# 攻防世界web做题步骤

原创

Seven1_xwx 已于 2022-02-09 19:47:22 修改 277 收藏

文章标签： 前端 php web安全

于 2021-12-05 01:15:31 首次发布



本文链接：https://blog.csdn.net/Seven1_xwx/article/details/121601817



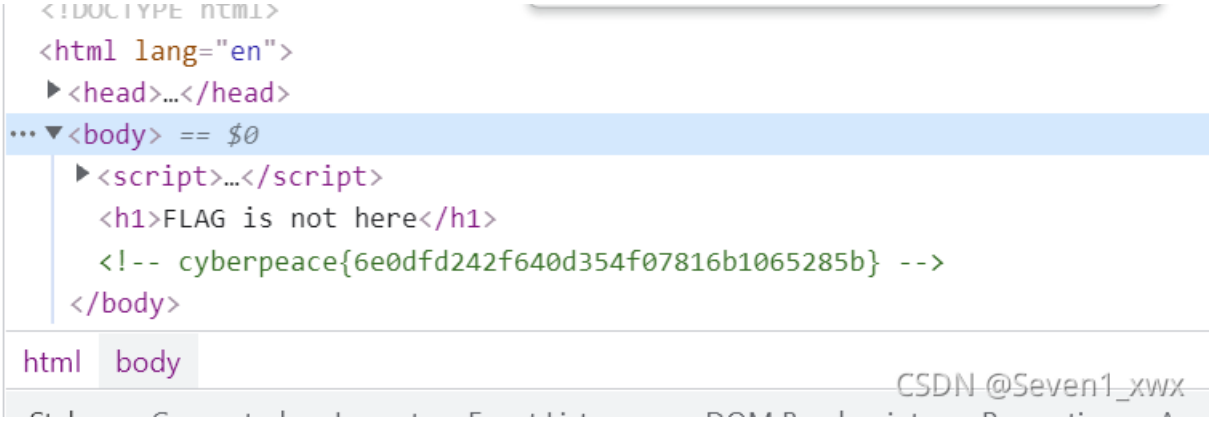
## 攻防世界web新手做题步骤

第一题：view_source

题目：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

获取场景后，打开网址发现如图所示：


所以我们按F12查看网页源代码，这时候就能看到




即可获得flag。

第二题：robots

题目：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。

同样先复制网页查看




显示出来是空白页，由题目意思可知，此题考查我们对robots协议的了解：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，所以我们直接在网址后面加 robots.txt，就会看到如下图


就能看到“flag_is_”，就把那个加在网址后面在搜索


既能获得flag。

第三题：backup

题目：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！

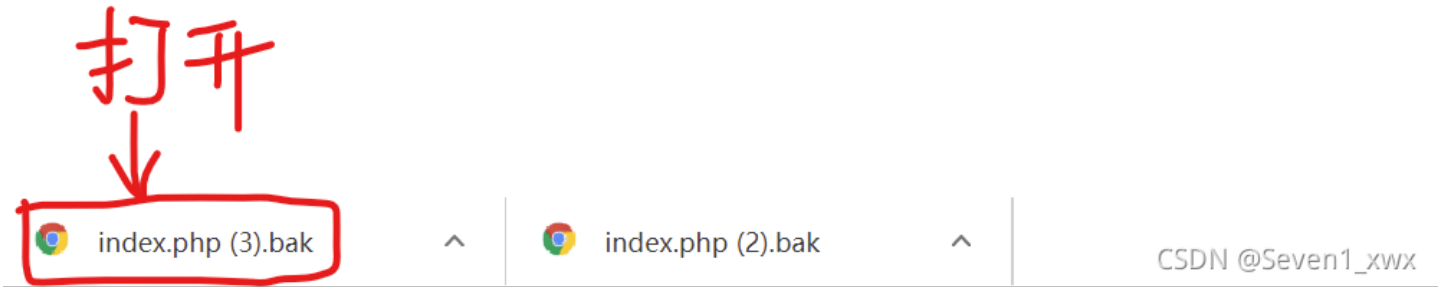
打开网址后发现如图所示文字：


根据题目提示：备份文件

查找后知道备份文件后缀名：bak（被自动或是通过命令创建的辅助文件，它包含某个文件的最近一个版本），所以我们尝试在网址后面加后缀名，得到下载包后打开

```
<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>
```

