

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](#)

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/weixin_38912654/article/details/103585145

版权

目录

[view_source](#)

[get_post](#)

[robots](#)

[backup](#)

[cookie](#)

[disabled_button](#)

[simple_js](#)

(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。



view_source 31 最佳Writeup由Healer_aptx • Anchorite提供 WP 建议

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_38912654

【目标】

学会查看源代码

【工具】

firefox浏览器

【分析过程】

get_post  18 最佳Writeup由神秘人·孔雀翎提供  WP  建议

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




分享wp点券赚金币
[马上去写](#)
https://blog.csdn.net/weixin_38912654

【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}

https://blog.csdn.net/weixin_38912654

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。

robots 👍 23 最佳Writeup由MOLLMY提供 WP 建议

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: http://111.198.29.45:50246 删除场景

倒计时: 03:59:53 延时

题目附件: 暂无

题目已答对

分享wp点赞赚金币哦 https://blog.csdn.net/weixin_38912654

【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>

The screenshot shows a web browser window with the address bar containing <http://111.198.29.45:50246/robots.txt>. The browser's developer tools are open, showing the network tab with a request to <http://111.198.29.45:37462/?a=1>. The response content is displayed as follows:

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

HTML访问robots.txt发现f1ag_1s_h3re.php

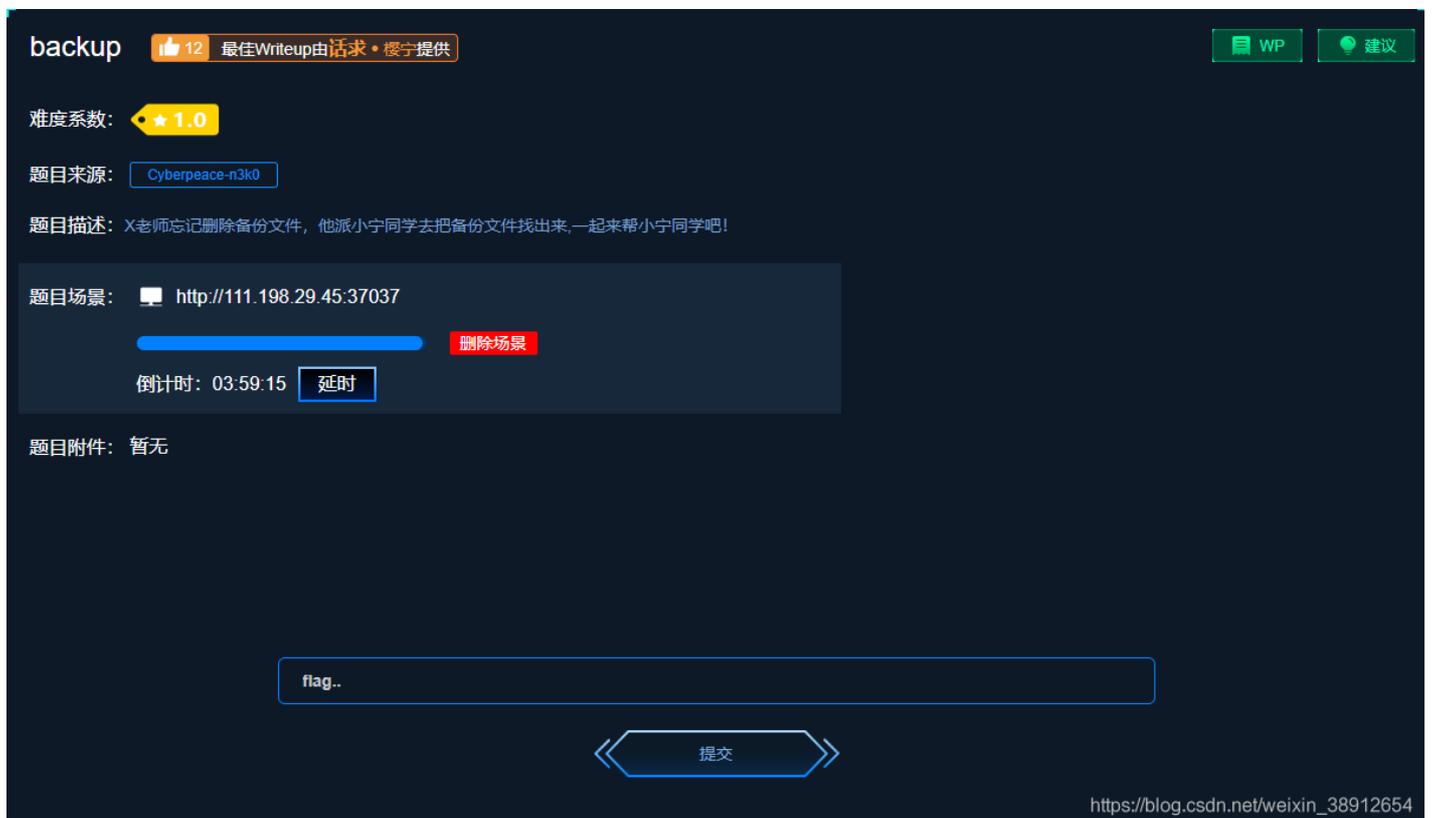
访问f1ag_1s_h3re.php得到flag



https://blog.csdn.net/weixin_38912654

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!



https://blog.csdn.net/weixin_38912654

【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)

