XCTF攻防世界-Web-WriteUp

原创

192.168.1.1_admin 于 2019-12-17 21:04:13 发布 437 收藏 1
文章标签： CTF WEB WEB安全 攻防演练

目录

（本篇博客作为自己的学习记录，含有部分前辈大佬的码字，但是在操作上有更新之处，并且步骤较为详细，工具简单，介绍更为具体，特此记录以备回顾之需，也供其他学者借鉴，互相交流学习。）

---

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。

【目标】

学会查看源代码

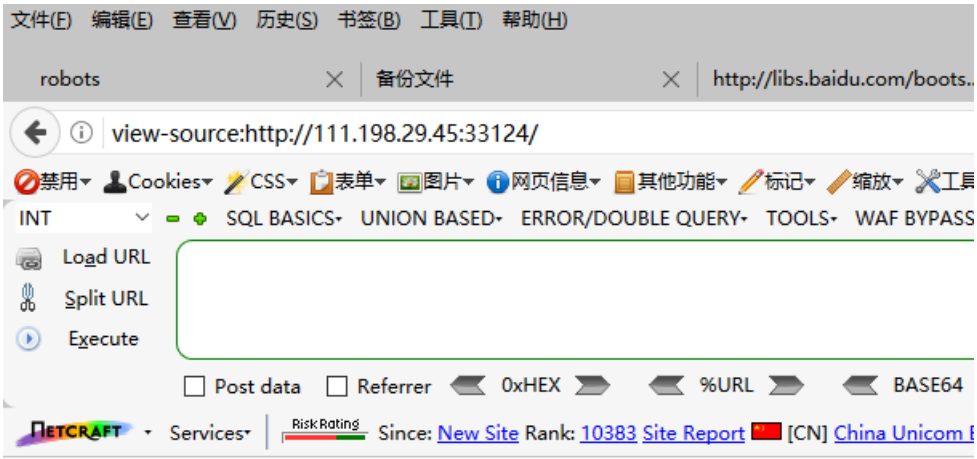
【工具】

firefox浏览器

【分析过程】

方法一：可以通过*view-source:*的方法来访问源码：*html view-source:http://10.10.10.175:32796*

在url中提交后便可访问页面源码，在源码中可找到flag。



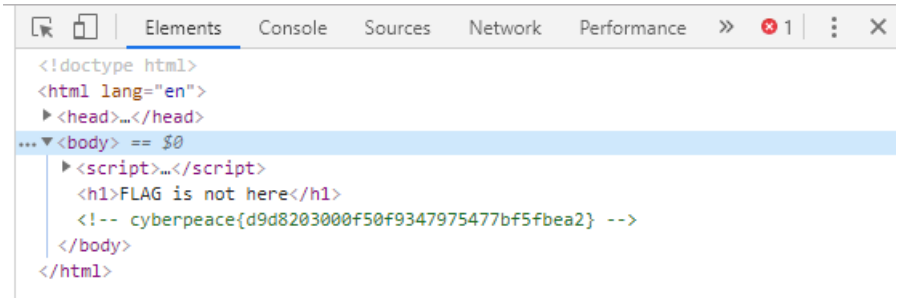

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Where is the FLAG</title>
</head>
<body>
<script>
document.oncontextmenu=new Function("return false")
document.onselectstart=new Function("return false")
</script>


