

# 攻防世界Web新手区Write Up

原创

[Evaristexu](#)  于 2020-04-27 17:26:51 发布  112  收藏

分类专栏: [CTF](#) 文章标签: [web 安全](#)

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/Evaristexu/article/details/105793797>

版权



[CTF 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

## view\_source

👍 54 最佳Writeup由Healer\_aptx • Anchorite提供

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/Evaristexu>

## FLAG is not here

```
<!DOCTYPE html>
<html lang="en">
  <head>
  </head>
  <body>
    <script>
      <h1>FLAG is not here</h1>
      <!--cyberpeace{263c41425f1c8fd89942c4037439ec80}-->
    </script>
    <remove-web-limits-iqxin id="rwl-iqxin" class="rwl-exempt" style="position: fixed; top: 0px; left: 0px;">
    </remove-web-limits-iqxin>
  </body>
</html>
```

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

↵ F12快捷键

## robots

👍 57 最佳Writeup由MOLLMY提供

难度系数: ★ 1.0

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: [点击获取在线场景](#)

题目附件: 暂无

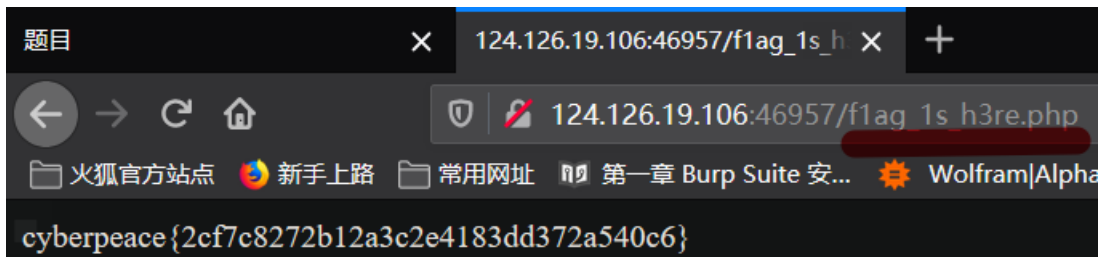
<https://blog.csdn.net/Evaristexu>

打开后什么提示都没有,打开协议

```
124.126.19.106:46957/robots.txt
```

```
User-agent: *  
Disallow:  
Disallow: f1ag_1s_h3re.php
```

访问下方的Disallow



→ 如何查看网页的robots协议

backup 18 最佳Writeup由话求·樱宁提供

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

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!

题目场景: [点击获取在线场景](#)

题目附件: 暂无

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

php的备份有两种: **.php~** 和 **\*.php.bak** 如果网站存在备份文件,在地址栏最末加上/index.php~或/index.php.bak,即可得到备份

文件

添加了/index.php.bak后自动下载文件，用文本编辑器打开发现flag

→ 备份文件扩展名

The image shows a CTF challenge interface for a challenge named 'cookie'. It features a difficulty rating of 1.0, a source of 'Cyberpeace-n3k0', and a description in Chinese: '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？'. The challenge scenario is listed as 4% and there are no attachments.

The image shows a browser's developer tools window with the 'Cookie' tab selected. A table lists a cookie named 'look-here' with the value 'cookie.php', domain '124.126.19.106', and path '/'. The 'Expires / Max-Age' column shows '会话' (session). The 'Data' pane on the right shows the cookie's details, including its domain, expiration, and creation time.

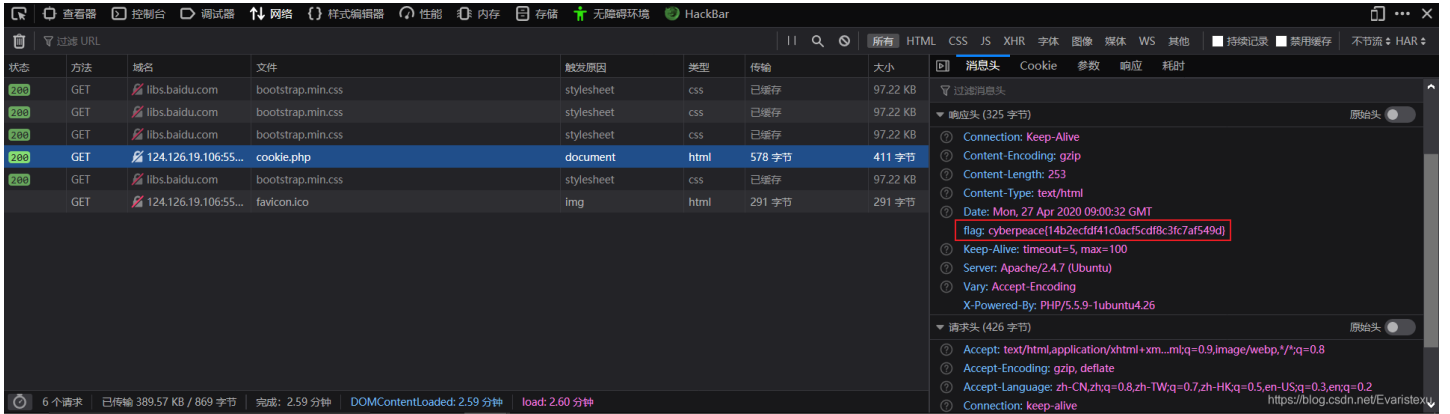
发现cookie.php文件

打开文件

The image shows a browser address bar with the URL '124.126.19.106:55449/cookie.php' entered.