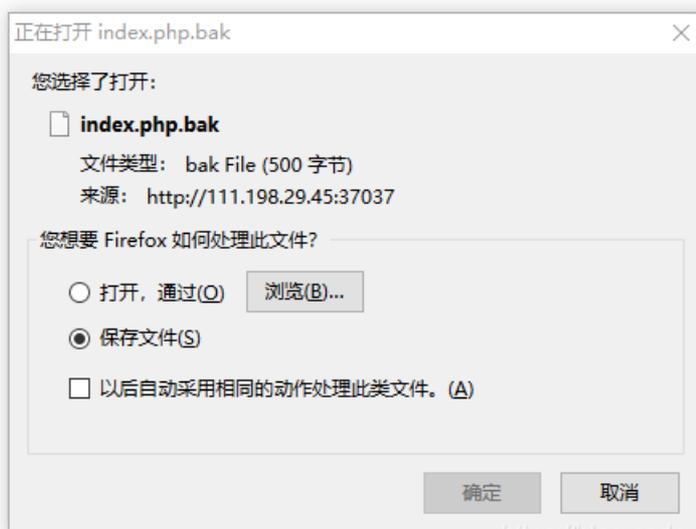
【工具】

不需要

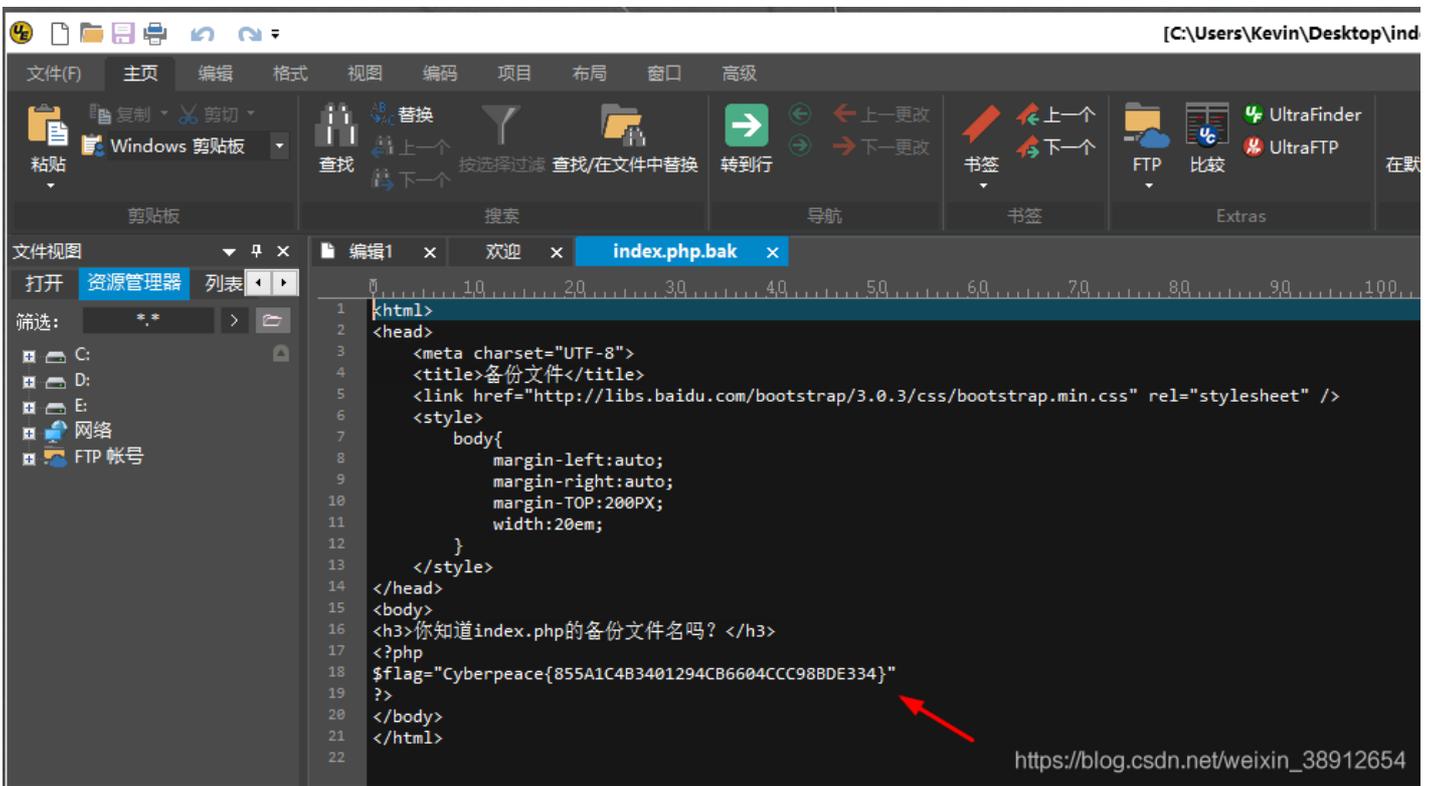
【分析过程】

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）。

