

攻防世界新手区

原创

H0ne 于 2021-02-07 16:15:05 发布 2034 收藏 1

文章标签: [web](#)

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/qq_53142368/article/details/113740252

版权

学习目标:

做自己喜欢的事

学习内容:

攻防世界新手区练习

学习时间:

2021年2月6日

学习产出:

1.



The screenshot shows a CTF challenge interface with the following details:

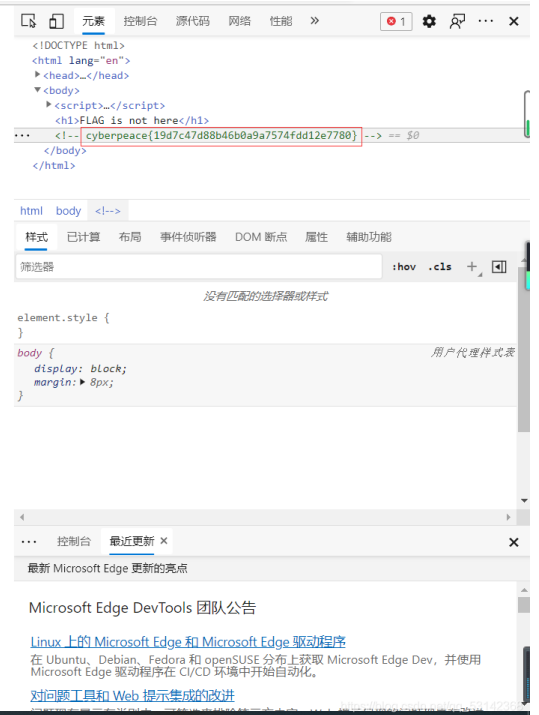
- Challenge Title:** view_source
- Difficulty:** 1.0 (indicated by a yellow star icon)
- Source:** Cyberpeace-n3k0
- Description:** X老师让小宁同学查看一个网页的源代码, 但小宁同学发现鼠标右键好像不管用了。
- Scenario:** 点击获取在线场景
- Attachments:** 暂无
- Metadata:** 148 likes, Best Writeup by Healer_aptx • Anchorite
- Buttons:** WP (Writeup), 建议 (Suggest)
- URL:** https://blog.csdn.net/qq_53142368

打开后会出现

FLAG is not here

查看其HTML

FLAG is not here



2.

← 返回  本题用时: 10分6秒

robots  164 最佳Writeup由MOLLMY提供  

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/qq_53142368

首先需要了解啥是robot协议

Robots协议的详解

Robots协议是Web站点和搜索引擎爬虫交互的一种方式, Robots.txt是存放在站点根目录下的一个纯文本文件。该文件可以指定搜索引擎爬虫只抓取指定的内容, 或者是禁止搜索引擎爬虫抓取网站的部分或全部内容。当一个搜索引擎爬虫访问一个站点时, 它会首先检查该站点根目录下是否存在robots.txt, 如果存在, 搜索引擎爬虫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, 那么搜索引擎爬虫就沿着链接抓取。

另外, robots.txt必须放置在一个站点的根目录下, 而且文件名必须全部小写。如果搜索引擎爬虫要访问的网站地址是 <http://www.w3.org/>, 那么robots.txt文件必须能够通过<http://www.w3.org/robots.txt>打开并看到里面的内容。https://blog.csdn.net/qq_53142368

在其后缀加入robots.txt后得到

```
← → ↻ ⚠ 不安全 | 111.200.241.244:45734/robots.txt ☆ ⚙ 👤 ·  
User-agent: *  
Disallow:  
Disallow: flag_ls_h3re.php
```

https://blog.csdn.net/yg_53142368

然后在URL后面加入f1ag_1s_h3re.php

```
← → ↻ ⚠ 不安全 | 111.200.241.244:45734/f1ag_1s_h3re.php ☆ ⚙ 👤 ...  
cyberpeace(931158a597f5509c33f90e9e81325d13)
```

https://blog.csdn.net/yg_53142368

3.

