XCTF攻防世界练习区-web题(新手)

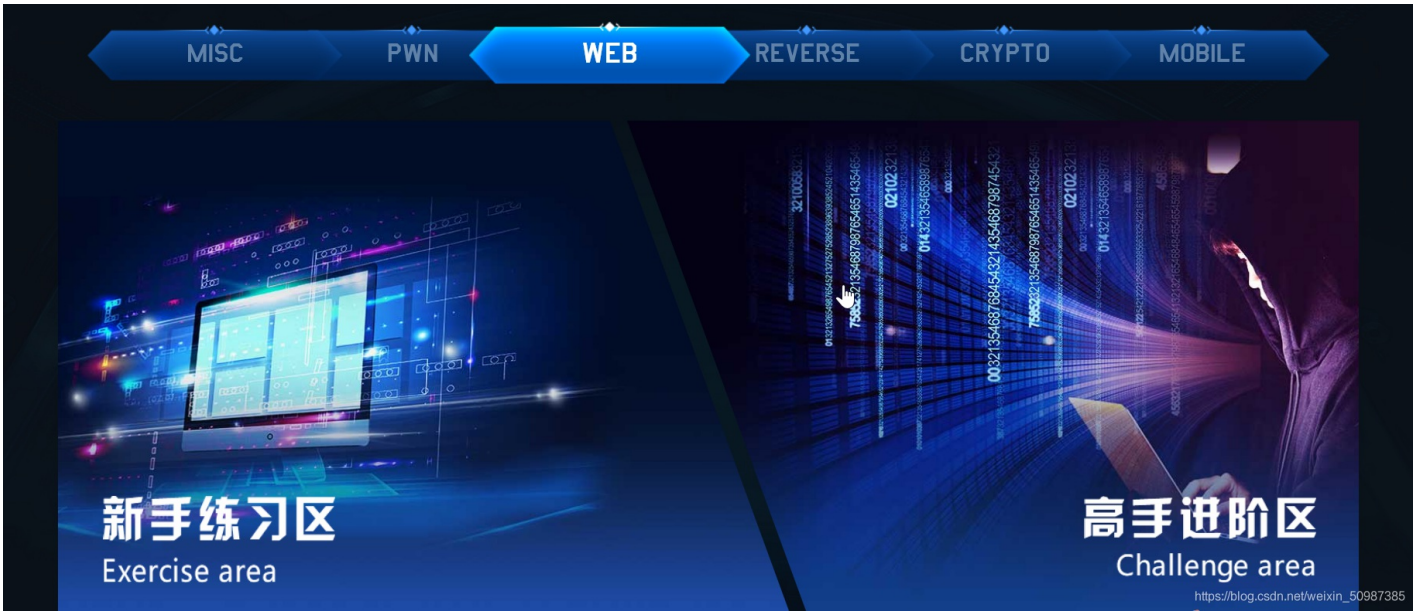
原创

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

本文链接：https://blog.csdn.net/weixin_50987385/article/details/114499572

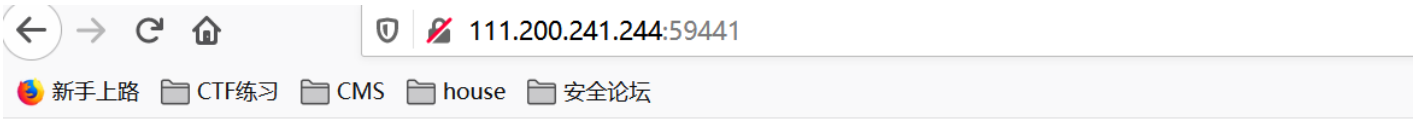
XCTF攻防世界练习区-web题(新手)

