

# xctf 攻防世界 web

原创

[poggiouxay](#) 于 2021-03-13 17:54:31 发布 4755 收藏 18

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/m0\\_55854679/article/details/114597133](https://blog.csdn.net/m0_55854679/article/details/114597133)

版权

## 文章目录

### [xctf 攻防世界 web新手区](#)

#### [001 view source](#)

原理：

方法1：

方法2：

方法3：

方法4：

#### [002 robots](#)

原理：

方法：

#### [003 backup](#)

原理：

方法：

#### [004 cookie](#)

原理：

方法：

#### [005 disabled\\_button](#)

方法：

#### [006 weak\\_auth](#)

原理：

方法：

#### [007 simple\\_php](#)

原理

方法：

#### [008 get\\_post](#)

原理：

方法：

#### [009 xff\\_referer](#)

原理：

方法:

010 webshell

原理:

方法1:

方法2:

011 command\_execution

原理:

方法:

012 simple\_js

原理:

方法:

## xctf 攻防世界 web新手区

### 001 view source

**FLAG is not here**

[https://blog.csdn.net/m0\\_55854679](https://blog.csdn.net/m0_55854679)

**原理:**

查看网页源码。(前端js禁用鼠标左键和右键,导致右键无法查看源码)。

**方法1:**

1. 按F12键打开开发者工具;
2. cyberpeace{80816c5d107e33f3103324c8c4de1d91} 即为所要找的flag。



## 方法2:

在网页url前面添加 `view-source:`

## 方法3:

使用burp抓包传到“repeater”里面，点击“go”即可查看源代码。

## 方法4:

- 1.浏览器禁用js（以火狐浏览器为例）
- 2.在地址栏输入 `about:config` 点击回车键
- 3.点击“了解此风险”
- 3.在搜索地址栏中输 `javascript.enabled`
- 4.鼠标右键第一个 `javascript.enabled` ,再点击切换值由true变成false时候说明已经关闭。



## 002 robots

### 原理:

robots.txt是搜索引擎中访问网站的时候要查看的第一个文件。当一个搜索蜘蛛访问一个站点时，它会首先检查该站点根目录下是否存在robots.txt，如果存在，搜索机器人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，所有的搜索蜘蛛将能够访问网站上所有没有被口令保护的页面。

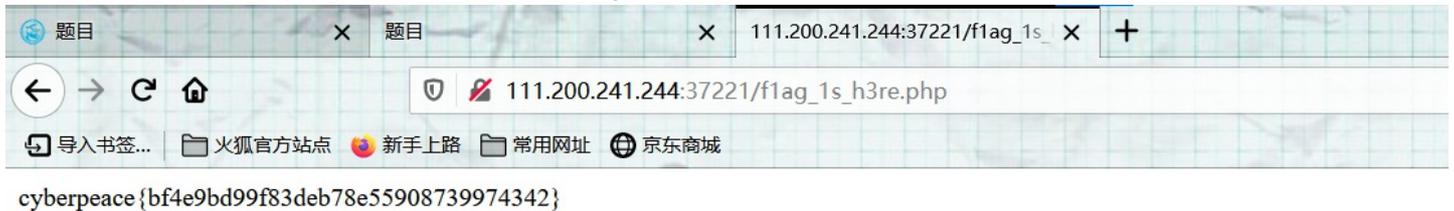
### 方法:

1.在网页的url后面添加 `/robots.txt`，发现有一个不允许访问的php文件；



[https://blog.csdn.net/m0\\_55854679](https://blog.csdn.net/m0_55854679)

2.在网页url后边添加这个php文件路径，访问它爆出flag。



[https://blog.csdn.net/m0\\_55854679](https://blog.csdn.net/m0_55854679)