backup 👍 44 最佳Writeup由 **话求** · 樱宁提供 WP 建议

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: 4%

题目附件: 暂无

https://blog.csdn.net/qq_53142368

打开后

你知道index.php的备份文件名吗?

https://blog.csdn.net/qq_53142368

首先需要了解啥是index.php备份文件名

index.php的备份文件

原创 「已注销」 2020-09-22 20:33:51 293 收藏 版权

文件名: index.php.bak

点赞Mark关注该博主, 随时了解TA的最新博文

https://blog.csdn.net/qq_53142368

所以在URL后面加上index.php.bak

发现bak文件直接打不开, 所以需要在 bak文件所在的文件夹中用记事本的形式打开, 查看他的HTML

```
index.php (11).bak - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
<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>
</html>
```

```
</style>
</head>
<body>
<h3>你知道index.php的备份文件名吗? </h3>
<?php
$flag="Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}"
?>
</body>
</html>
```

第 8 行, 第 30 列 100% Windows (CRLF) UTF-8 3142368

找到cyberspace

4.

World of Attack&Defense

答题 竞赛 排行榜 队伍 商城

返回 本题用时: 10秒

cookie 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老师告诉小宁他在cookie里放了东西, 小宁疑惑地想: '这是夹心饼干的意思吗?'

题目场景: 点击获取在线场景

题目附件: 暂无

https://blog.csdn.net/qq_53142368

首先需要了解啥是cookie协议



你知道什么是cookie吗?

cookie (储存在用户本地终端上的数据)

[编辑](#)
[讨论](#)
[上传视频](#)

本词条由“科普中国”科学百科词条编写与应用工作项目 审核。

Cookie，有时也用其复数形式 Cookies。类型为“小型文本文件”，是某些网站为了辨别用户身份，进行Session跟踪而储存在用户本地终端上的数据（通常经过加密），由用户客户端计算机暂时或永久保存的信息 [1]。

所以在URL上加上cookie.php得到结果是



See the http response

看到这种情况看到提示说查看response，响应头就一定藏着flag

2 个请求 已传输 703 字节 / 578 字节 完成: 1.11 秒 DOMContentLoaded: 716 毫秒

消息头	Cookie	请求	响应	耗时	栈跟踪
传输		578 字节 (大小 411 字节)			
响应头 (325 字节)					
Connection: Keep-Alive					
Content-Encoding: gzip					
Content-Length: 253					
Content-Type: text/html					
Date: Sun, 07 Feb 2021 06:50:30 GMT					
Flag: cyberpeace(cc21423edf64d31d1de02cc4a4005b24)					
Keep-Alive: timeout=5, max=100					
Server: Apache/2.4.7 (Ubuntu)					
Vary: Accept-Encoding					
X-Powered-By: PHP/5.5.9-1ubuntu4.26					
请求头 (423 字节)					
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*; q=0.8					

See the http response

5.

disabled_button 👍 62 最佳Writeup由沐一清提供 WP 建议

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://111.200.241.244:47644

删除场景

倒计时: 03:59:25 延时

题目附件: 暂无

题目已答对

分享wp点赞赚金币哦 马上写
https://blog.csdn.net/qg_5314238



发现点不了这个flag

```

<h3>一个不能按的按钮</h3>
<form action method="post">
  <input disabled class="btn btn-default" style="height:50px;width:200px;"
    type="submit" value="flag" name="auth"> == $0
</form>

```

发现有一个disabled，disabled属性可设置或返回是否禁用单选按钮。所以删掉disabled属性



6.

