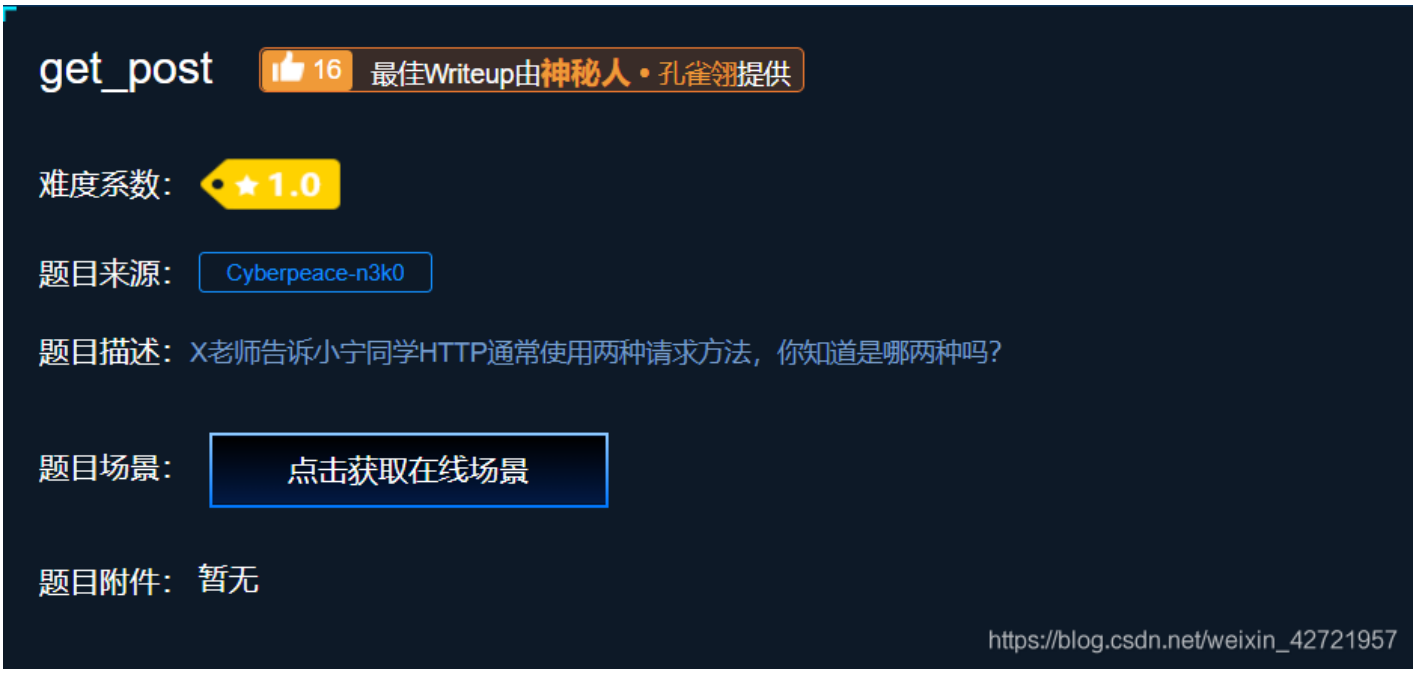
顾名思义就是查看源码

FLAG is not here

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。

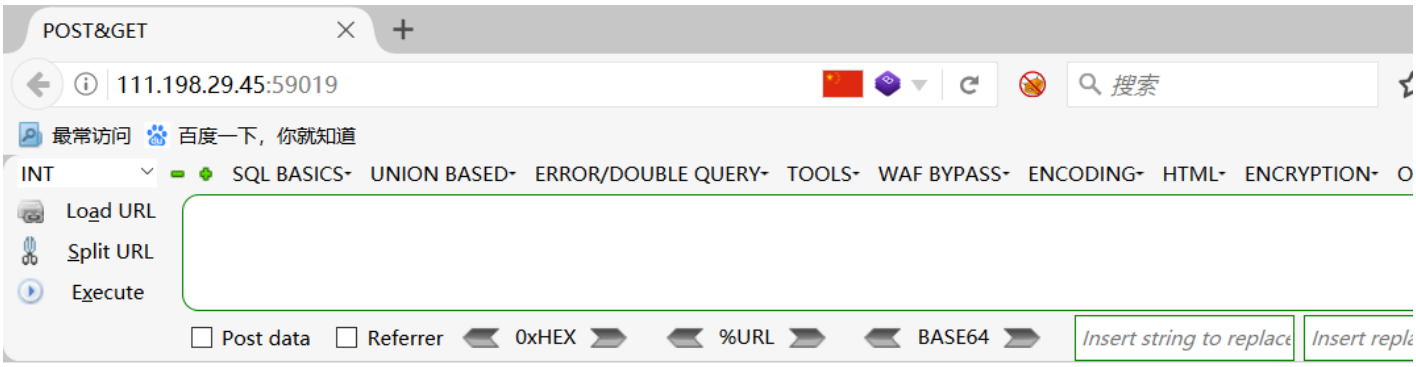


第二题：get_post



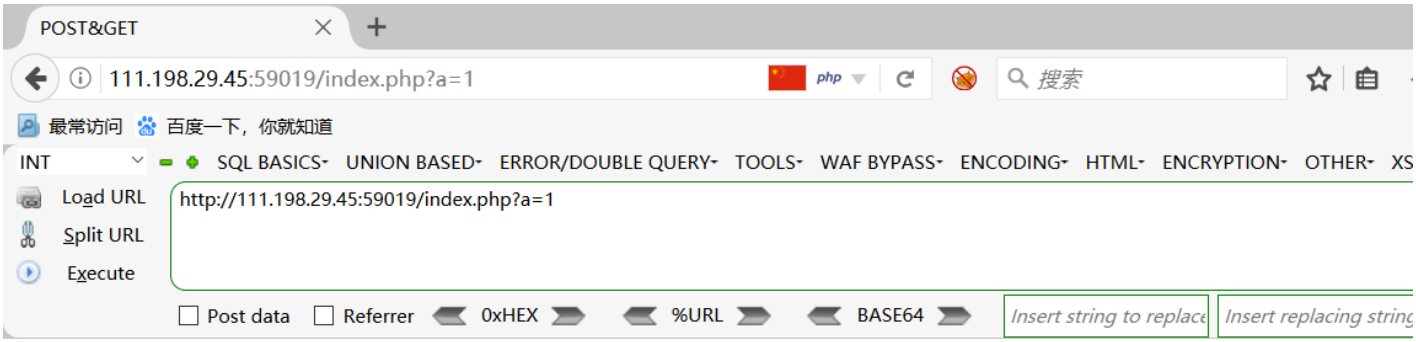
HTTP通常使用的两种请求方式就是get和post

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

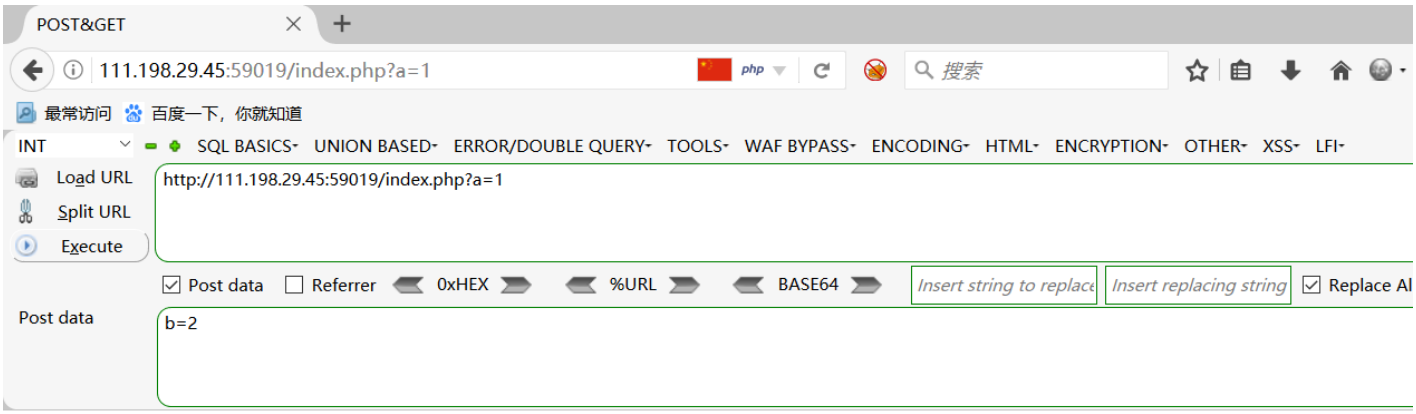
既然要用GET方式，就在url后面构造参数a并赋值为1试试吧



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

