# xctf 攻防世界 web

# 原创

poggioxay ① 于 2021-03-13 17:54:31 发布 ② 4755 论 收藏 18 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。本文链接: <u>https://blog.csdn.net/m0\_55854679/article/details/114597133</u>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

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。

□ 查看器 D 控制台 D 调试器 ↑↓ 网络 {} 样式编辑器 ○	性能 🚯 内存 😑 存储 肯 无障碍环境 🎬 应用程序 🧃	HackBar
Q、搜索 HTML	+	※ ▼ 过滤样式 :hov .cls +
<pre></pre> //remain and a contract of the cont		元素 🗘 { 内联
<pre><body> @@@<td></td><td></td></body></pre>		
<pre></pre> / /  //tal> html > body		

# 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trun变成false时候说明已经关闭。

④ 导入书签 □火狐首方站点 ● 新手上路 □常用网址 ● 京东商城 ● Get the pikachu		□ 移动设备上的书签
Q java		
browser.urlbar.filter.javascript	true	⇒
javascript.enabled	false	<b>⇒</b>
javascript.options.asmjs	true	⇒
javascript.options.asyncstack	true	⇒
and the second	- Interstrate	og.csan.netrnu, 55854879

## 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。

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;

⑧ 题目	×题目	×	111.200.241.244:37221/robots.tv X	+		A H	
(← → C'	۵	✓ 111.200.241.244:3722	1/robots.txt				
<b>9</b> 导入书签	🖹 火狐官方站点 🍯 新手	路 📄 常用网址 🖨 京东商城					

User-agent: \* Disallow: Disallow: flag\_1s\_h3re.php

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。

<ul><li>&gt;</li></ul>	题目	×	111.200.241.244:37221/f1ag_1s_ × +							
(←) → C <sup>(h)</sup> (♥) <sup>(µ)</sup> 111.200.241.244:37221/f1ag_1s_h3re.php										
<ul> <li>日 导入书签</li> <li>一 火狐官方站点</li> <li>(a) 新手上路</li> <li>一 常用网址</li> <li>伊 京东商城</li> </ul>										

cyberpeace {bf4e9bd99f83deb78e55908739974342}

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?

https://blog.csdn.net/m0\_55854679

1.逐	一尝ì	式常	用的文件	名后缀,为	发现是 <mark>.bak</mark> ;					
2.在	网页ι	』rl后	面添加/	index.php	.bak ;					
题目				×	404 Not Found	×	+			THE
+	$\rightarrow$	G	ŵ		۹ 111.200.241.2	244:54835/in	dex.php.	.bak		
Ðé	入书名	\$	<b>一</b> 火狐1	官方站点 🧯	新手上路 🧎 常用网址	京东商城				

# 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

https://blog.csdn.net/m0\_55854679

#### 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.

2.4	] index.php.bak - 记事本				_	- ×	
3	5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>						
	<li><li>k href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet"</li></li>	/>					
	<style></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td>body{</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td>margin-left:auto;</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td>margin-right:auto;</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td>margin-TOP:200PX;</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td>width:20em;</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><th></th><th>}</th><th></th><th></th><th></th><th></th><th></th><th></th></tr><tr><td></td><td></style>						
<	/head>						
<	body>						
<	h3>你知道index.php的备份文件名吗?						
<	?php						
\$	flag="Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}"						
?	>						
<	/body>						
<	/html>						
						~	
<						>	
		第1行, 第1列	100%	Windows (CRLF)	UTF-8	https://block	

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

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;

□ ① 查看器 ② 控制台 □ 调试器 1 网络 { } 样式编辑器 ① 性能 ① 内存 日 存储 1 无趣得环境 2 照 应用程序 ● HackBar												
	▼ 项目过滤器									+ C 🖻	▼ 过滤值	
http://111.200.241.244:42621	名称	值	Domain	Path	Expires / Max-Age	大小	HttpOnly	Secure	SameSite	最后访问	▼ 数据	^
<ul> <li>▷ ☐ Indexed DB</li> <li>▷ 급 本地行館</li> <li>▷ 급 本地行館</li> <li>▷ 급 法存銷</li> <li>▷ 偿存存館</li> </ul>	look-here	cookle.php	111.200.241.244	/	<b>会話</b>	19	false	false	None	Tue, 09 Mar 2021 11:56	▼ look-here: 'cookie.php' Domain: '111.200.241.244' Expires / Max-Age: '金融' HostOnly: true HttpOnly: false Path: '/' SameSite: 'None' Secure: false	v
● 7 过速输出										错误 磐	告日志信息调试 CSS XHR	请求 🔅 🗙