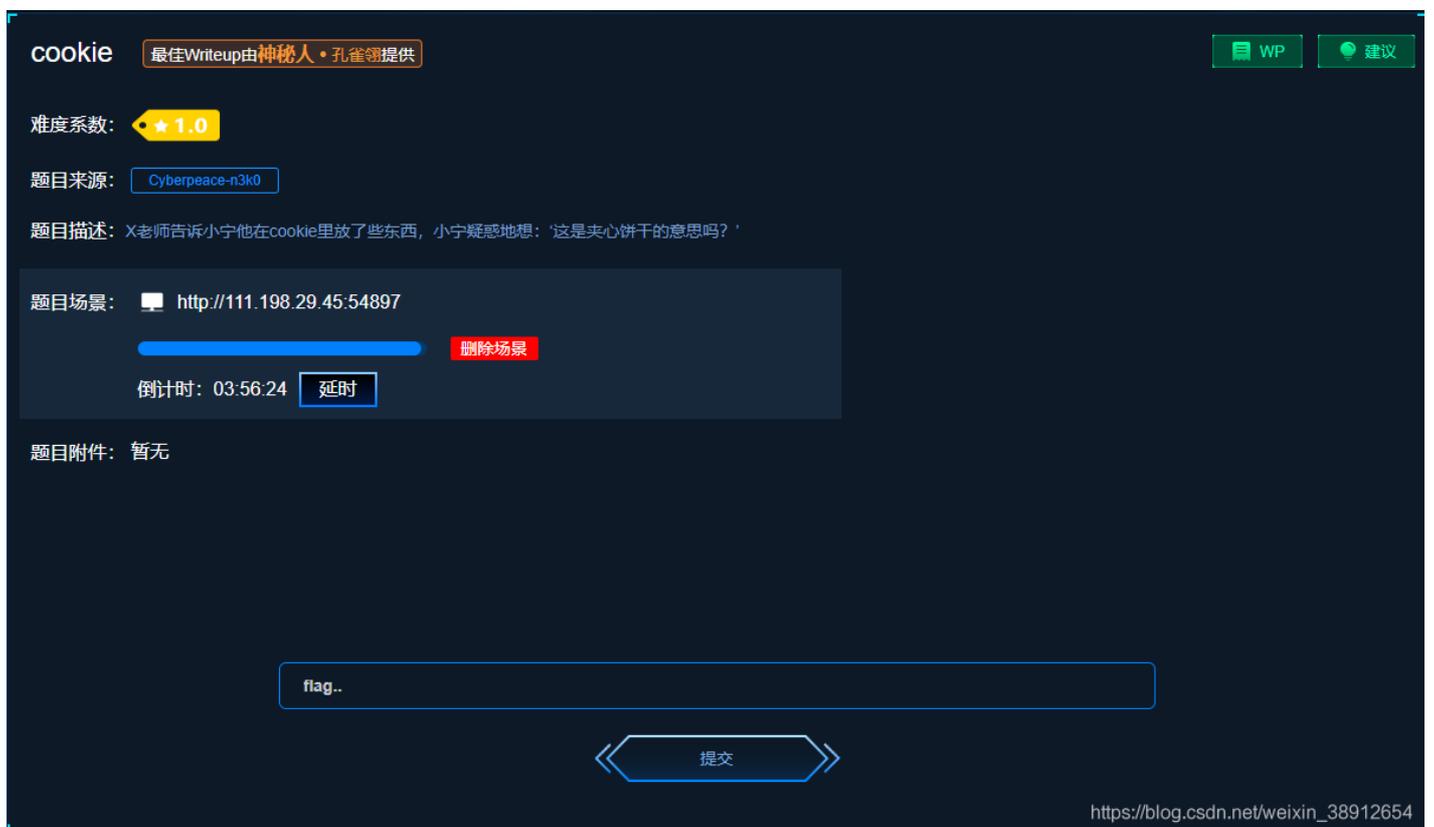


下载到本地用UE或者记事本打开，即可看到flag



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】

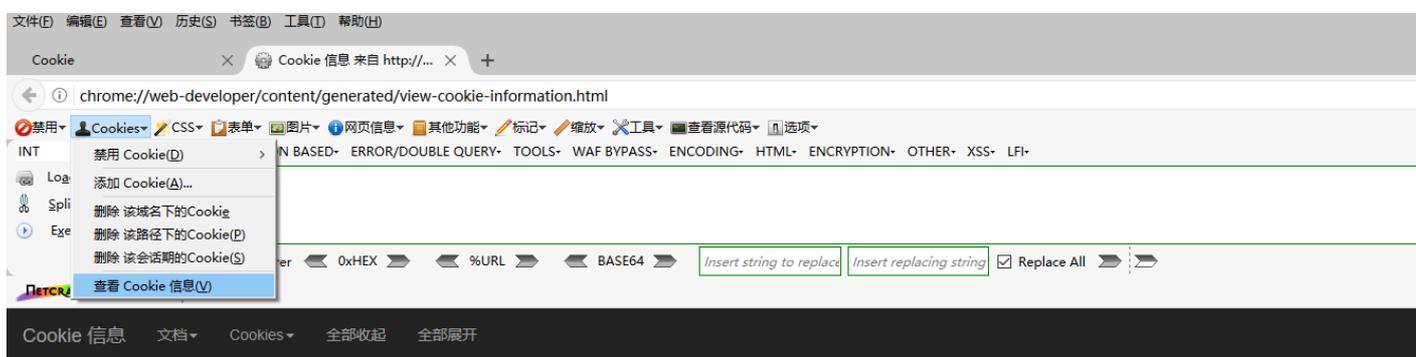
火狐渗透版

或者浏览器开发者工具

【分析过程】

查看cookies信息

火狐渗透版



<http://111.198.29.45:54897/>

共 1 cookie

名称	look-here
值	cookie.php
主机/域名	111.198.29.45
路径	/
到期	在会话结束时
安全的	否
HttpOnly	否

删除... 编辑...

