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

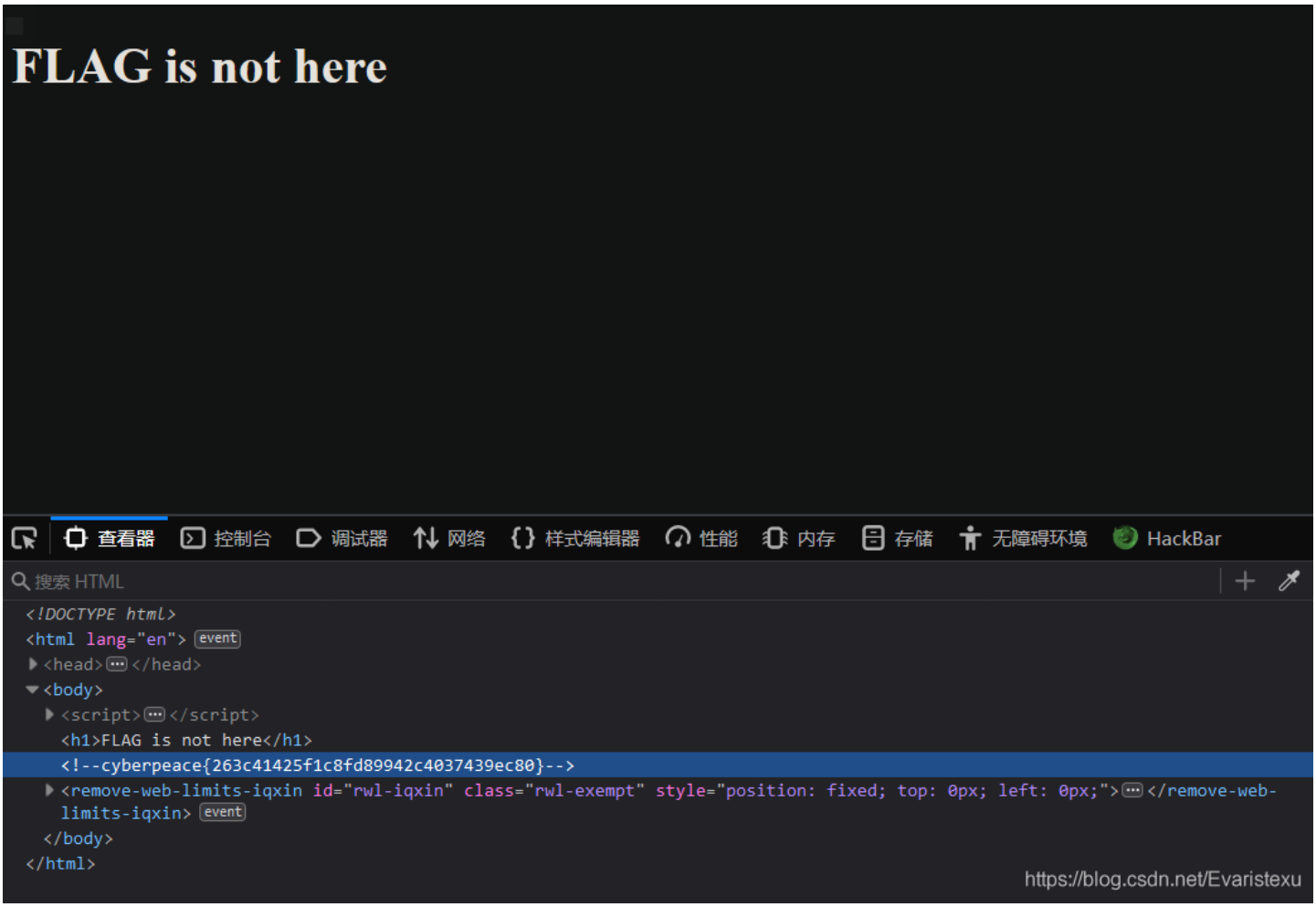
版权

CTF 专栏收录该内容

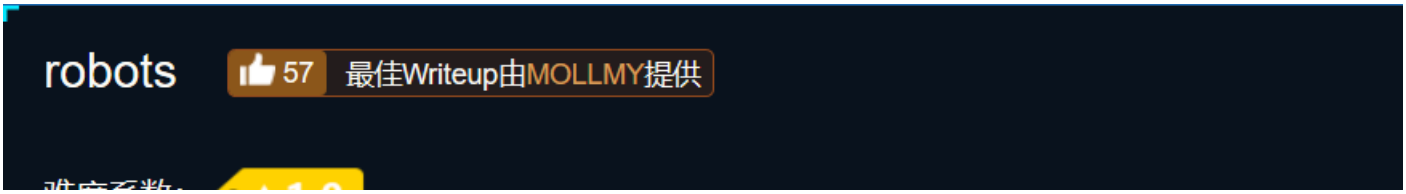
4 篇文章 0 订阅

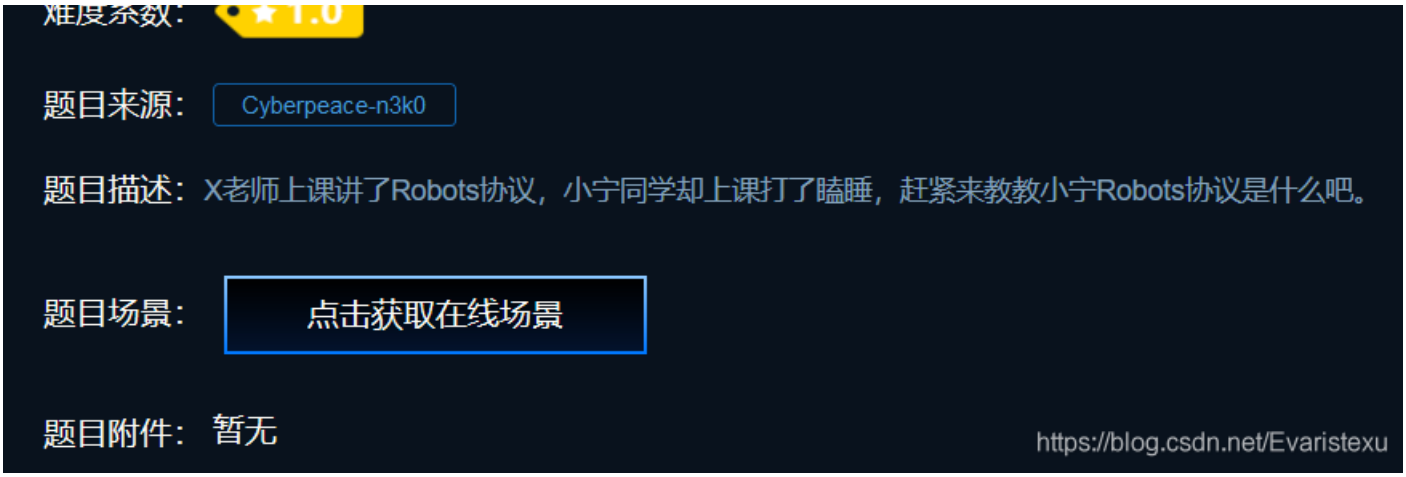
订阅专栏


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

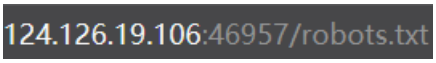

FLAG is not here
查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 HackBar
搜索 HTML
<!DOCTYPE html>
<html lang="en"> event
<head> </head>
<body>
<script> </script>
<h1>FLAG is not here</h1>
<!--cyberpeace{263c41425f1c8fd89942c4037439ec80}-->
<remove-web-limits-iqxin id="rwl-iqxin" class="rwl-exempt" style="position: fixed; top: 0px; left: 0px;"> </remove-web-limits-iqxin> event
</body>
</html>
https://blog.csdn.net/Evaristexu