<h1>FLAG is not here</h1>


<!-- cyberpeace{d9d8203000f50f9347975477bf5fbea2} -->

</body>
</html>
```


方法二：F12键直接查看网址源代码



---

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？

【目标】

了解http请求方法，此处考察get和post两个最常用的请求方法。

HTTP协议中共定义了八种方法或者叫“动作”来表明对Request-URI指定的资源的不同操作方式，具体介绍如下：

·GET：向特定的资源发出请求。

·POST：向指定资源提交数据进行处理请求（例如提交表单或者上传文件）。数据被包含在请求体中。POST请求可能会导致新的资源的创建和/或已有资源的修改。

·OPTIONS：返回服务器针对特定资源所支持的HTTP请求方法。也可以利用向Web服务器发送'*'的请求来测试服务器的功能性。

·HEAD：向服务器索要与GET请求相一致的响应，只不过响应体将不会被返回。这一方法可以在不必传输整个响应内容的情况下，就可以获取包含在响应消息头中的元信息。

·PUT：向指定资源位置上传其最新内容。

·DELETE：请求服务器删除Request-URI所标识的资源。

·TRACE：回显服务器收到的请求，主要用于测试或诊断。

·CONNECT：HTTP/1.1协议中预留给能够将连接改为管道方式的代理服务器。

【工具】

推荐火狐浏览器 渗透版

【分析过程】

在url后添加/？a=1即可发送get请求。

勾选post data即可发起POST请求

操作

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{74b902b1438e81f4dc063b0e09a42fcf}

---

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。

【目标】

掌握robots协议的知识

robots.txt是搜索引擎中访问网站的时候要查看的第一个文件。当一个搜索蜘蛛访问一个站点时，它会首先检查该站点根目录下是否存在robots.txt，如果存在，搜索机器人就会按照该文件中的内容来确定访问的范围；如果该文件不存在，所有的搜索蜘蛛将能够访问网站上所有没有被口令保护的页面。

【工具】

不需要

【分析过程】

标签栏提示：robots,可以直接想到robots.txt,扫目录也可以扫到:

直接在地址栏输入http://111.198.29.45:50246/robots.txt