https://adworld.xctf.org.cn/task?now_checked_num=3&name=web



001 view_source

打开http://111.200.241.244:59441



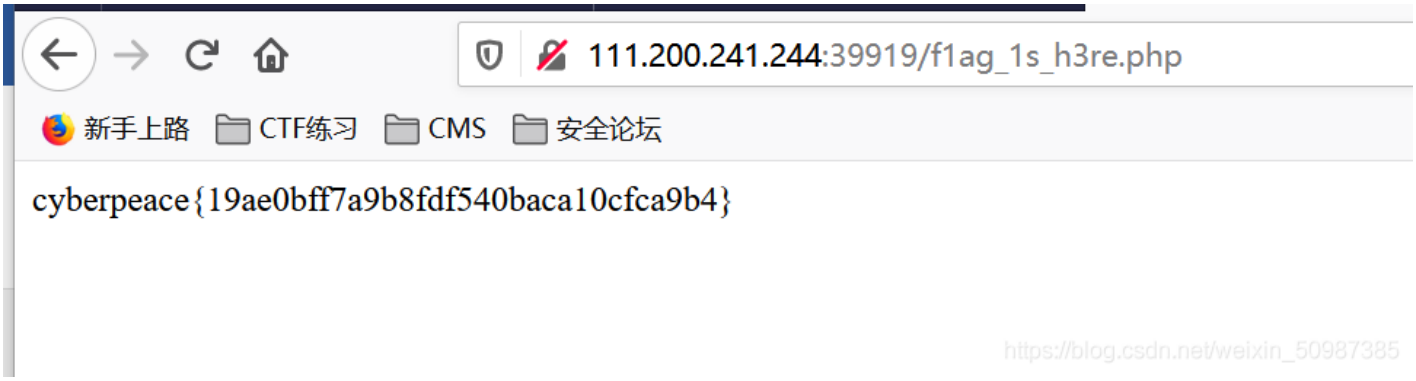
FLAG is not here

F12查看源码，发现flag在源码注释中

002 robots

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

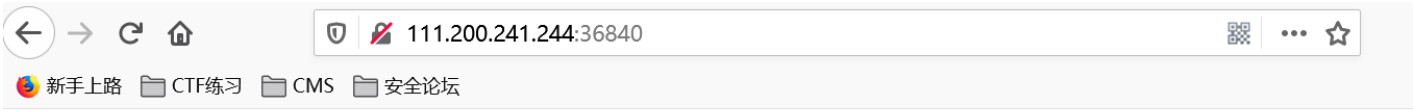
发现存在flag_1s_h3re.php，打开http://111.200.241.244:39919/f1ag_1s_h3re.php