flag



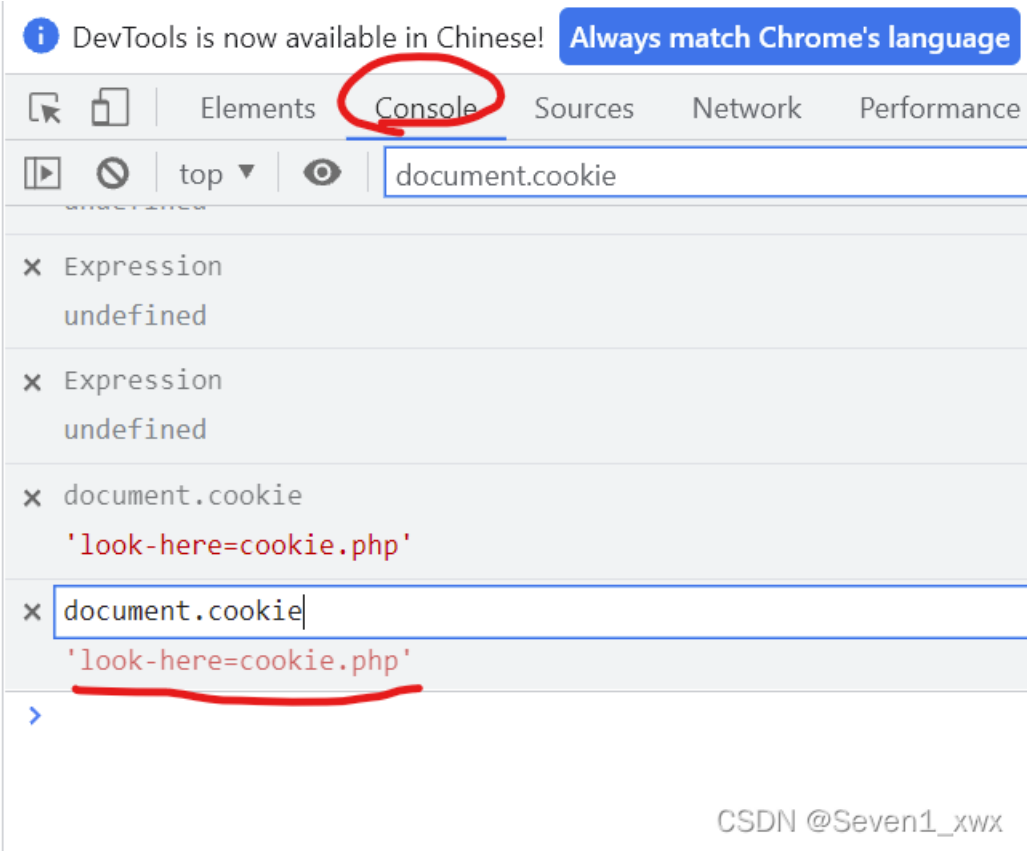

即可找到flag。

第四题：cookie

题目：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？

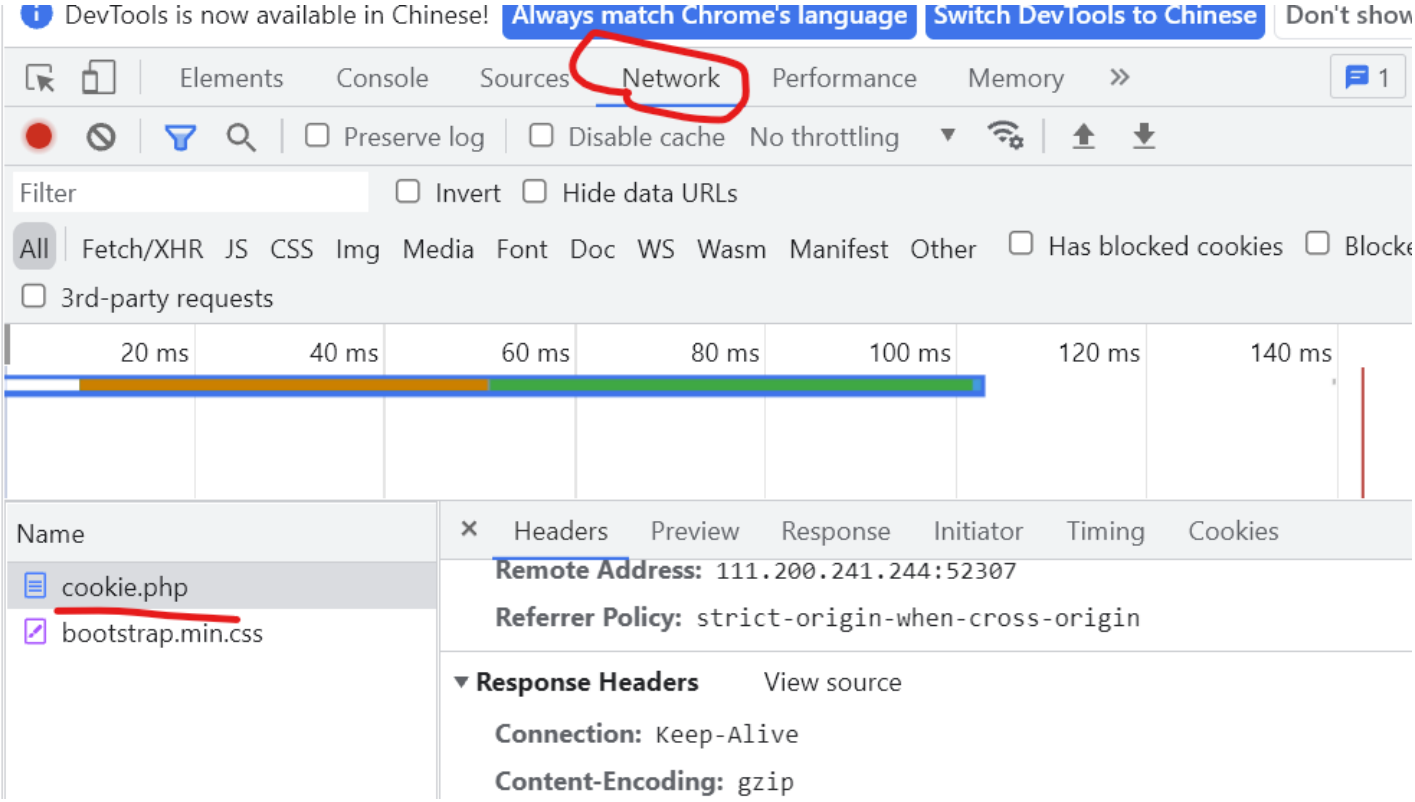
还是先打开网址，看到下图所示

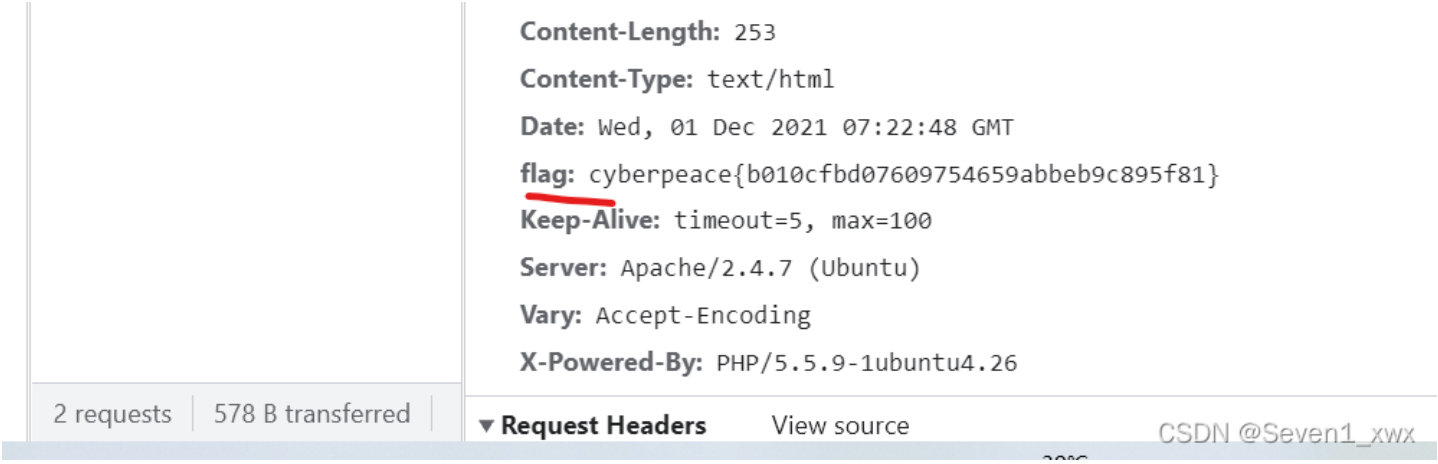
所以还是先查看网页代码，然后如下图