→F12快捷键


robots
57 最佳Writeup由MOLLMY提供

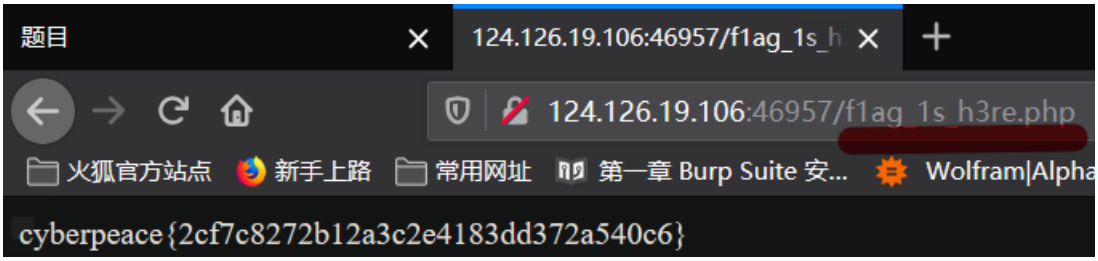


打开后什么提示都没有,打开协议




```
User-agent: *
Disallow:
Disallow: flag_1s_h3re.php
```

访问下方的Disallow



→如何查看网页的robots协议

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

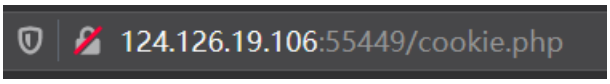
文件

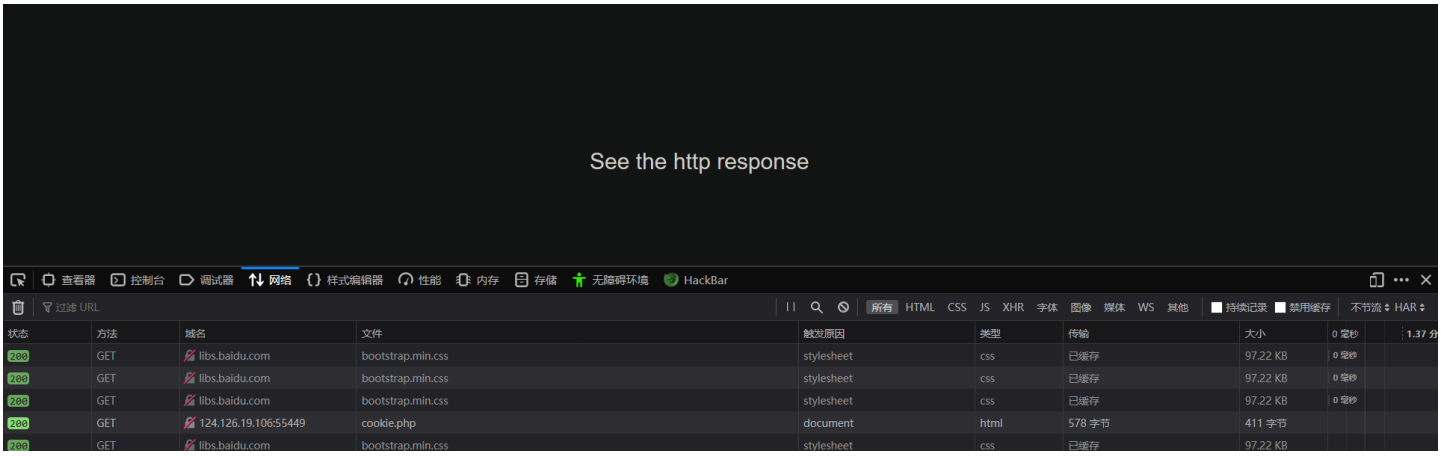
添加了/index.php.bak后自动下载文件，用文本编辑器打开发现flag

→ 备份文件扩展名

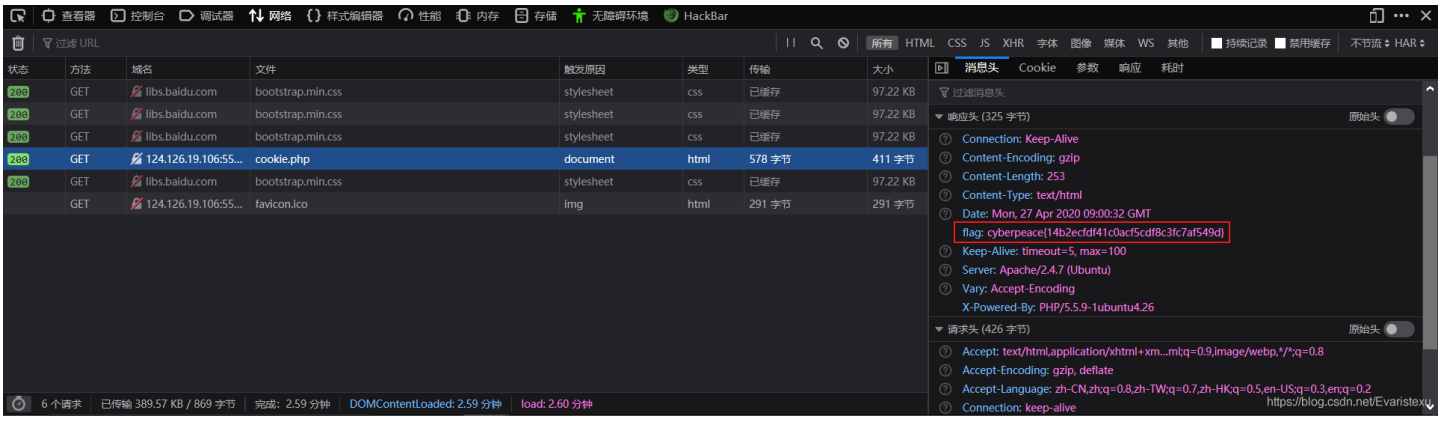
发现cookie.php文件

打开文件

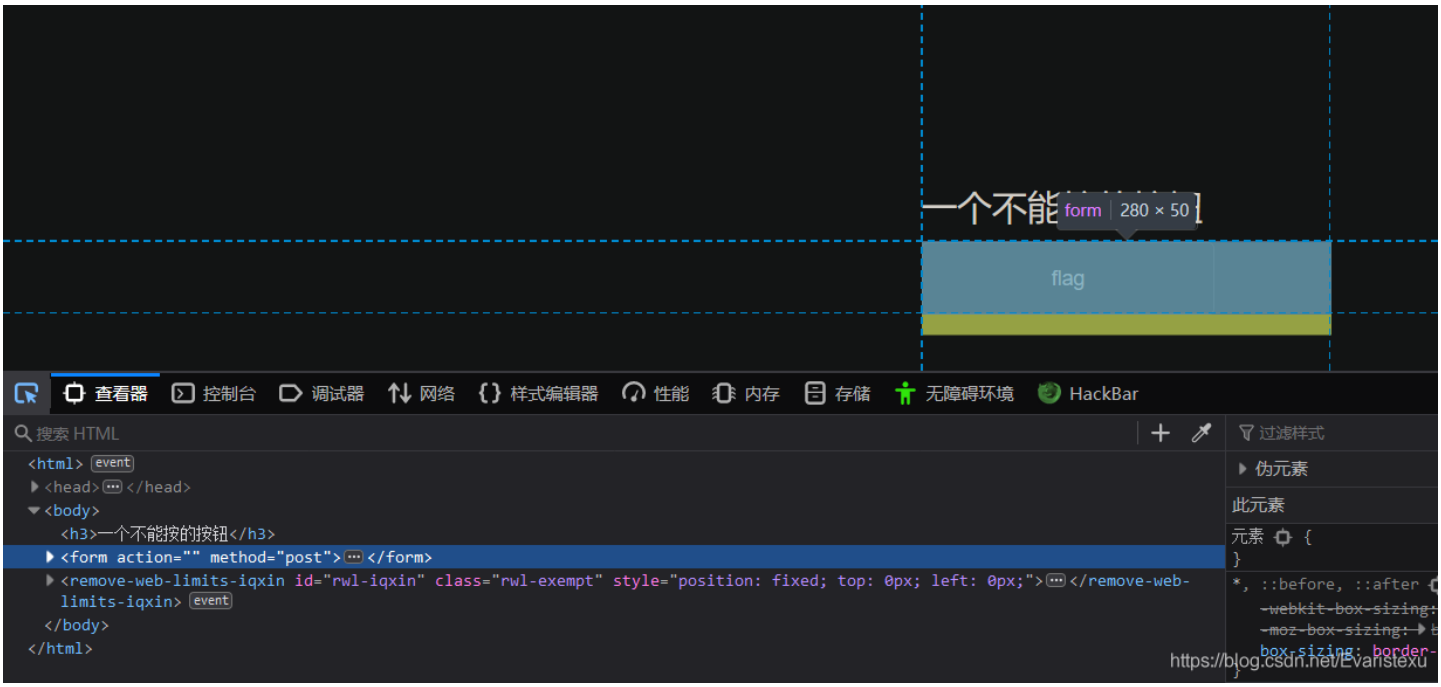


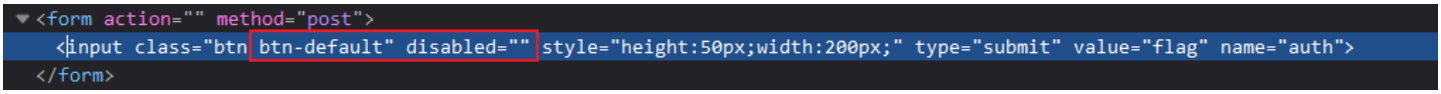


提示查看该文件(cookie.php)的响应



→cookie信息的查看





将disabled改为enabled即可

点击按钮出现flag

前端控件属性修改

随便输入一个,验证失败跳转页面,查看源代码

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>weak auth</title>
</head>
<body>

<script>alert('password error');</script><!--maybe you need a dictionary-->


</body>
</html>

```

https://blog.csdn.net/Evaristexu

使用BurpSuite暴力破解


```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;
}
?>
```

该题的详细解答

_→php基本代码审计