发现flag=cyberpeace{19ae0bff7a9b8fdf540baca10cfca9b4}

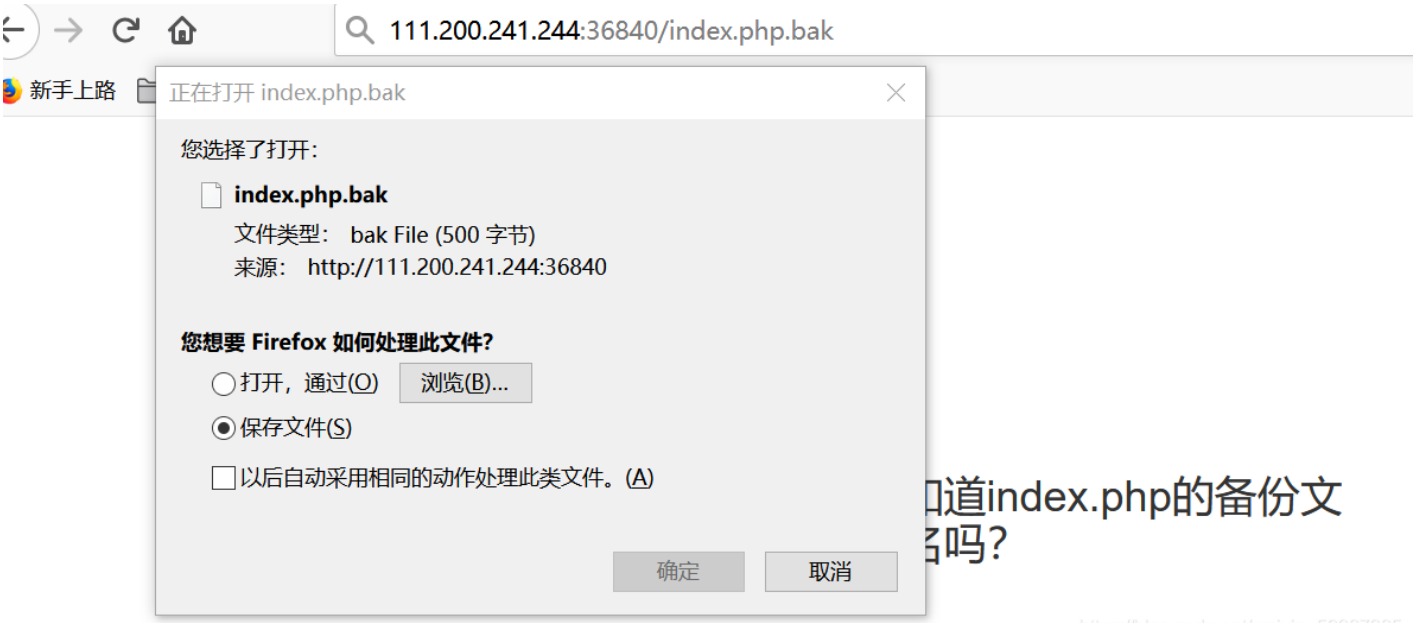
003 backup

打开http://111.200.241.244:36840



你知道index.php的备份文件名吗?

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



道index.php的备份文件名吗?