3.cyberpeace{bf4e9bd99f83deb78e55908739974342}即为所要找的flag。

## 003 backup

原理：

常见的备份文件后缀名有：`.git .svn .swp .svn .~ .bak .bash_history`。

方法：

你知道index.php的备份文件名吗？

- 1.逐一尝试常用的文件名后缀，发现是 `.bak`；
- 2.在网页url后面添加 `/index.php.bak`；



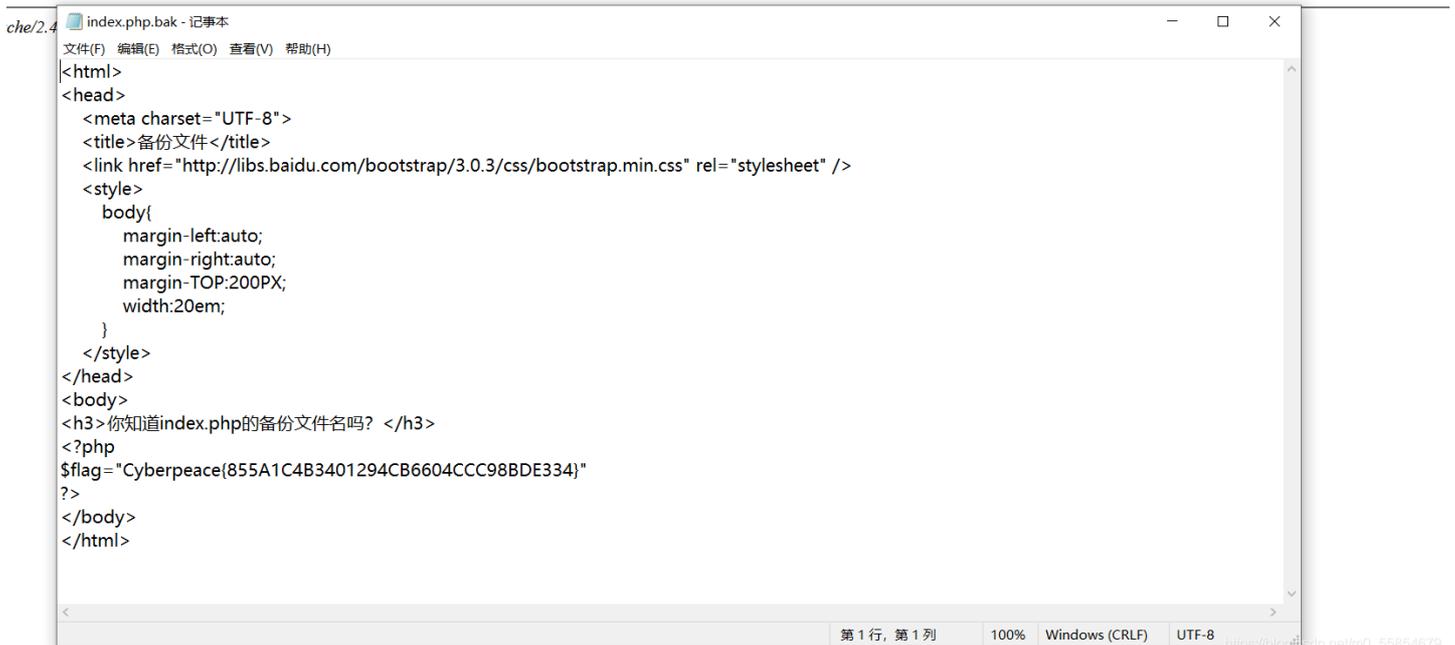
## Not Found

The requested URL / index.php.bak was not found on this server.

Apache/2.4.7 (Ubuntu) Server at 111.200.241.244 Port 54835

- 3.访问此网页将会跳转至该网页的源码；

requested URL / index.php.bak was not found on this server.