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}

第三题：robots

题目既然提到了robots协议，那么就让我们百度一下吧

收藏 517 123

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 。

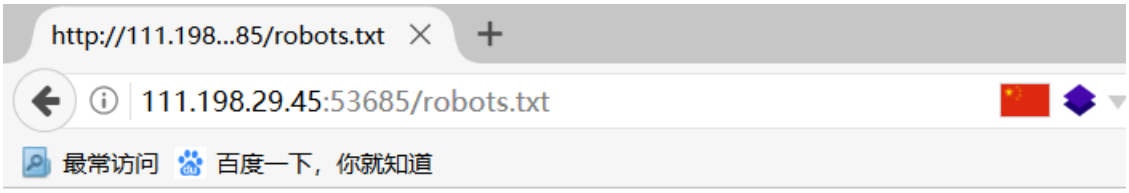
robots协议也叫robots.txt（统一小写）是一种存放于网站根目录下的ASCII编码的文本文件，它通常告诉网络搜索引擎的漫游器（又称网络蜘蛛），此网站中的哪些内容是不应被搜索引擎的漫游器获取的，哪些是可以被漫游器获取的。因为一些系统中的URL是大小写敏感的，所以robots.txt的文件名应统一为小写。robots.txt应放置于网站的根目录下。如果想单独定义搜索引擎的漫游器访问子目录时的行为，那么可以将自定的设置合并到根目录下的robots.txt，或者使用robots元数据（Metadata，又称元数据）。

