

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。

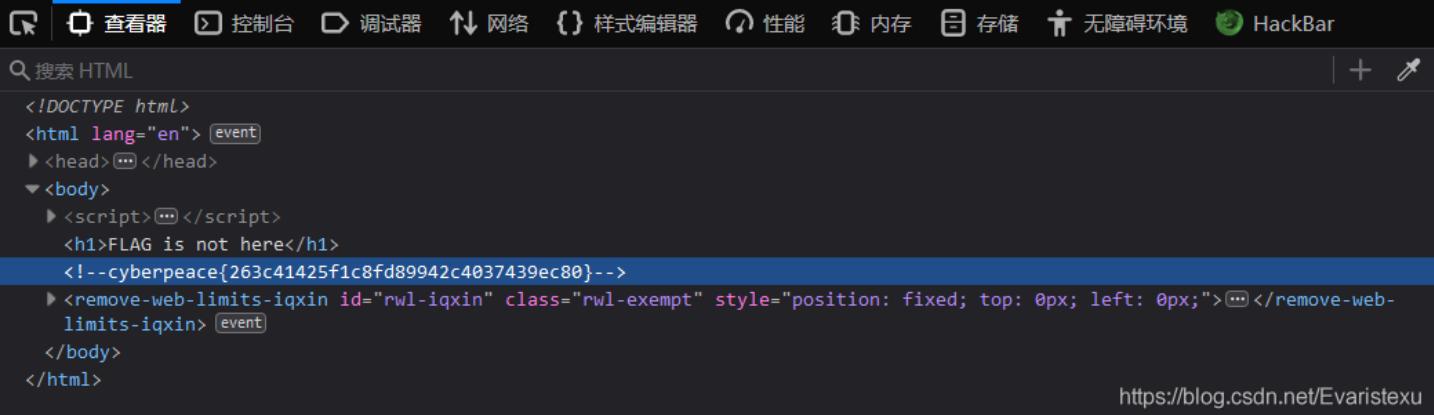
题目场景:

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"> [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

难度系数：

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

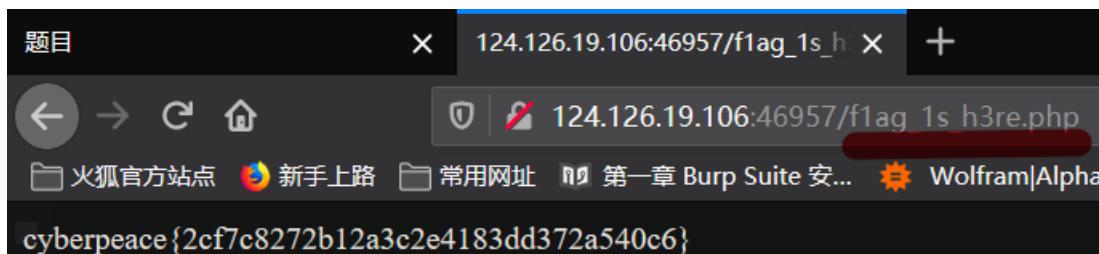
<https://blog.csdn.net/Evaristexu>

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: flag_1s_h3re.php
```

访问下方的Disallow



→ 如何查看网页的robots协议

backup 最佳Writeup由话求 • 樱宁提供

难度系数：

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

cookie 最佳Writeup由**神秘人 · 孔雀翎**提供

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

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？’

题目场景: 4%

题目附件: 暂无 <https://blog.csdn.net/Evaristexu>

你知道什么是cookie吗?

名称	值	Domain	Path	Expires / Max-Age	大小	HttpOnly	Secure	SameSite	最后访问
look-here	cookie.php	124.126.19.106	/	会话	19	false	false	None	Mon, 27 Apr 2020 08:5...

发现cookie.php文件

打开文件

124.126.19.106:55449/cookie.php

See the http response

状态	方法	域名	文件	触发原因	类型	传输	大小	0毫秒	1.37 分
200	GET	# lib.baidu.com	bootstrap.min.css	stylesheet	css	已缓存	97.22 KB	0毫秒	
200	GET	# lib.baidu.com	bootstrap.min.css	stylesheet	css	已缓存	97.22 KB	0毫秒	
200	GET	# lib.baidu.com	bootstrap.min.css	stylesheet	css	已缓存	97.22 KB	0毫秒	
200	GET	124.126.19.106:55449	cookie.php	document	html	578 字节	411 字节		
200	GET	# lib.baidu.com	bootstrap.min.css	stylesheet	css	已缓存	97.22 KB		

提示查看该文件(cookie.php)的响应

The screenshot shows a browser developer tools Network tab. It lists several requests for 'bootstrap.min.css' and one request for 'cookie.php'. The 'cookie.php' request is selected, showing its response details. The 'headers' section of the response shows a 'flag' header with the value 'cyberpeace{14b2ecfdf41c0acf5cdf8c3fc7af549d}'. This value is highlighted with a red box.

→ cookie信息的查看

The screenshot shows a challenge page titled 'disabled_button'. It includes a '难度系数: ★ 1.0' section, a '题目来源: Cyberpeace-n3k0' section, and a '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?' section. Below this is a '题目场景:' section with a URL 'http://124.126.19.106:46032'. The URL is followed by a progress bar and a '删除场景' button. A timer shows '倒计时: 03:59:53' and a '延时' button. At the bottom, it says '题目附件: 暂无' and provides a link 'https://blog.csdn.net/Evaristexu'.



A screenshot of a browser's developer tools element inspector. The element being inspected is a button with the value "flag". A tooltip above the button says "一个不能按的按钮" (A button that cannot be clicked). The element's style is defined by the following CSS rule:

```
* { -webkit-box-sizing: border-box; -moz-box-sizing: border-box; box-sizing: border-box; }
```

The browser's address bar shows the URL: <https://blog.csdn.net/Evaristexu>.

A screenshot of the browser's element inspector showing the HTML code for the button element. The code is as follows:

```
<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

A screenshot of the web page. It contains the text "一个不能按的按钮" (A button that cannot be clicked) and a button with the value "flag". The button is styled with a black background and white text. Below the button, there is some additional text.

→ 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 [延时](#)

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

1 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 [延时](#)

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