- 4.Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}即为所要找的flag。

## 004 cookie

### 原理：

Cookie是当主机访问Web服务器时，由 Web 服务器创建的，将信息存储在用户计算机上的文件。一般网络用户习惯用其复数形式 Cookies，指某些网站为了辨别用户身份、进行 Session 跟踪而存储在用户本地终端上的数据，而这些数据通常会经过加密处理。

### 方法：

你知道什么是cookie吗？

[https://blog.csdn.net/m0\\_55854679](https://blog.csdn.net/m0_55854679)

- 1.按F12键打开开发者工具；
- 2.在存储一栏中可以看到 `look-here cook.php`；



- 3.在网页url后面添加 `/cookie.php` 并访问；



See the http response

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	Tue, 09 M

4.在网络一栏点击查看 `cookie.php` 的数据包，在消息头一栏中data下方即为我们要找的flag `cyberpeace{10b877df52e8426bc4336e90c2ca4c6c}`。

See the http response

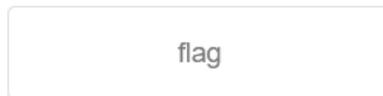
The screenshot shows the browser's developer tools network tab. A request to `cookie.php` is selected. The response headers are expanded, showing the following information:

- Content-Length: 253
- Content-Type: text/html
- Date: Tue, 09 Mar 2021 12:07:39 GMT
- flag: cyberpeace{10b877df52e8426bc4336e90c2ca4c6c}
- Keep-Alive: timeout=5, max=100
- Server: Apache/2.4.7 (Ubuntu)

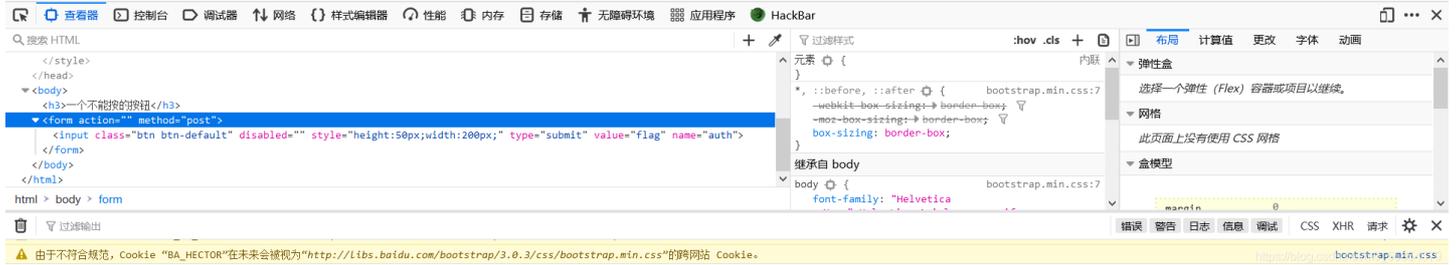
## 005 disabled\_button

方法:

一个不能按的按钮



- 1.按F12键打开开发者工具;
- 2.在查看器一栏下的源码 disabled 改为 able 或将“disabled=”删去;

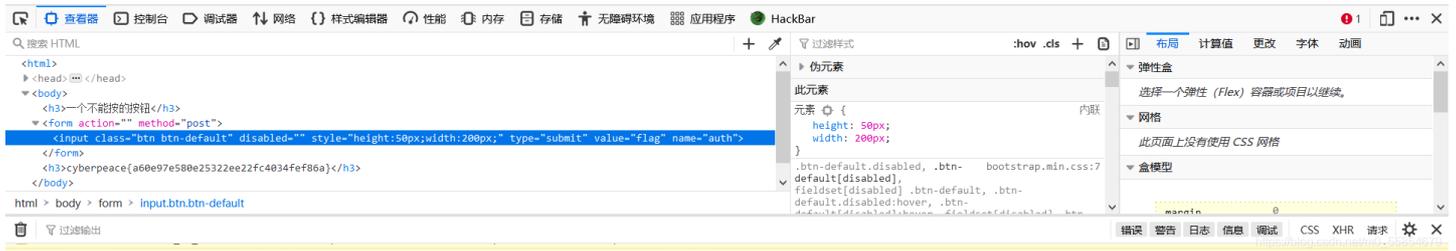


3.点击按钮，cyberpeace{a60e97e580e25322ee22fc4034fef86a}即为我们要找的flag。

一个不能按的按钮



cyberpeace{a60e97e580e25322ee22fc4034fef86a}



## 006 weak\_auth

原理:

弱口令(weak password)没有严格和准确的定义，通常认为容易被别人（他们有可能对你很了解）猜测到或被破解工具破解的口令均为弱口令。弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等。

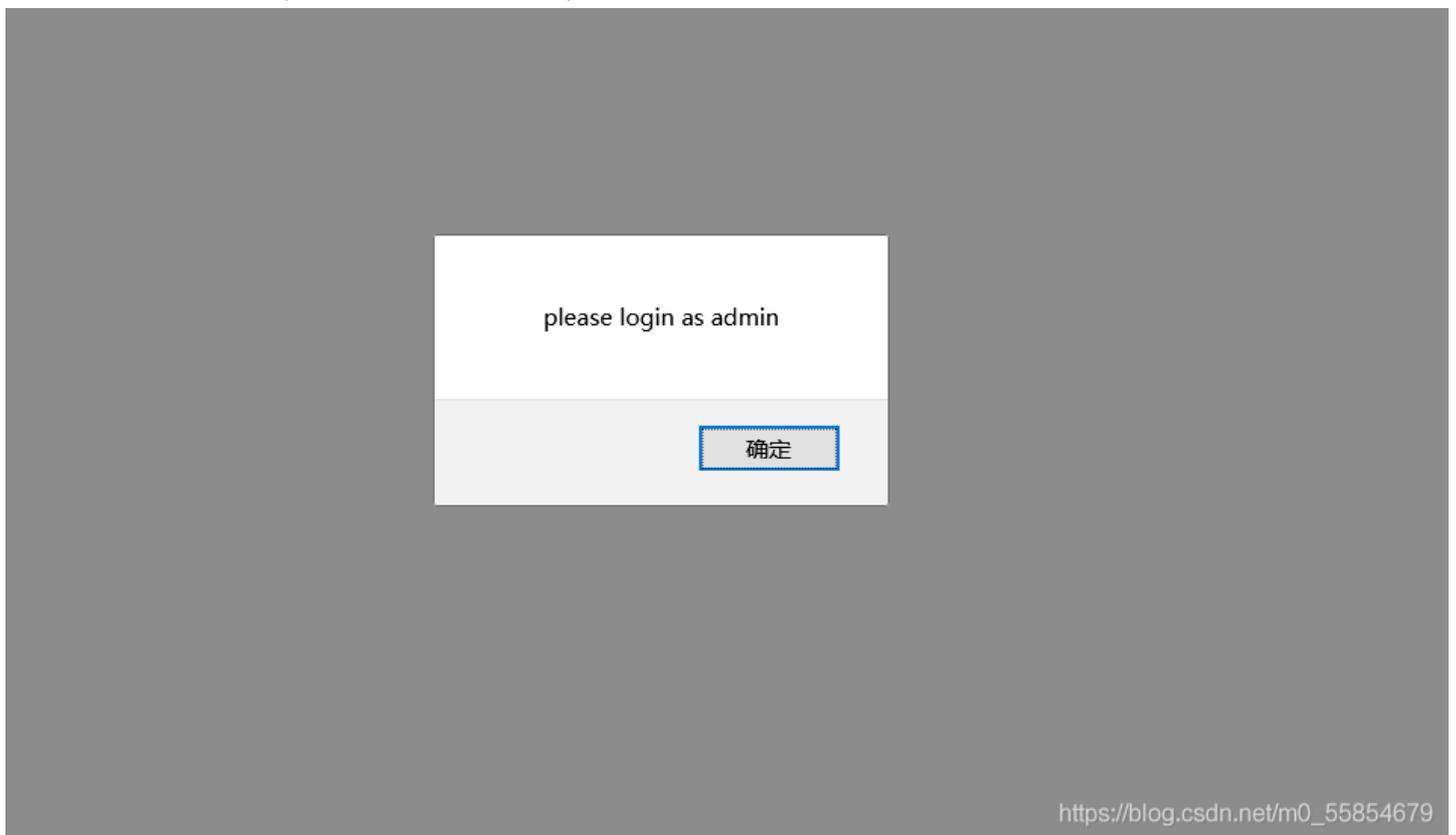
方法:

# Login



[https://blog.csdn.net/m0\\_55854679](https://blog.csdn.net/m0_55854679)

1.随便输入用户名和密码,提示要用admin用户登入;



2.使用 **burpsuite** 截下登录的数据包,把数据包发送到 **intruder** 爆破;

3.加载字典, 查看响应包列表, 发现密码为123456时, 响应包的长度和别的.不一样., 即为正确的密码。

4.输入正确的用户名和密码, 即发现我们要找的flag。

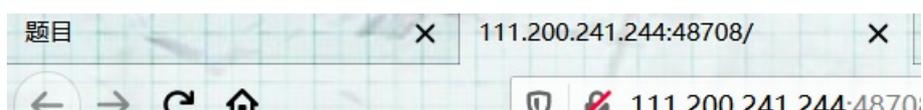
## 007 simple\_php

### 原理

php弱类型, **作用是将两个变量转换成相同类型再比较,而必须是两个变量类型相同值也相同才会返回真。** `is_numeric($num)`表示如果num是数字或数字字符串则返回true, 否则返回false。

如果num是字符串类型, 则会从前读到第一个非数字后停止, 只截取前面的数字字符部分。

### 方法:





```
<?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/m0\\_55854679](https://blog.csdn.net/m0_55854679)

- 1.进行代码审计，发现同时满足 `$a==0` 和 `$a` 时，显示flag1。
- 2.php中的弱类型比较会使'abc' == 0为真，所以输入a=abc时，可得到flag1（abc可换成任意字符）。
- 3.在网页url后面添加 `/index.php?a=abc`，访问此网页，即可发现我们要找的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;
}
?>
```

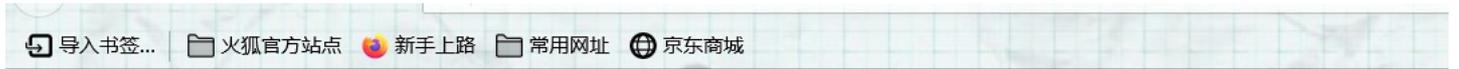
Cyberpeace{647E37C7627CC3E401

[https://blog.csdn.net/m0\\_55854679](https://blog.csdn.net/m0_55854679)

## 原理:

通过url使用get传参格式: 网址?参数名=值&参数名=值。有时需要在?前面加个/。

## 方法:



# 请用GET方式提交一个名为a,值为1的变量

[https://blog.csdn.net/m0\\_55854679](https://blog.csdn.net/m0_55854679)

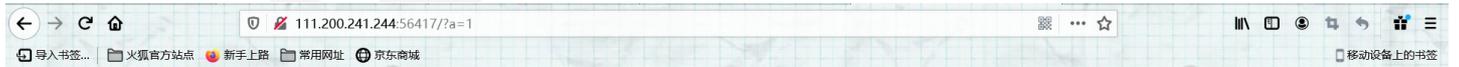
- 1.使用火狐浏览器按F12键打开开发者工具,使用hackbar插件;
- 2.打开hackbar,用get方式传递a=1,即在网页url后面添加 `/?a=1`;

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



- 3.勾选Post data,并输入 `b=2`,点击 **Execute**,即可发现我们要找的flag. `cyberpeace{4d7b677cdfd350b39e50fc89c4341322}`



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{4d7b677cdfd350b39e50fc89c4341322}`



## 009 xff\_referer

### 原理:

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。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。

### 方法:

ip地址必须为123.123.123.123

[https://blog.csdn.net/m0\\_55854679](https://blog.csdn.net/m0_55854679)

- 1.使用burpsuite抓包，修改http头为 X-Forwarded-For ,在请求中加入 X-Forwarded-For: 123.123.123.123 ；
- 2.得到响应，发现还要来自谷歌，接着继续在请求头内添加 Referer: https://www.google.com 。