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

HTML访问robots.txt发现f1ag_1s_h3re.php

访问f1ag_1s_h3re.php得到flag

cyberpeace{836480c6838bfa114fefc7f5ce94f010}

---

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！

【目标】

掌握有关备份文件的知识

常见的备份文件后缀名有: .git .svn .swp .~ .bak .bash_history（共6种）

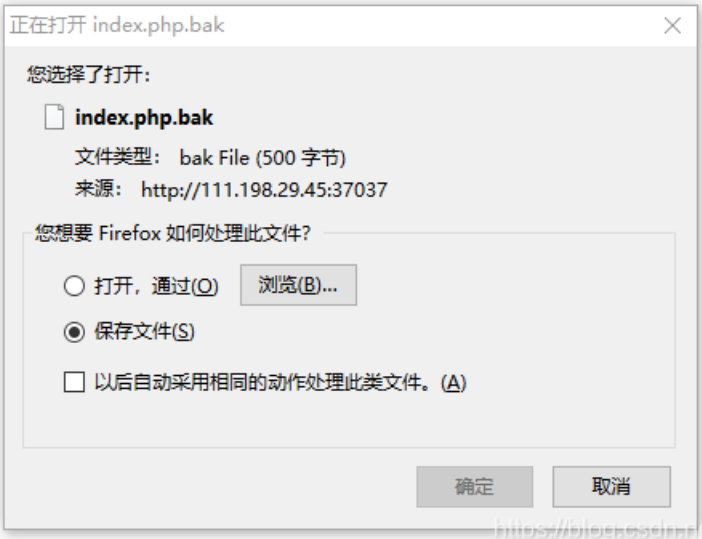
【工具】

不需要

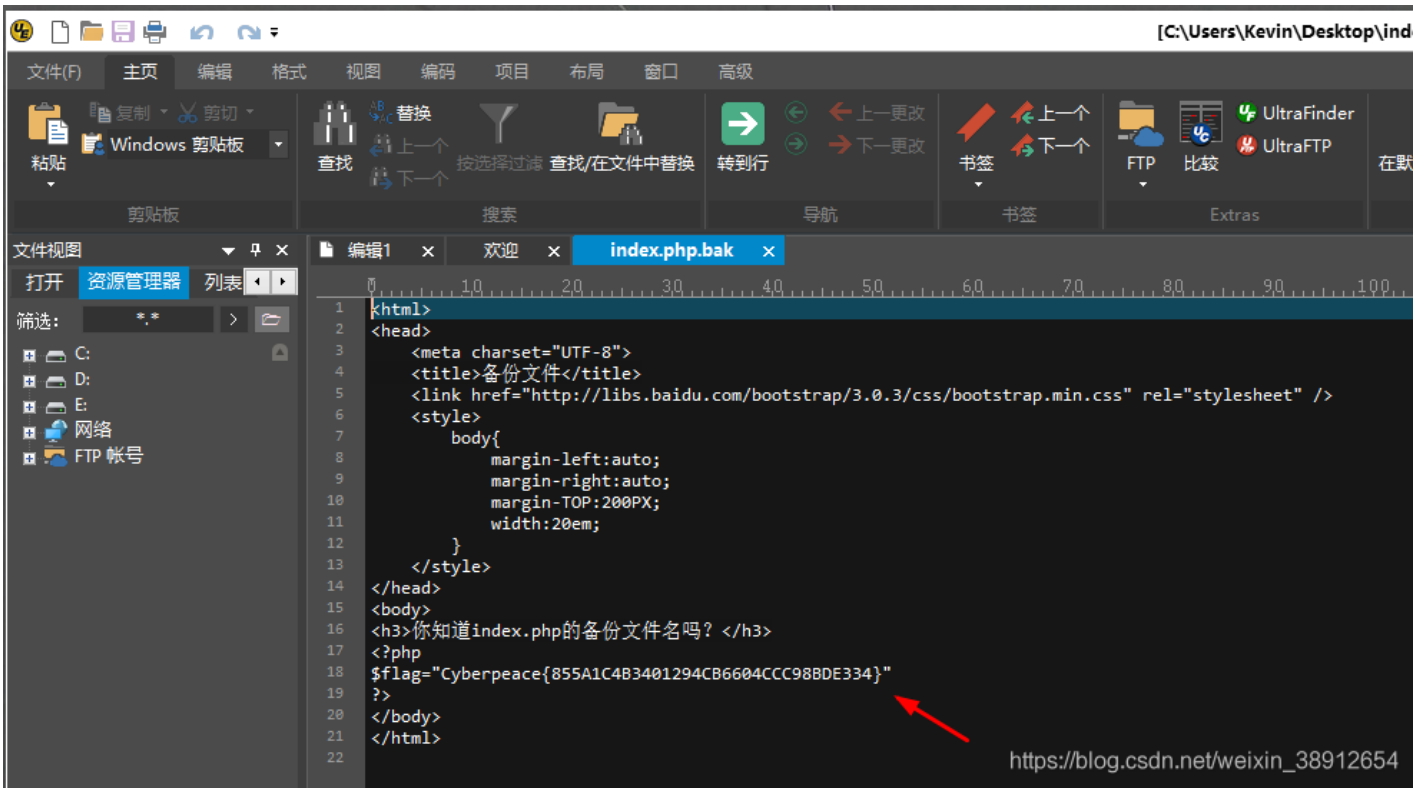
【分析过程】

问你知道index.php的备份文件名吗？可以手动猜测,直接把常用的备份文件后缀加上去 http://111.198.29.45:37037/index.php.bak，试出来了；

也可以使用扫目录脚本或软件（我觉得这个麻烦）。



下载到本地用UE或者记事本打开，即可看到flag



---