https://blog.csdn.net/weixin_38912654

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

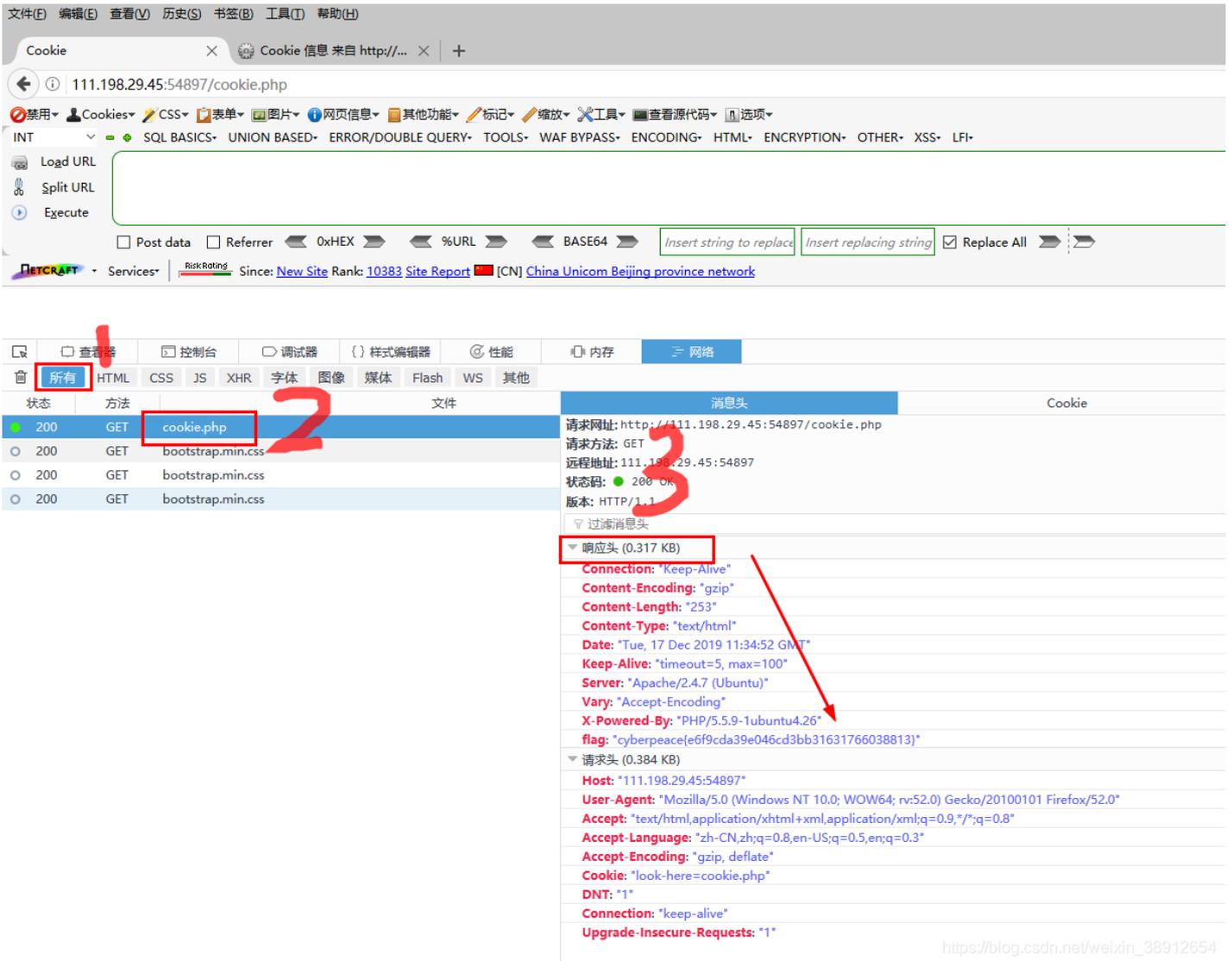
可以看到有个cookie.php

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

See the http response

https://blog.csdn.net/weixin_38912654