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

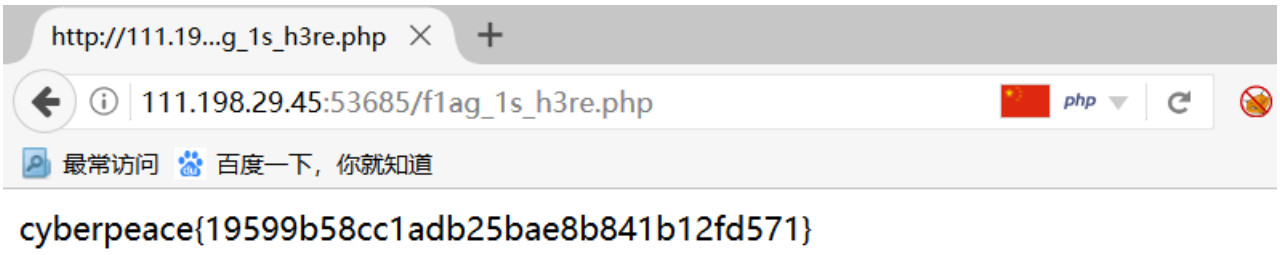
既然有了初步的了解，就先打开链接看看吧

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
```


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}

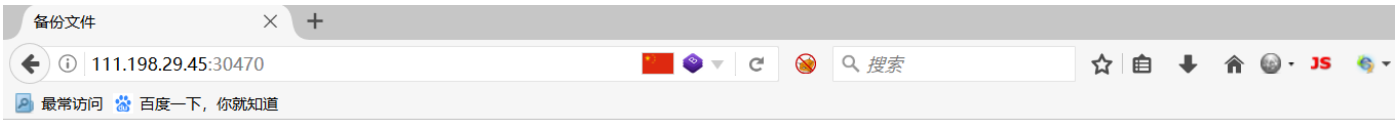
第四题：backup

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：

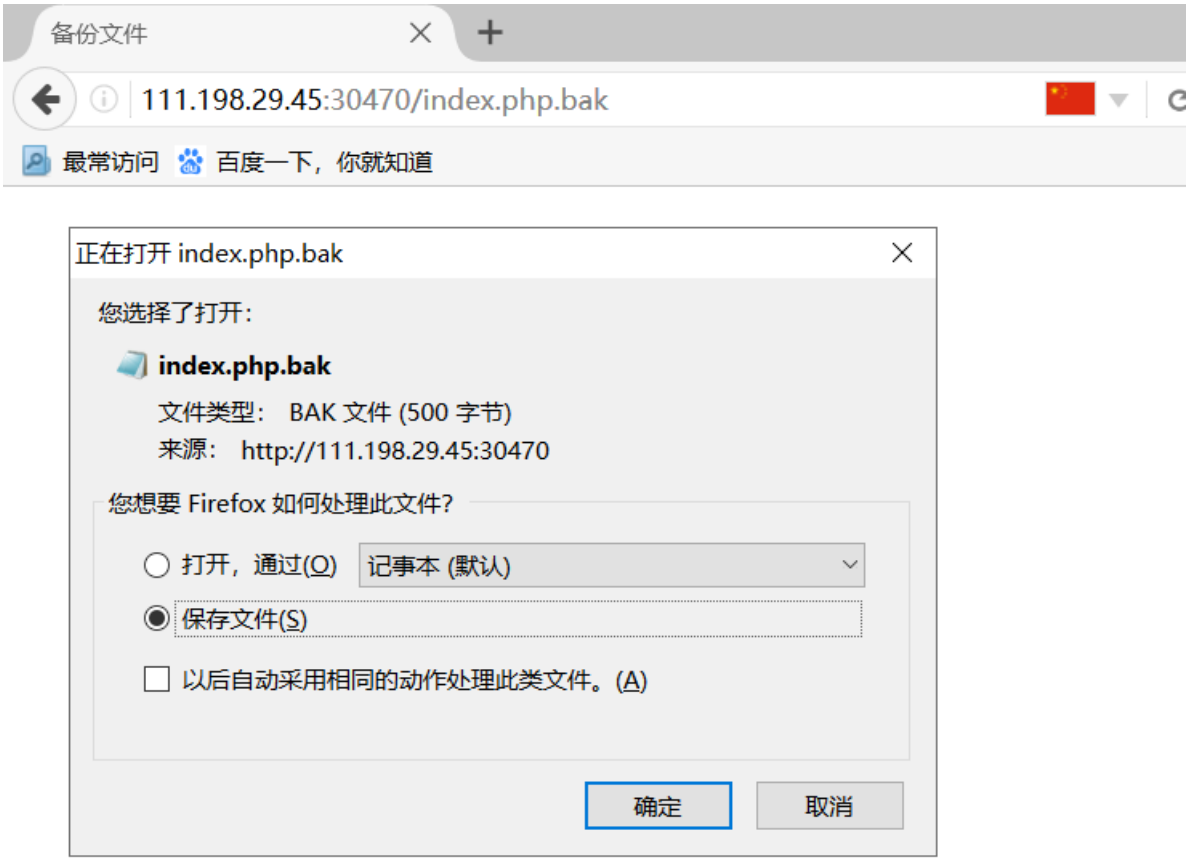
```
.git
.svn
.swp
.svn
.~
.bak
.bash_history
```

打开链接看看题目

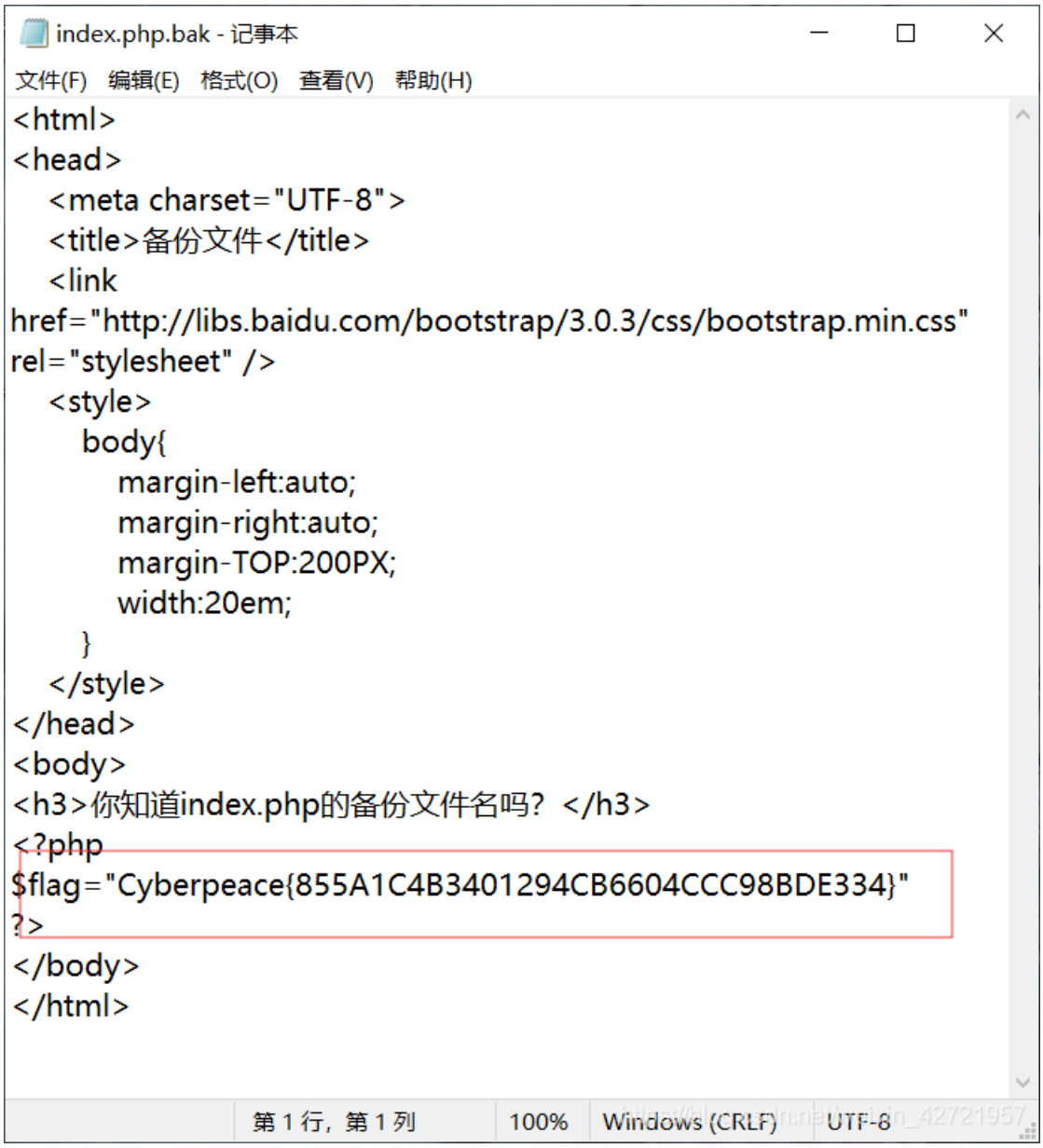


你知道index.php的备份文件名吗?