cookie

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

【目标】

掌握有关cookie的知识

Cookie 可以翻译为“小甜品，小饼干”，Cookie 在网络系统中几乎无处不在，当我们浏览以前访问过的网站时，网页中可能会出现 ：你好 XXX，这会让我们感觉很亲切，就好像吃了一个小甜品一样。这其实是通过访问主机中的一个文件来实现的，这个文件就是 Cookie。在 Internet 中，Cookie 实际上是指小量信息，是由Web服务器创建的，将信息存储在用户计算机上的文件。一般网络用户习惯用其复数形式 Cookies，指某些网站为了辨别用户身份、进行Session 跟踪而存储在用户本地终端上的数据，而这些数据通常会经过加密处理。

【工具】

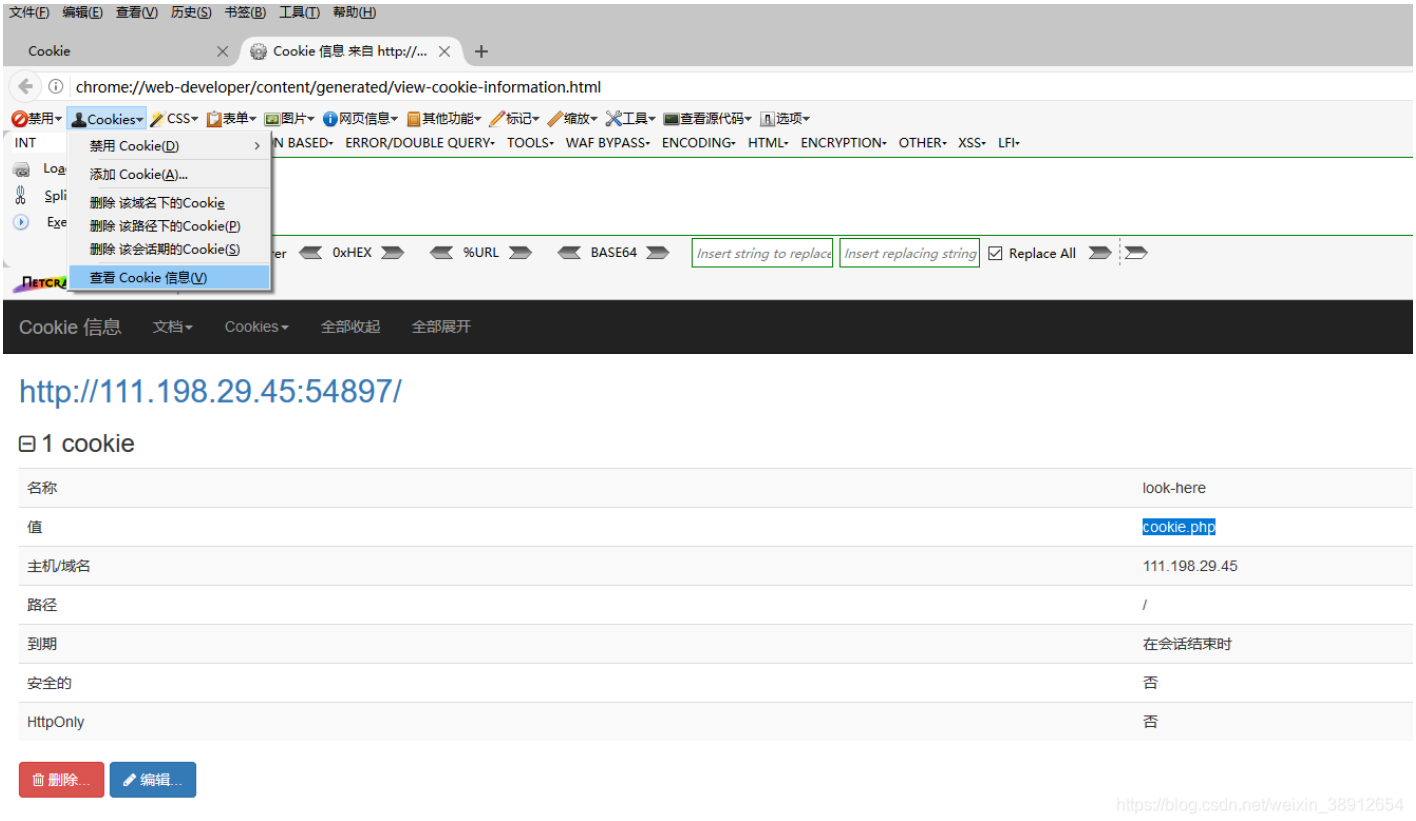
火狐渗透版

或者浏览器开发者工具

【分析过程】

查看cookies信息

火狐渗透版



可以看到有个cookie.php

发送cookie.php请求http://111.198.29.45:54897/cookie.php

浏览器开发者工具

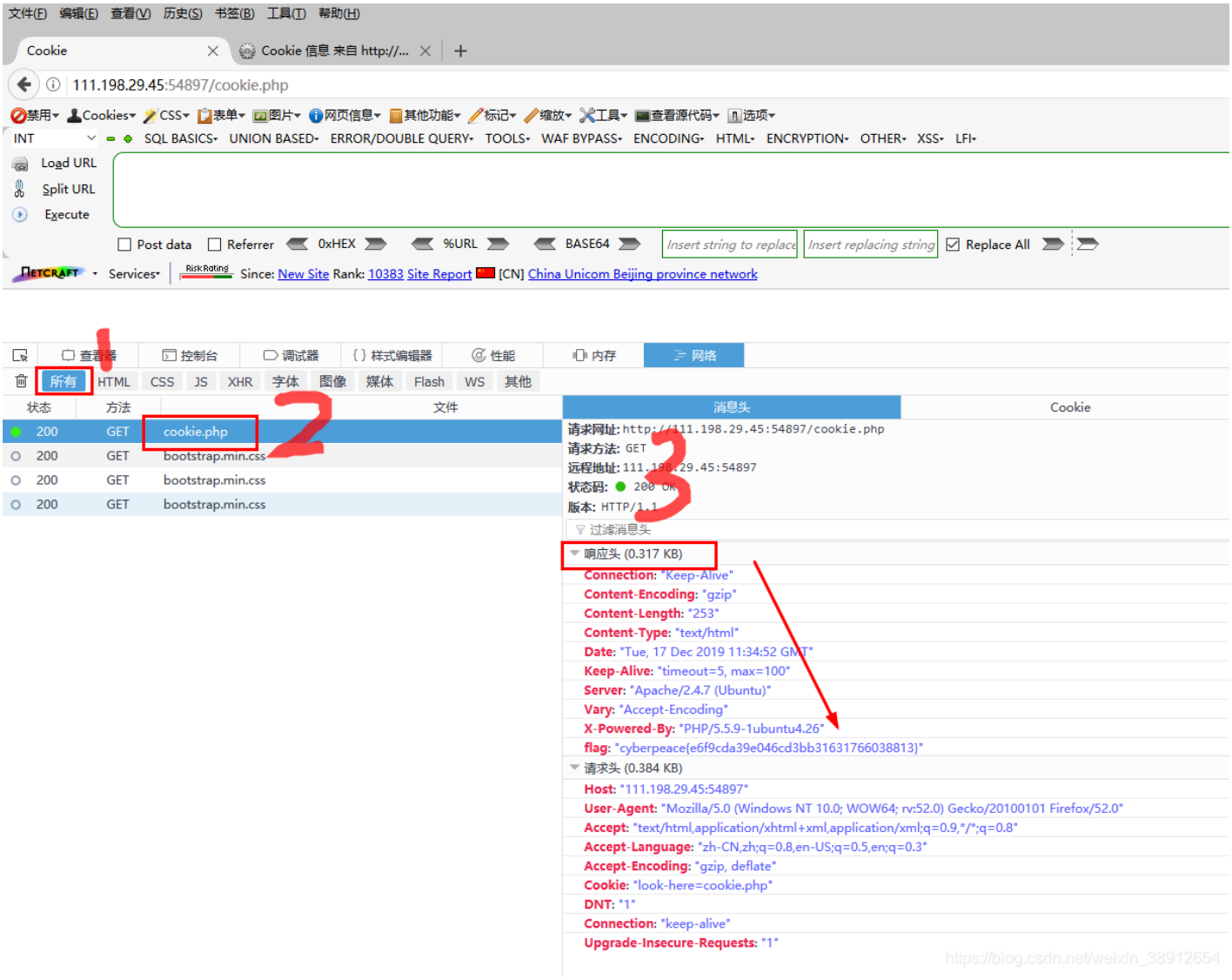