#### 3.在网页url后面添加 /cookie.php 并访问;

← → ୯ ɗ	0 💋 111.200.241.244:42621/cookie.php	题 … 公	₹ III.	۲	4
●导入书签 [	] 火狐官方站点 🤞 新手上路 🛅 常用网址 🌐 京东商城				C

え 白 査看器 🖸 控制台 D 调试器	器 ↑↓ 网络 {}样	式编辑器 🕥 性能 🕕 P	9存 🗄 存储 肯 无	障碍环境 闘 应用科	副字 🕘 HackBar					
E Cookie	▼ 项目过滤器									
http://111.200.241.244:42621	名称	值	Domain	Path	Expires / Max-Age	大小	HttpOnly	Secure	SameSite	最后访问
E Indexed DB	look-here	cookie.php	111.200.241.244	1	会话	19	false	false	None	Tue, 09 M
日本地存储										
🗄 会话存储										
■ 緩存存储										

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

R	○ 査君器	▶ 控制台 ▶ 调试器	▶ 网络 {}样式编辑器 ⑦ 性能 ② 内存	🗄 存储 肯 无障碍环境 🖁	器 应用程序	HackBar			<b>9</b> 1 🗍 … X
Û	▼ 过滤 URL						II Q Ø	所有HTML CSS JS XHR 字体图像》媒体WS 其他	禁用缓存 不节流 🕻 🔅
状态	方法	域名	文件	发起者	类型	传输	大小	D 消息头 Cookie 请求 响应 耗时	
200	GET	🔏 111.200.241.244:4	cookie.php	document	html	578 字节 (已竟速)	411 字节	▼ 过滤消息头	拦截 重发 ♥
404	GET	🔏 111.200.241.244:4	favicon.ico	FaviconLoader.jsm:19.	. html	已缓存	292 字节	<ul> <li>Content-Length: 253</li> </ul>	^
								Content-Type: text/html     Date: Tue, 09 Mar 2021 12:07:39 GMT     flag: cyberpeace(10b877df52e8426bc4336e90c2ca4c6c)     Keeo-Alive: timeout=5. max=100	
Ō	2 个请求 已	传输 703 字节 / 578 字节	完成: 386 毫秒 DOMContentLoaded: 291 毫秒	load: 305 毫秒				③ Server: Abache/2.4.7 (Ubuntu)	~
Û	▼ 过滤输出							错误警告日志信息调试	CSS XHR 请求 🗘 🗙
►	GET http://11	1.200.241.244:42621/fa	vicon.ico					[HTTP/	1.1 404 Not Found Oms]

# 005 disabled\_button

方法:



flag

#### 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;

□ 查看器 ○ 控制台 ○ 调试器 ↓ 网络 { } 样式编辑器 ○ 性能 ① 内存 目 存储 〒 无障碍环境 2 照 应用程序	HackBar	0 ··· ×
Q. 搜索 HTML	+ ✔ 〒过滤样式 :hov.cls + 🗈 🗊 布局 计算值 更改 字体 动	画
	へ 元素 ゆ { 内联 ヘ ▼ 弾性盒	^
Cody>	,::before, ::after 🗅 { bootstrap.min.css:7 选择一个弹性 (Flex) 容器或项目以继续。	
<h3>一个不能按的按钮</h3> ▼ <form action="" method="post"></form>	-webkit box sizing: » border box; マ -moz-box-sizing: » border-box; マ	
<pre><input class="btn btn-default" disabled="" name="auth" style="height:50px;width:200px;" type="submit" value="flag"/></pre>	> box-sizing: border-box; 此页面上没有使用 CSS 网格	
	继承自 body ▼ 盒模型	
	<pre>body</pre>	
html > body > form	font-family: "Helvetica wargin 0	×
■ 7 过迷输出	错误 警告 日志 信息 调试 CSS XHF	∛ 请求 🔆 🗙
▲ 由于不符合规范, Cookie "BA_HECTOR"在未来会被视为"http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css"的跨网站 Cooki	de. https://blog.cso.bo	otstrap.min.css