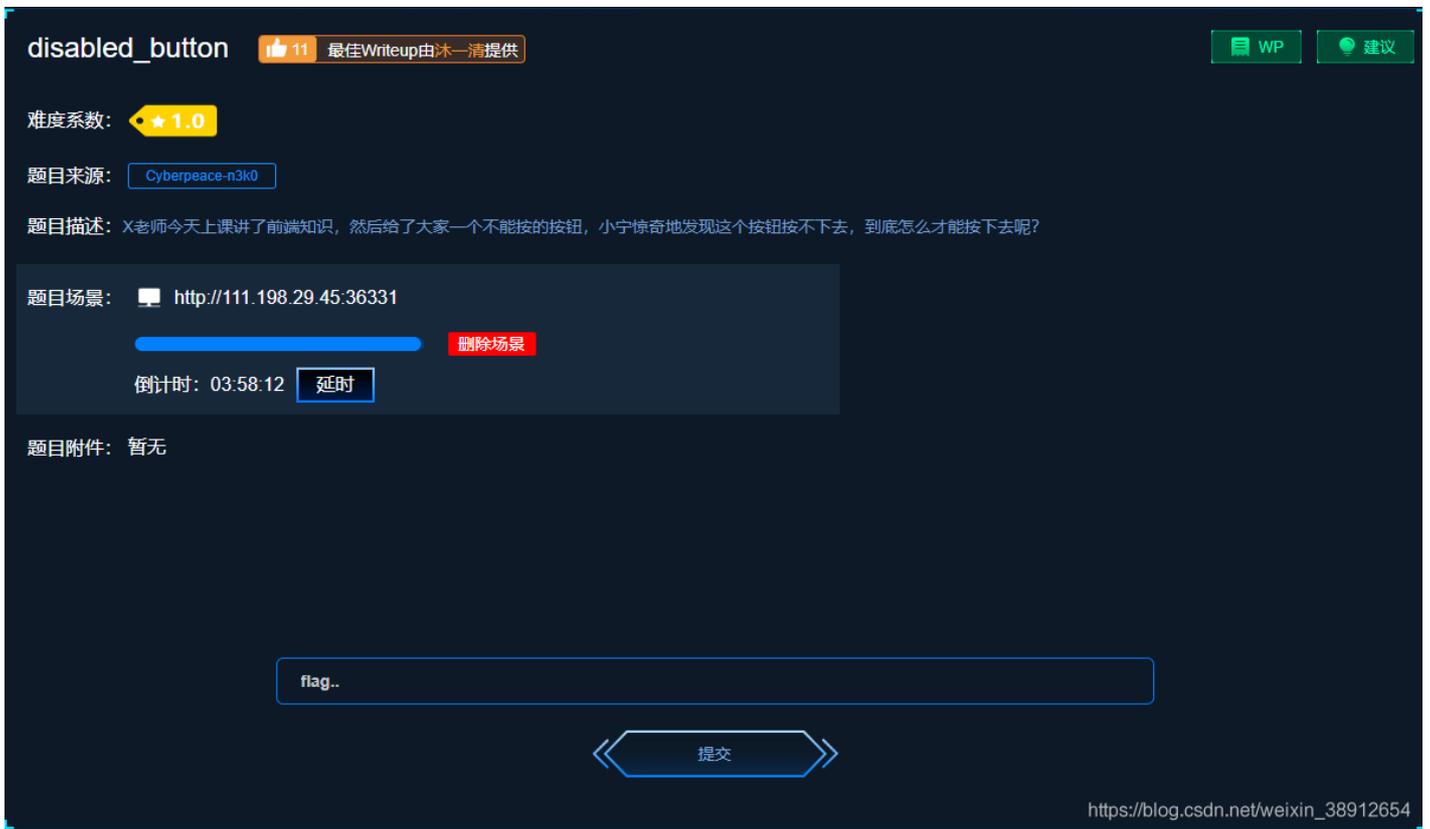
提示看http响应，那就F12进去看响应头信息



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

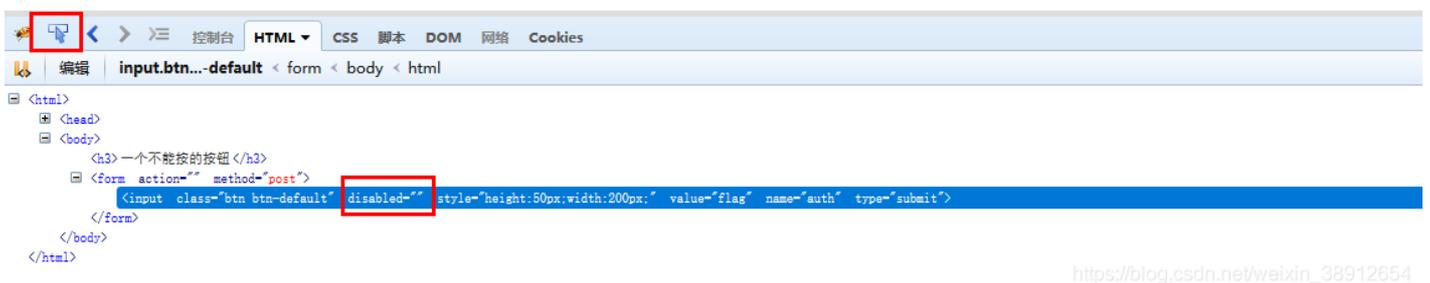
对于HTML的基本语法知识需要一定的了解，对于每个标签，有一些不可用属性，如：disabled，借助开发者工具可以删除这些属性，从而让其变得可用！