F12-存储-Cookie-look here-look here：cookie.php

可以看到有个cookie.php

发送cookie.php请求http://111.198.29.45:54897/cookie.php

See the http response

提示看http响应，那就F12进去看响应头信息

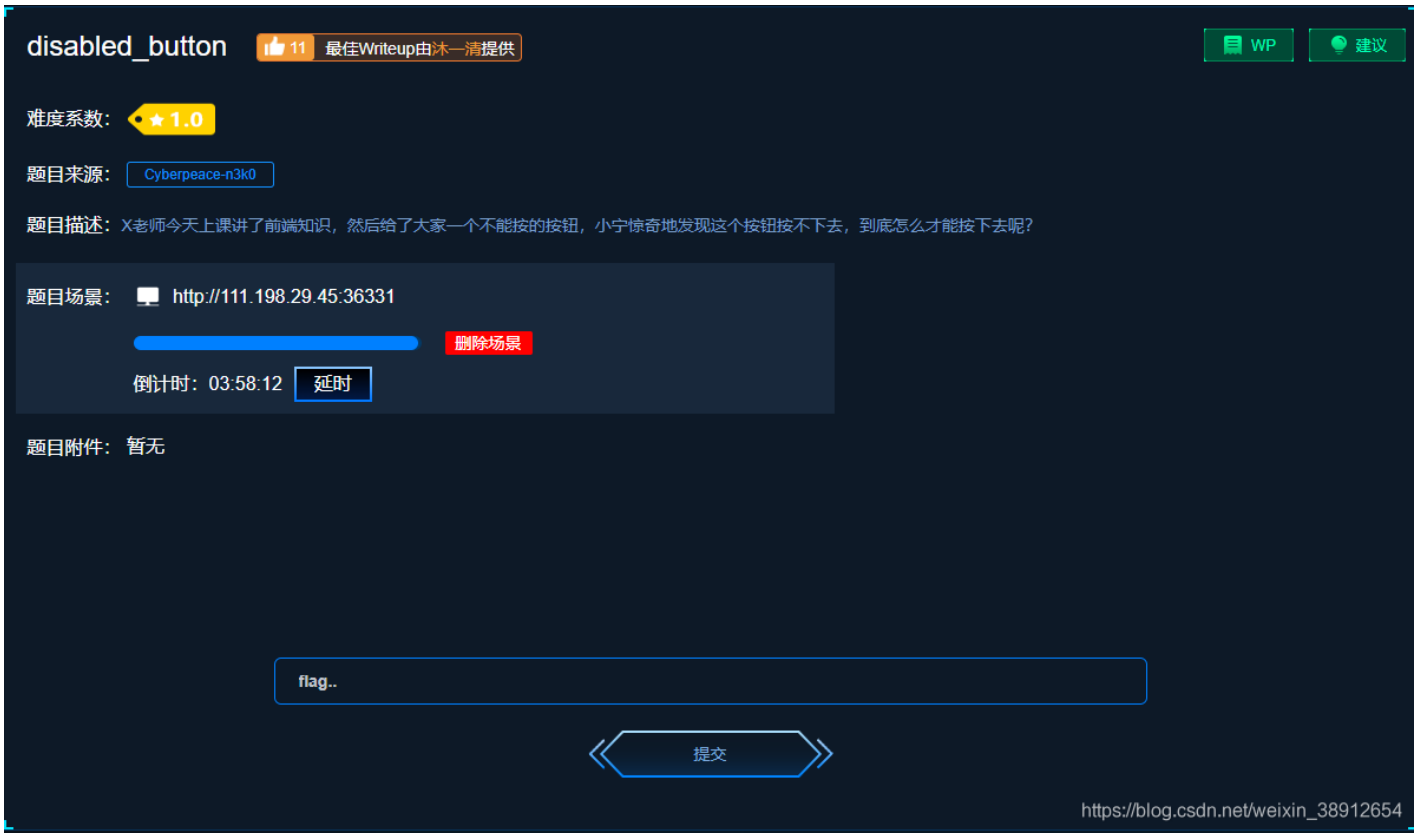


在响应头里发现flag。

---

disabled_button

题目描述：X老师今天上课讲了前端知识，然后给了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？



【目标】

初步了解前端知识

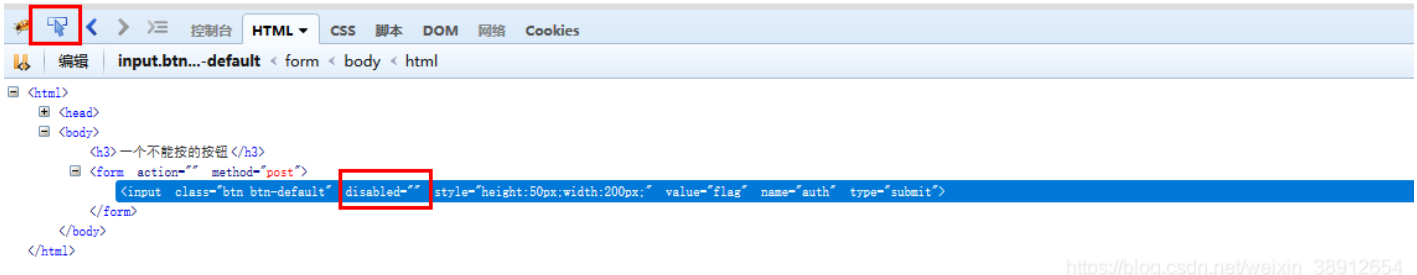
对于HTML的基本语法知识需要一定的了解，对于每个标签，有一些不可用属性，如：disabled，借助开发者工具可以删除这些属性，从而让其变得可用！

【工具】

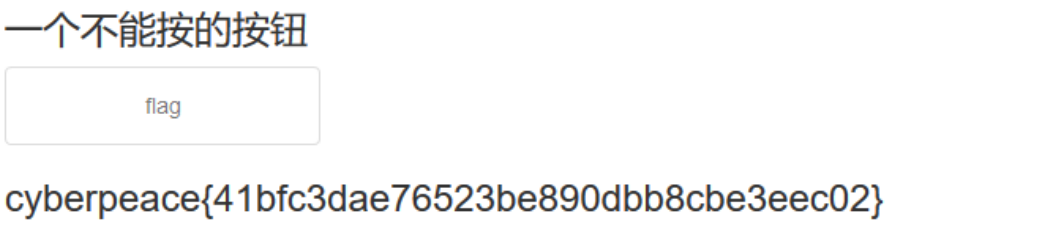
开发者工具

【分析过程】

F12，然后在出现的调试会话框左上角箭头点击一下然后去点击flag按钮定位代码段，将标签input中的disabled（不可用）属性删除，x掉调试框。