flad

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}

□ 查看器 ② 控制台 □ 调试器 1 网络 {} 样式编辑器 □ 性能 ① 内存 目 存储 十 无障碍环境 譅 应用程序	HackBar	<b>9</b> 1 🗇 … ×
Q. 搜索 HTML	- 🖋 🗑 过滤样式 :hov.cls +	・ 🗈 🖬 布局 计算值 更改 字体 动画
<pre>chtml&gt; b devide @ c (bood)</pre>	^ ▶ 伪元素	^ ▼弹性盒 ^
<pre>read&gt; </pre> <pre> * <body> </body></pre>	此元素	选择一个弹性 (Flex) 容器或项目以继续。
<h3>一个不能設め识皮钮</h3> ▼ <form action="" method="post"></form>	元素 • {	<sup>为联</sup> ▼ 网格
<pre><input class="btn btn-default" disabled="" name="auth" style="height:50px;width:200px;" type="submit" value="flag"/> <td>width: 200px;</td><td>此页面上没有使用 CSS 网格</td></pre>	width: 200px;	此页面上没有使用 CSS 网格
<hr/>	.btn-default.disabled, .btn- bootstrap.min.cs default[disabled],	5:7 ▼ 盒模型
html > body > form > input.btn.btn.default	<pre>fieldset[disabled] .btn-default, .btn- default.disabled:hover, .btn- default[disabled].btm</pre>	v mannin 0 v
		错误警告告日志信息。调调试CSSXHR请求 🔆 🗙
		111020000000000000000000000000000000000

# 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。



	$\sim$		
IU	u		
	-		

reset

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;

	please login as admin	
	确定	
2使用 <u>burnsuite</u> 截下登录的数据包 拍		https://blog.csdn.net/m0_55854679

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,<mark>作用是将两个变量转换成相同类型再比较,而</mark>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。



https://blog.csdn.net/m0\_55854679

进行代码审计,发现同时满足 \$a==0 和 \$a 时,显示flag1。
 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)。
 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。

```
←
   \rightarrow C
           ŵ
                              111.200.241.244:48708/index.php?a=abc
日 导入书签... 
火狐官方站点 
新手上路 
常用网址 
京东商城
<?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
```

### 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:

日 导入书签... 一 一 火狐官方站点 🥶 新手上路 🦳 常用网址 🖨 京东商城

# 请用GET方式提交一个名为a,值为1的变量

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

□ 查看器	D 控制台 D 调试器 1↓网络 {}样式编辑器 ① 性能 ① 内存 🗄 存储 🛉 无臁碍环境  应用程序 🖲 HackBar	<b>9</b> 1 🗊 … ×
Encryption -	Encoding - SQL - XSS - LFI - XXE - Other -	Commit now! HackBar v2
Load URL	http://111.200.241.244:56417/?a=1	
🗶 Split URL		
Execute Execute	Post data Referer User Agent Cookies Add Header Clear All	

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}

← → ⊂ ŵ	Ū	2 111.200.241.244:56417/?a=1	BC •••	☆	III\ 🗊	۲	4 9	1	₩ =
● 导入书签 📄 >	火狐官方站点 🍯 新手上路	常用网址					]移动	设备上	⊑的书签

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
cvberpeace{4d7b677cdfd350b39e50fc89c4341322}

□ ○ 査看器 □ 控制台 □ 调试器 1 ↓ 网络 {} 样式编辑器 ○ 性能 ① 日	内存 🖯 存储 肯 无障碍环境 🚟 应用程序 🔵 🕂	ckBar 91 🗇 … 🗙
Execute     Post data Referer User Agent Cookies	Add Header Clear All	î
b=2		H Upgrade-Insecure-Requests: 1
		H Connection: keep-alive
		H Accept-Encoding: gzip, deflate
⑦ 过滤输出		错误警告日志信息调试 CSS XHR 潮求 🔆 🗙