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' section displays the following text:

```

1 GET / HTTP/1.1
2 Host: 111.200.241.244:41530
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 Upgrade-Insecure-Requests: 1
9 X-Forwarded-For: 123.123.123.123
10 Referer: https://www.google.com
11 Cache-Control: max-age=0

```

The 'Response' section displays the following HTML code:

```

23 </head>
24 <body>
25   <p id="demo">
26     ip00000123.123.123.123
27   </p>
28   <script>
29     document.getElementById("demo").innerHTML="0000https://www.google.com";
30   </script>
31   <script>
32     document.getElementById("demo").innerHTML="cyberpeace{2ee2c35520202ddf77898a62f3764043}";
33   </script>
34 </body>
35 </html>

```

3.cyberpeace{2ee2c35520202ddf77898a62f3764043}即为我们要找的flag。

## 010 webshell

### 原理：

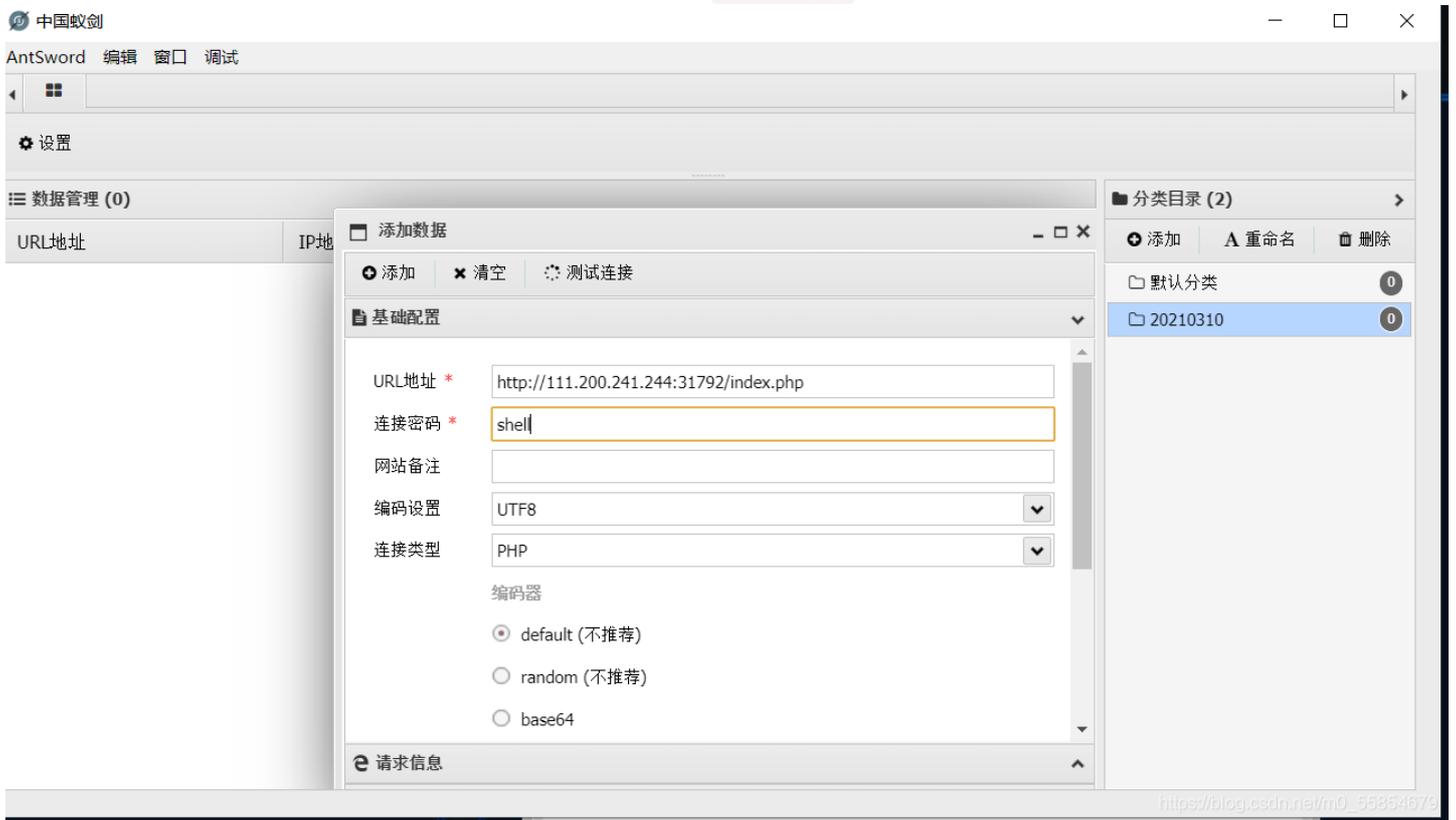
利用文件上传漏洞，往目标网站中上传一句话木马，然后你就可以在本地通过中国菜刀chopper.exe即可获取和控制整个网站目录。@表示后面即使执行错误，也不报错。eval（）函数表示括号内的语句字符串什么的全都当做代码执行。\$\_POST['attack']表示从页面中获得attack这个参数值。