点击按钮，即可得到flag。



---

simple_js

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{xxxxxxxxx})

【目标】

掌握有关js的知识

【工具】

开发者工具

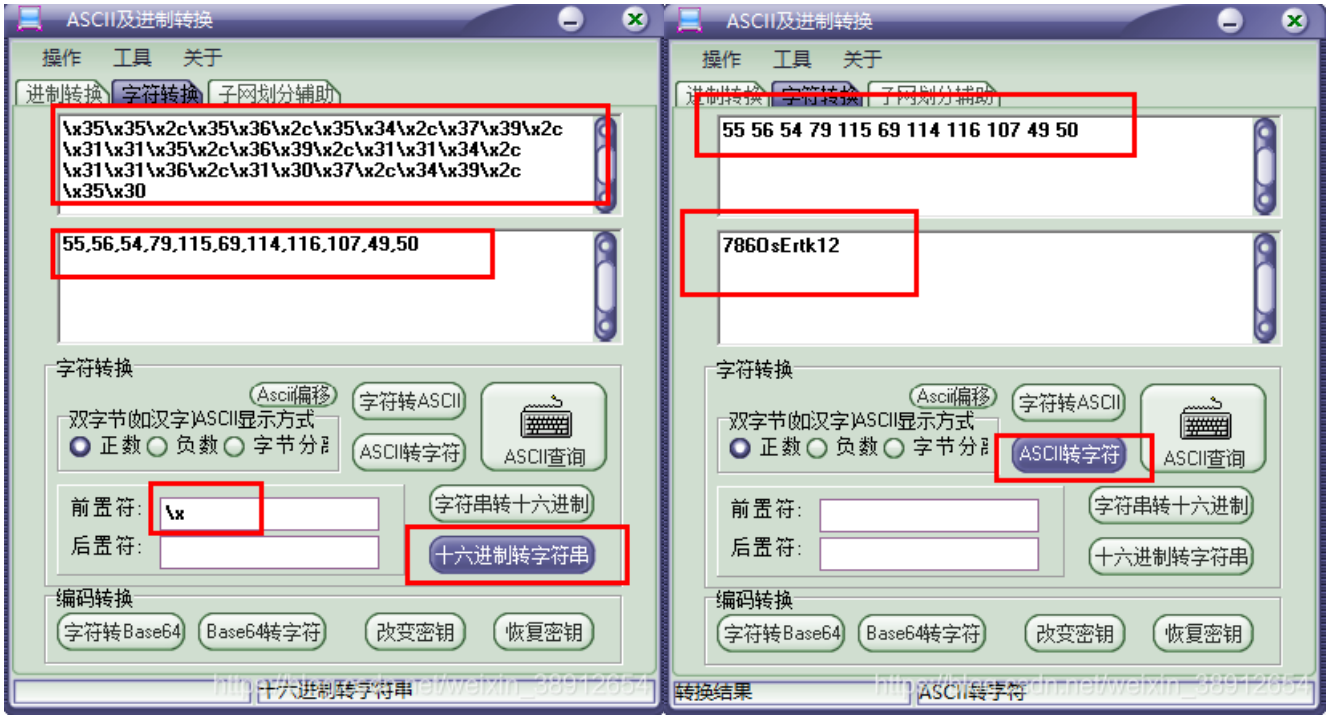
【分析过程】

进入环境后Ctrl+U查看代码

会发现dechiffre返回值与参数pass_enc没有任何关联，返回值是固定的，即不论输入什么都是一样得输出。所以猜测密码在string这一行里。

先将16进制数输出进制

```
}
String["fromCharCode"](dechiffre("\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c\x35\x30"));
```



进制转换工具http://www.xitongzhijia.net/soft/59990.html

得出：786OsErtk12

此时你是不是觉得就完了？不要太激动，这不是正确flag，请注意审题：

（太坑了）

最终flag：Cyberpeace{786OsErtk12}

未完。。。。。。