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：

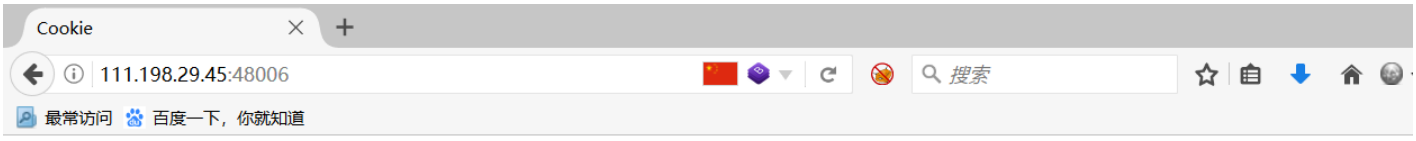


保存文件并打开查看得到flag


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

第五题：cookie

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?

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

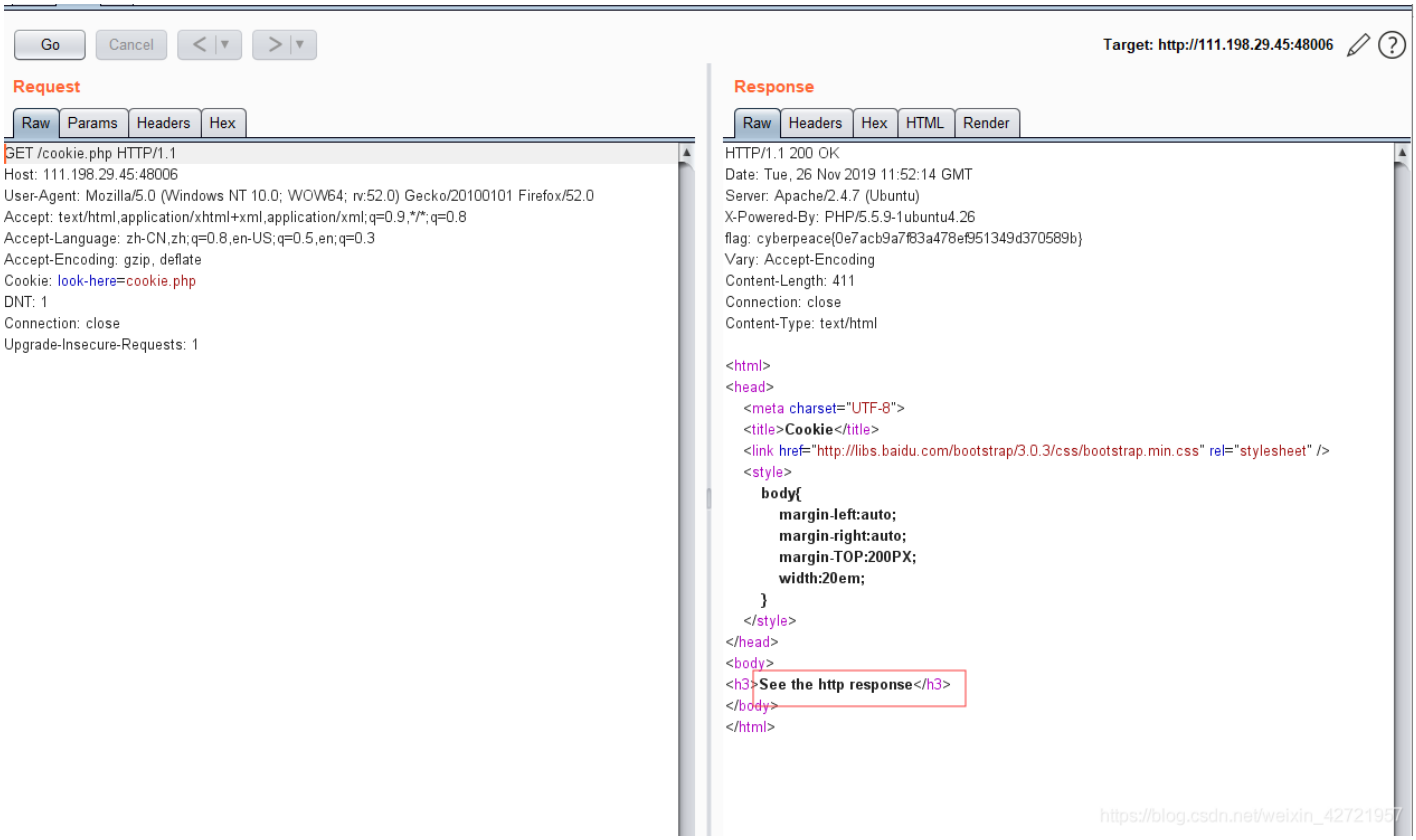
Request to http://111.198.29.45:48006

Forward | Drop | Intercept is on | Action

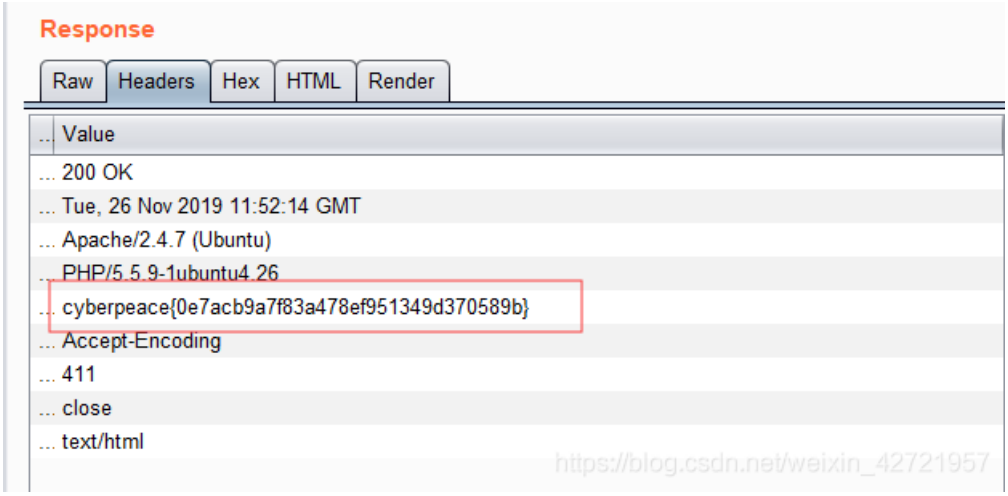
Raw | Params | Headers | Hex