### 方法1：

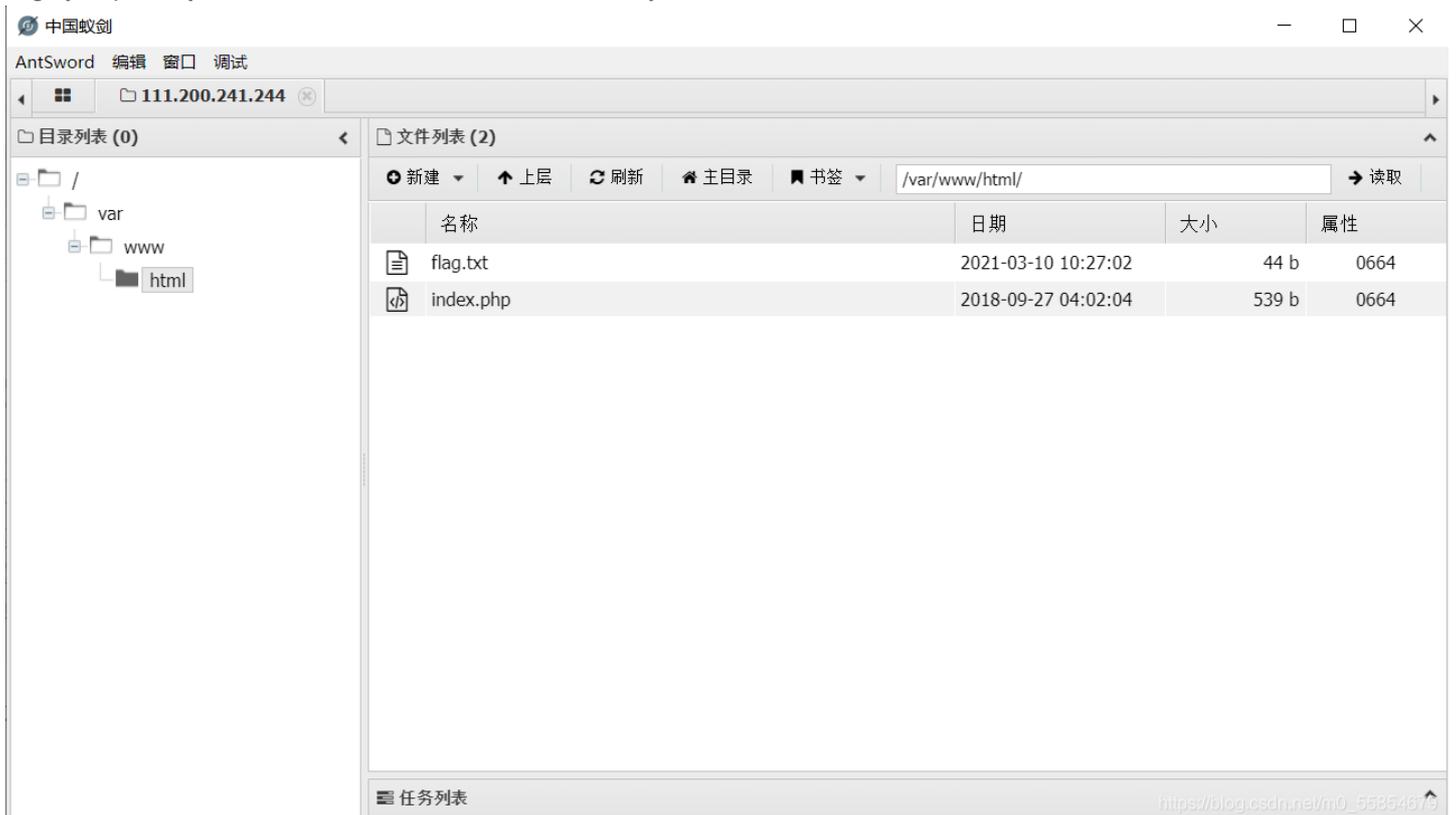
你会使用webshell吗？

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

- 1.题目给了一句话木马，密码即为 `shell`；
- 2.利用蚁剑连接，单击右键，“添加数据”，在网页的url后面添加 `/index.php` ,点击测试连接；



- 3.连接成功后，点击"添加数据"页面左上角的“添加”，就可以在网站目录下面看到 `flag.txt` 的文件，点击即可发现我们要找的 `flag cyberpeace{d0cd04ece3bdd323e226055e04acd3c6}`。



## 方法2:

1.按F12键打开开发者工具;

2.勾选 `post data`;

你会使用webshell吗?

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



3.使用post传参 `shell=system('cat flag.txt')`，即可发现我们要找的flag。

```
cyberpeace{d79db190eaac2fc9f3c398720832a143}
```

## 011 command\_execution

### 原理:

Web应用防护系统（也称为：网站应用级入侵防御系统。英文：Web Application Firewall，简称：WAF）。

WAF对来自Web应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站进行有效防护。

|的作用为将前一个命令的结果传递给后一个命令作为输入。

&&的作用是前一条命令执行成功时，才执行后一条命令。

ls命令用于显示指定工作目录下之内容（列出目前工作目录所含之文件及子目录）

cat 命令用于连接文件并打印到标准输出设备上。