# 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

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。

_	$\times$

l	ş	Burp	Suite Com	nmunity Edition v	2020.12.1 - T	emporary Proj	ect	

Dashboard	Target Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	
1 ×										
Send	Cancel <	$  \cdot   \cdot  $								Target: http://111.200.241.244:41530 🖉
Request										II 🔳 II
Pretty Raw	\n Actions ∨									
1 GET / HTT 2 Host: 111 3 User-Agen 4 Accept: t 5 Accept-La 6 Accept-En 7 Connectio 8 Upgrade-I 9 X-Forward 0 Referer: 1 Cache-Con 2 3	<pre>P/1.1 .200.241.244:415 t: Mozilla/5.0 ( ext/html,applica coding: grip, de n: close nsecure-Requests ed-For:123.123.1 https://www.goog trol: max-age=0</pre>	30 Windows NT 11 tion/xhtml+x; ;q=0.8,zh-TW flate : 1 23.123 le.com	0.0; Win64; ml,applicat ;q=0.7,zh-H	x64; rv:86.0 ion/xml;q=0.9 K;q=0.5,en-US	) Gecko/201 ,image/webp ;q=0.3,en;q	00101 Firefc ,*/*;q=0.8 =0.2	x/86.0			
2\$\$€→	Search									0 matches
Response										
Pretty Raw	Render \n Act	ions 🗸								
3 4 <body 5 <p i </p 6 <sc d <td><pre>d&gt; &gt; id="demo"&gt; p00000123.123.12 &gt; ript&gt; ocument.getEleme cript&gt; ript&gt; ocument.getEleme</pre></td><td>3.123 ntById("demo ntById("demo</td><td>").innerHTM</td><td>L="ODODhttps: L="cyberpeace</td><td>//www.googl {2ee2c35520</td><td>e.com"; 202ddf77898a</td><td>62£3764043}</td><td>";</td><td></td><td></td></sc </body 	<pre>d&gt; &gt; id="demo"&gt; p00000123.123.12 &gt; ript&gt; ocument.getEleme cript&gt; ript&gt; ocument.getEleme</pre>	3.123 ntById("demo ntById("demo	").innerHTM	L="ODODhttps: L="cyberpeace	//www.googl {2ee2c35520	e.com"; 202ddf77898a	62£3764043}	";		
d <td>cript&gt; Y&gt;</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	cript> Y>									
d 7	cript> y>									

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:



<?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;

							AntSword 编辑 窗口 调词
							✿ 设置
>	►分类目录 (2)						☰ 数据管理 (0)
重命名 💼 删除	●添加 /	- 🗆 ×		ł	📘 添加数据	IP地	URL地址
0	🗅 默认分类		: 测试连接	清空	Ο 添加		
0	□ 20210310	*			■基础配置		
			//111 200 241 244·31792/index nhp	* htt	URI t#tit		
		=	 /111.200.211.211.31732/index.php	*	达 体 应 和		
		- 1		sne	圧接強い		
					网站奋注		
		*		UT	编码设置		
		~		PH	连接类型		
				编码			
			efault (不推荐)	۲			
			ndom (不推荐)	$\bigcirc$			
		-	ase64	$\bigcirc$			
		~			<b>2</b> 请求信息		
		• •	ise64	0	<b>2</b> 请求信息		

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}。

1 1 中国戦剑									_		×
AntSword 编辑 窗口 调试											
111.200.241.244 (8)											
□ 目录列表 (0)	□文	件列表 (	(2)								^
	0 第	新建 👻	◆ 上层 🛛 📿 刷新	★ 主目录	■书签 ▼	/var/www,	/html/			→ 读I	权
e var		名称	R			E	日期	大小		属性	
	Ē	flag.t	xt			20	021-03-10 10:27:02		44 b	0664	4
		index	.php			20	18-09-27 04:02:04		539 b	0664	4
	■任	务列表								at/m0_558	54679

#### 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 对各类网站站点进行有效防护。

|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。



# PING

请输入需要ping的地址

PING

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

Enter password	
确定取消	
	https://blog.csdn.net/m0_55854679

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。



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

print(s)

4.将得到的数组用chr()函数处理,可得到字符串786OsErtk12,规范flag格式,即可得到我们所要找的flag cyberpeace{786OsErtk12}。