返回 本题用时: 1时23分0秒 web 积分: 3分

weak_auth 👍 101 最佳Writeup由小太阳的温暖提供 WP 建议

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: 点击获取在线场景

题目附件: 暂无

实时消息
用户C7E0解出Crypto方向
得2.0积分,2金币,耗时1分41
202

https://blog.csdn.net/qq_53142368

随便登陆, 提示说要admin登陆

查看HTML没看到重要信息, 所以需要暴力破解了

用到burp suite (需要Python环境),所以提前先下载Python环境

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	434	
1	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	434	
2	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	437	
3	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	434	
4	abcdef	200	<input type="checkbox"/>	<input type="checkbox"/>	434	

https://blog.csdn.net/qq_53142368

看到这个123456返回长度不一样, 所以密码就是123456, 账号就是admin

← → ↻ ⚠ 不安全 | 111.200.241.244:53107/check.php

cyberpeace{643cbf1566ec38ac31e1b057a29535fa}

https://blog.csdn.net/qq_53142368

7.

simple_php

👍 143 最佳Writeup由MOLLMY提供


WP

建

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://111.200.241.244:30055

删除场景

倒计时: 03:55:30

延时

题目附件: 暂无

https://blog.csdn.net/qq_53142368

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

https://blog.csdn.net/qq_53142368

php中其中两种比较符号:

==: 先将字符串类型转化成相同, 再比较

===: 先判断两种字符串的类型是否相等, 再比较

注: <、>、<=、>=都存在和==相同的弱类型, 原理相同!!!

分析代码, 需要满足\$ a==0 and \$b>1234,b还不能是数字

我们使a=true 当比较时true转换为0 输出前半段

b=2000a 比较时转换为2000>1234.输出后半段

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

Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}

https://blog.csdn.net/qq_53142368

8.

返回 本题用时: 1分20秒

get_post 64 最佳Writeup由神秘人·孔雀翎提供 WP 建议

难度系数: ★★2.0

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: 0%

题目附件: 暂无

https://blog.csdn.net/qq_53142368

请用GET方式提交一个名为a,值为1的变量

https://blog.csdn.net/qq_53142368

这一看就是考get post呗

火狐官方网站 新手上路 常用网址 京东商城 来自 Microsoft Edge

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{e1f1c7ccee4a970d7039ee2ba0e7f876}



get方式提交即url上输入

post提交使用火狐浏览器(需要用到hackbar插件)

12.

返回
本题用时: 19分45秒

simple_js
688 最佳Writeup由Venom • IceM提供
WP
建

难度系数: ★★★★ 3.0

题目来源: root-me

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})

题目场景: 点击获取在线场景

题目附件: 暂无

https://blog.csdn.net/qq_53142368

打开页面后让你输入密码, (放心, 你是不可能输入对的)
查看页面的源代码

```

1 <html>
2 <head>
3 <title>JS</title>
4 <script type="text/javascript">
5 function dechiffre(pass_enc){
6   var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
7   var tab = pass_enc.split(',');
8   var tab2 = pass.split(',');var i, j, k, l=0, m, n, o, p = "", i = 0; j = tab.length;
9   k = j + (l) + (n=0);
10  n = tab2.length;
11  for(i = (o=0); i < (k = j = n); i++) {o = tab[i-1];p += String.fromCharCode(o = tab2[i]);
12    if(i == 5)break;}
13  for(i = (o=0); i < (k = j = n); i++) {
14    o = tab[i-1];
15    if(i > 5 && i < k-1)
16      p += String.fromCharCode(o = tab2[i]);
17  }
18  p += String.fromCharCode(tab2[17]);
19  pass = p;return pass;
20 }
21 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");
22
23 h = window.prompt("Enter password");
24 alert( dechiffre(h) );
25
26 </script>
27 </head>
28 </html>
29
30 </html>
31

```

https://blog.csdn.net/qq_53142368

发现了重要的东西
有2c 明显是十六进制
将这些十六进制数转换成十进制后,
55,56,54,79,115,69,114,116,107,49,50
sacl处理后得到
Cyberpeace{786OsErtk12}

- -
 -
- 9, 10, 11题小白还没弄懂, 等小白弄懂后, 再在上面补充。*