ping是定位网络通不通的一个重要手段。ping是用来探测本机与网络中另一主机之间是否可达的命令，如果两台主机之间ping不通，则表明这两台主机不能建立起连接。

### 方法:



# PING

[https://blog.csdn.net/m0\\_55854679](https://blog.csdn.net/m0_55854679)

- 1.执行一个ping带一个其他命令试试，可以能看到当前目录下的文件；
- 2.一直查看上一级目录 `1 | ls ../`，直到发现 `home` 文件中的 `flag.txt`；
- 3.利用cat命令打开flag文件 `,1 | cat ../../../../home/flag.txt`，得到flag.

## 012 simple\_js

原理：

javascript的代码审计

方法：



- 1.随便输入一段密码，跳转至空白界面后点击鼠标右键，查看页面源代码；
- 2.进行代码审计，发现不论输入什么都会跳到假密码，真密码位于 `fromCharCode`。

```

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

```

|| 英 ⌂ · 简 ☺ ⚙

- 3.将字符串用python处理，得到数组[55,56,54,79,115,69,114,116,107,49,50];

```

s="\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"
print(s)

```

- 4.将得到的数组用chr()函数处理，可得到字符串786OsErk12，规范flag格式，即可得到我们所要找的flag cyberpeace{786OsErk12}。

```

a=[55,56,54,79,115,69,114,116,107,49,50]
c=""
for i in a:
    b=chr(i)
    c=c+b
print(c)

```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)