```
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
```


先放到repeater里面看看反应

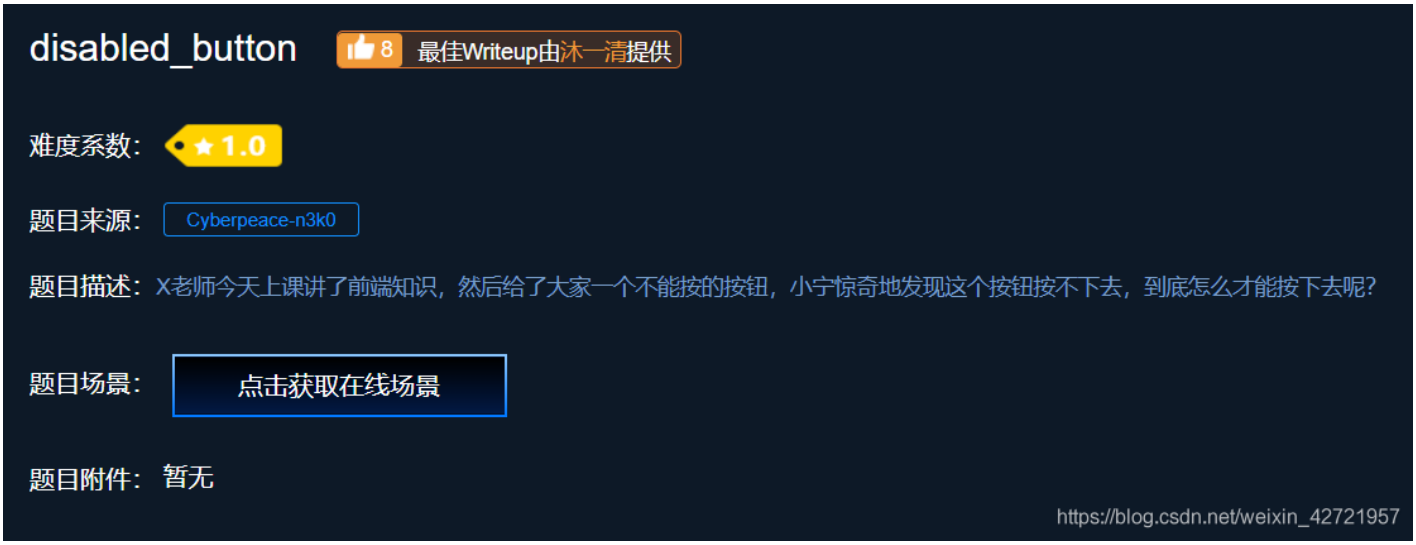


返回页面说看看http的response



so easy 。X老师的饼干果然是夹心的。

第六题：disabled_button



打开链接发现按钮果然不能按

既然说是涉及到前端知识，那我们先看看源码吧

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

哈哈，立竿见影。按钮能用啦。点击即可获得flag一枚。

剩余writeup请看攻防世界web新手练习区writeup（下）


https://blog.csdn.net/weixin_42721957