在网址后加“/cookie.php”再次搜索看到下图


那就按照提示，查看response





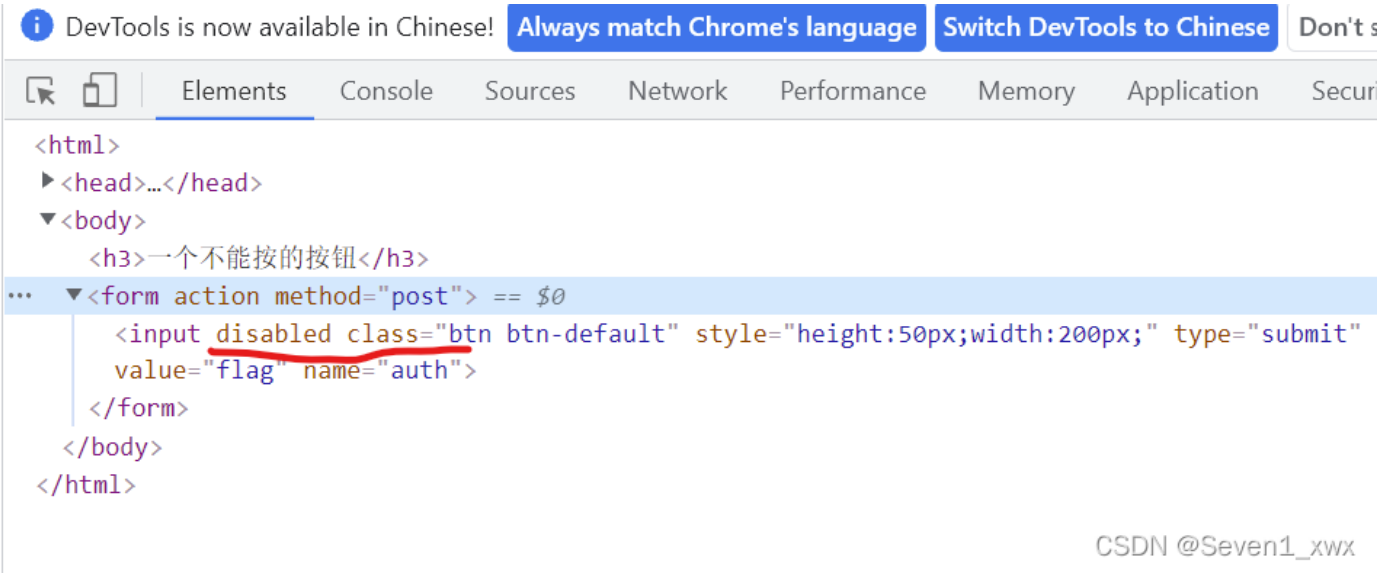

寻找后即可获得flag

第五题：disabled_button

题目：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？

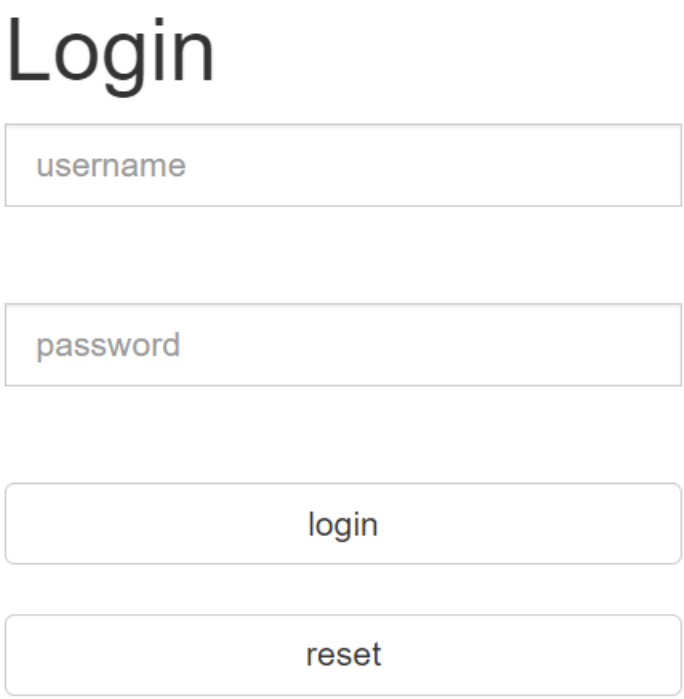
先打开网址，看到下图