【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。

一个不能按的按钮

cyberpeace{41bfc3dae76523be890dbb8cbe3eec02}

https://blog.csdn.net/weixin_38912654

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{xxxxxxxx})

The screenshot shows a CTF challenge interface for 'simple_js'. At the top, it has a title 'simple_js', a like count of 213, and a note '最佳Writeup由Venom • IceM提供'. There are buttons for 'WP' and '建议'. Below the title, the difficulty is '1.0', the source is 'root-me', and the description is '小宁发现了一个网页，但却一直输不对密码。(Flag格式为 Cyberpeace{xxxxxxxx})'. There is a button '点击获取在线场景' and a note '题目附件: 暂无'. At the bottom, there is a text input field containing 'flag..' and a '提交' button. The URL 'https://blog.csdn.net/weixin_38912654' is visible in the bottom right corner.

【目标】

掌握有关js的知识

【工具】

开发者工具

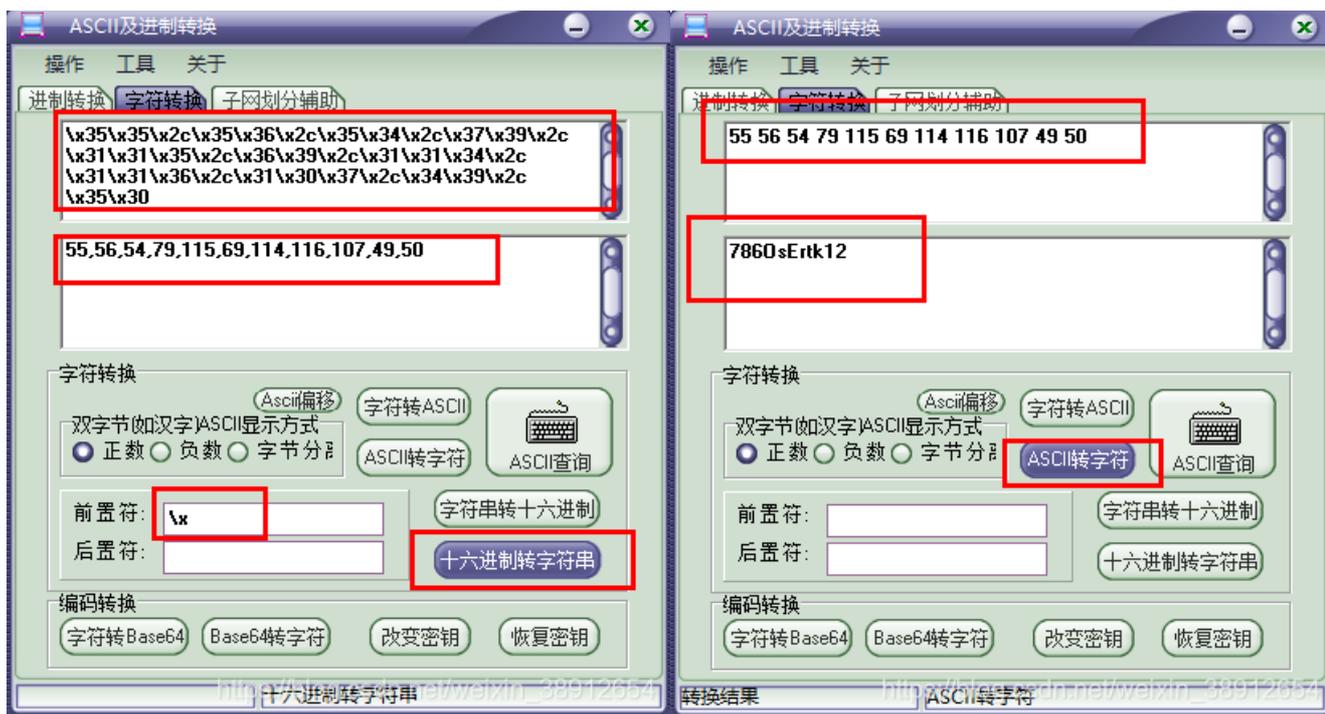
【分析过程】

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：7860sErtk12

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：

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})

(太坑了)

最终flag: Cyberpeace{7860sErtk12}

未完。。。。。