The image shows a browser's developer tools window with the 'Network' tab selected. The 'View Response' pane is open, displaying the HTML response from the server. The response content is 'See the http response'.

提示查看该文件(cookie.php)的响应



→ cookie信息的查看

disabled\_button 17 最佳Writeup由沐一清提供

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

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?

题目场景: <http://124.126.19.106:46032>

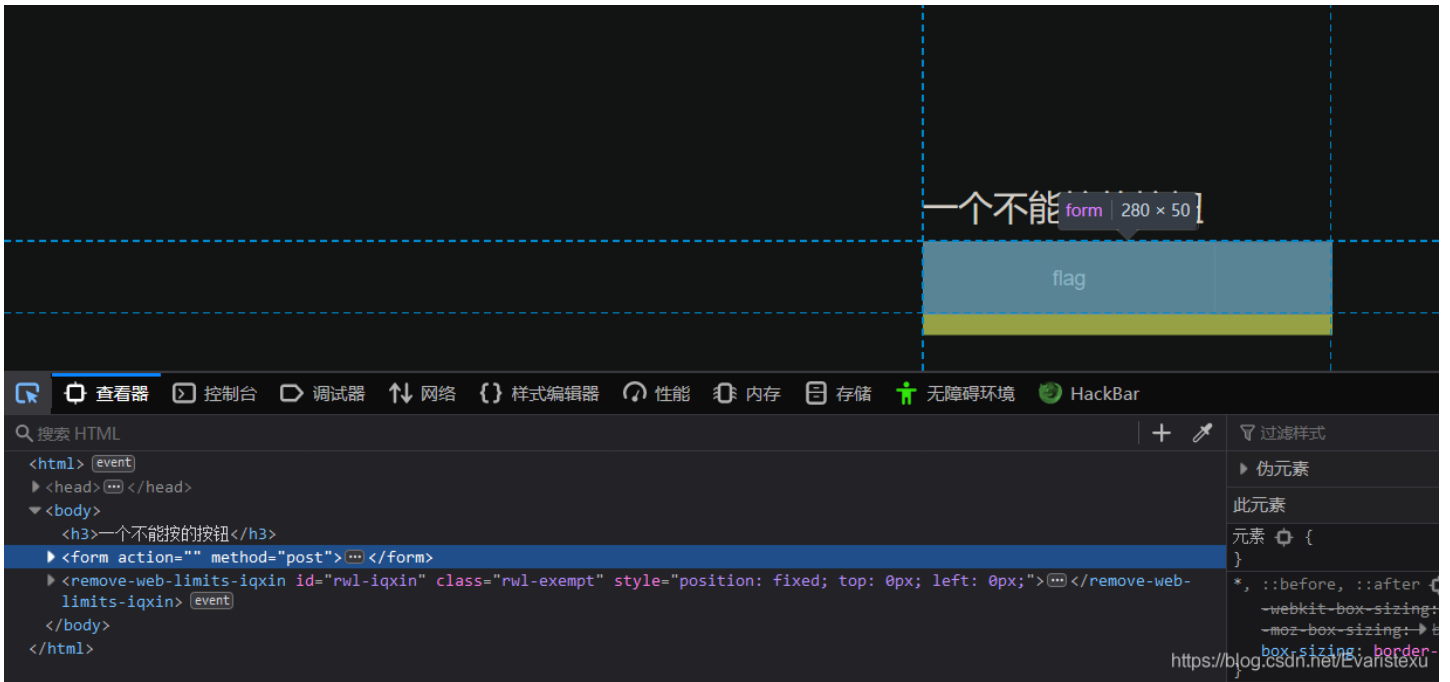
删除场景

倒计时: 03:59:53 延时

题目附件: 暂无

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





```
<form action="" method="post">
  <input class="btn btn-default disabled="" style="height:50px;width:200px;" type="submit" value="flag" name="auth">
</form>
```

将disabled改为enabled即可  
点击按钮出现flag



前端控件属性修改

# weak\_auth

👍 32 最佳Writeup由小太阳的温暖提供

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

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。

题目场景:  http://124.126.19.106:36280

删除场景

倒计时: 03:58:36

题目附件: 暂无

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

随便输入一个, 验证失败跳转页面, 查看源代码

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <title>weak_auth</title>
6 </head>
7 <body>
8
9 <script>alert('password error');</script><!--maybe you need a dictionary-->
10
11
12 </body>
13 </html>
14
```

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

→ 使用BurpSuite暴力破解

# simple\_php

👍 51 最佳Writeup由MOLLMY提供

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

题目描述: 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。

题目场景:  http://124.126.19.106:50986

删除场景

倒计时: 03:59:54

题目附件: 暂无

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

```
<?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;
}
?> |
```

该题的详细解答

→ php基本代码审计