看到flag那块点击不了，查看网页代码




把“disable”改成“able”试试，刷新后，获得flag

第六题：weak_auth
题目：小宁写了一个登陆验证页面，随手就设了一个密码
还是先打开网址






看到是个登录界面，点击reset，显示出下图所示


所以尝试用户名为“admin”，密码既然是随手设，那就猜，结果试出来密码为123456，获得flag

第七题：simple_php

题目：小宁听说php是最好的语言,于是她简单学习之后写了几行php代码

打开网址看到下图所示代码

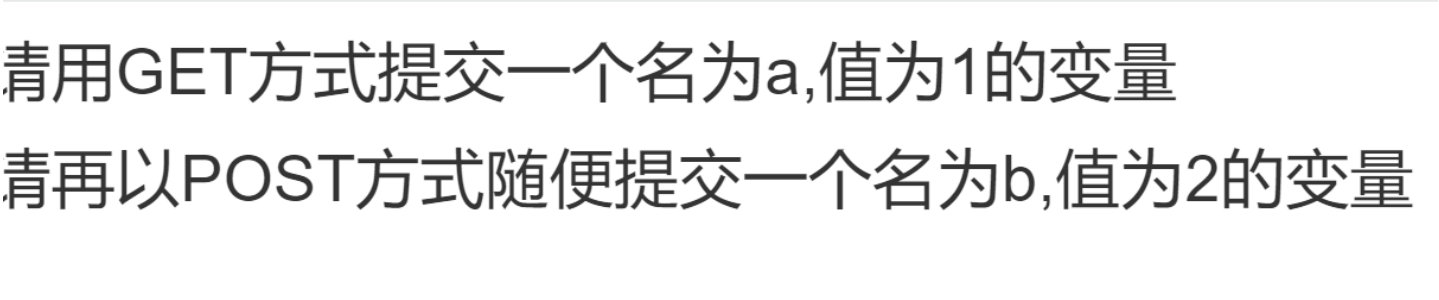
```php
<?php
show_source(__FILE__);
include("config.php");
$a=@$_GET['a'];
$b=@$_GET['b'];
if($a==0  and  $a){
        echo  $flag1;
}
if(is_numeric($b)){
        exit();
}
if($b>1234){
        echo  $flag2;
}
?>
```

根据代码可知，flag1是a=0但不为错，flag2是b>1234但b不能是数字

第八题：get_post

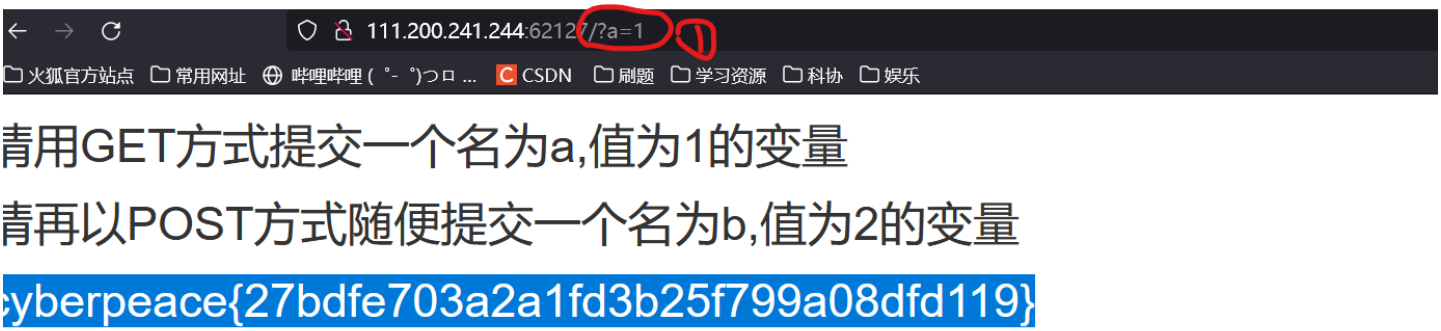
题目：X老师告诉小宁同学HTTP通常使用两种请求方法，你知道是哪两种吗？


根据题目提示“以GET方式”，结果如下图




然后如下图







即可获得flag

第九题：xff_referer

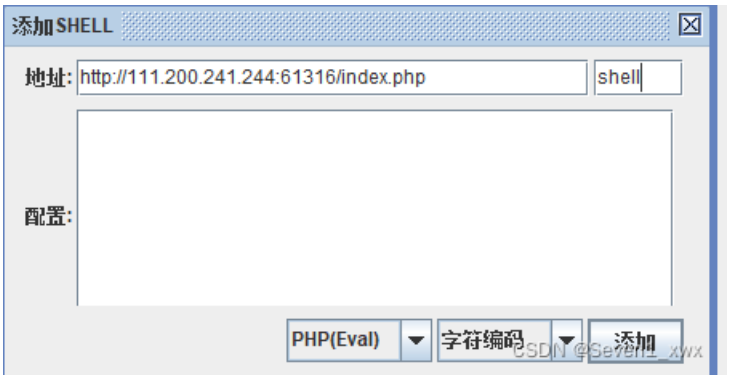
题目：X老师告诉小宁其实xff和referer是可以伪造的

（博主真的太困了.....先空个模板）

第十题：webshell

题目：小宁百度了php一句话,觉着很有意思,并且把它放在index.php里。

打开网址后，




第十一题：command_execution

题目：小宁写了个ping功能,但没有写waf,X老师告诉她这是非常危险的，你知道为什么吗。

第十二题：simple_js

题目：小宁发现了一个网页，但却一直输不对密码。