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>
```

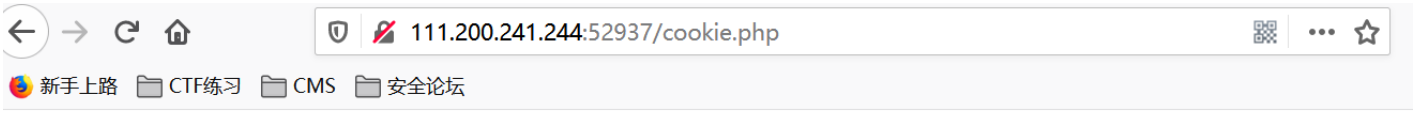

找到flag=Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}

004 cookie

打开http://111.200.241.244:52937

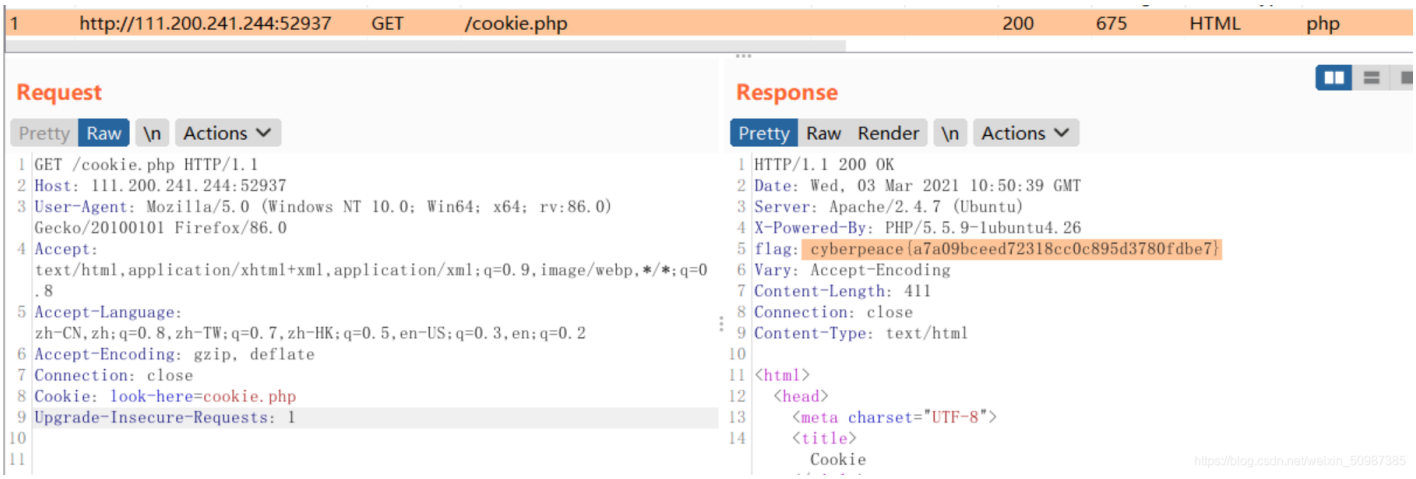
F12查看cookie信息，发现有cookie.php

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



See the http response

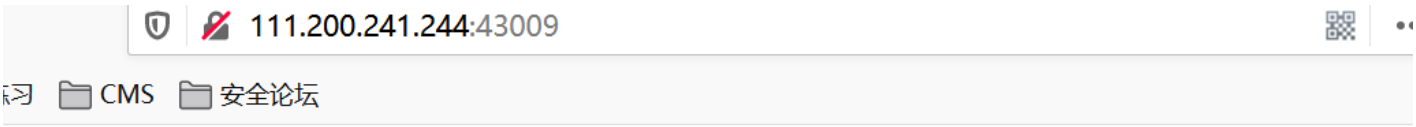
打开Burpsuite进行抓包



在Response响应消息中找到flag=cyberpeace{a7a09bceed72318cc0c895d3780fdbe7}

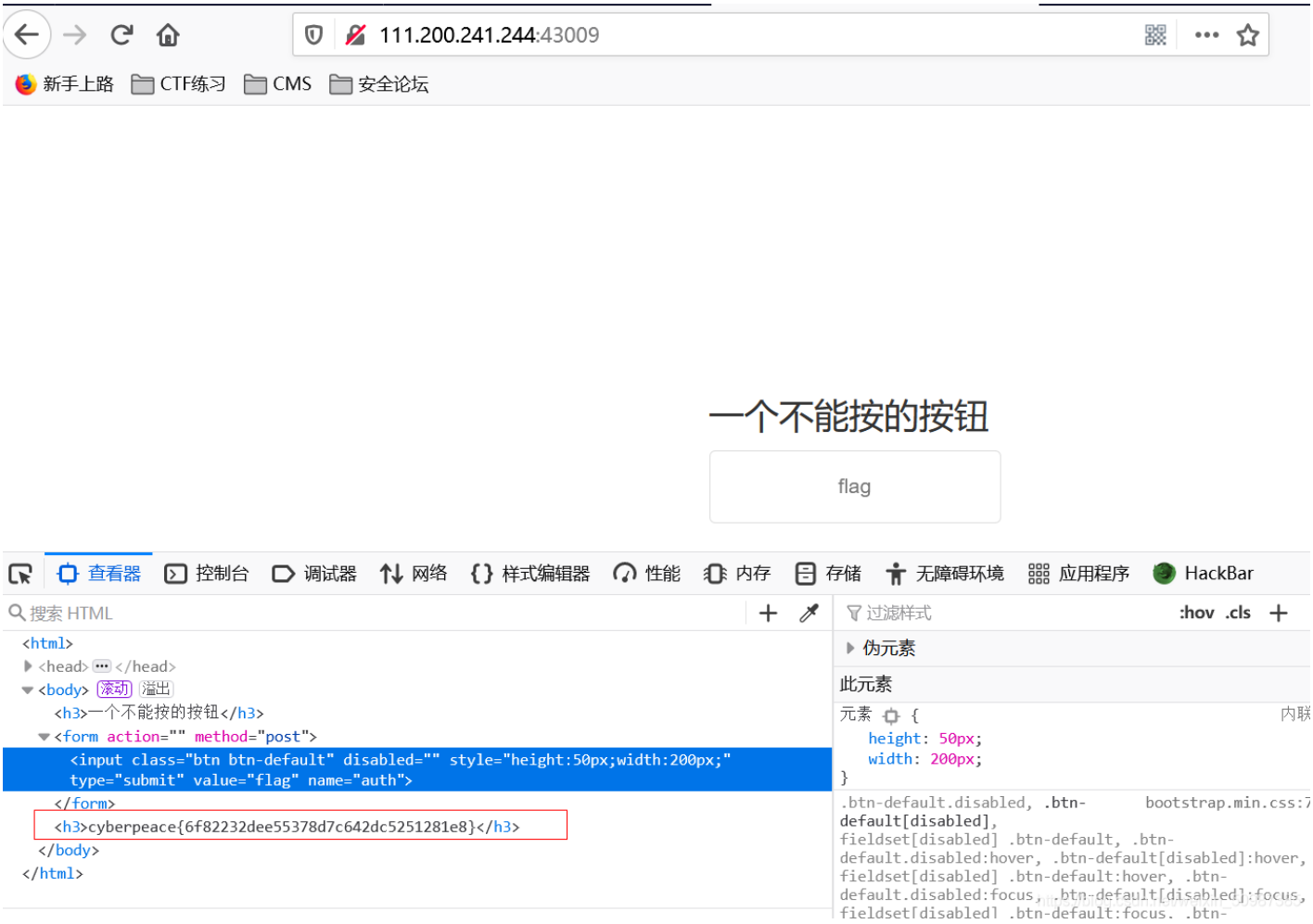
005 disabled_button

浏览器地址栏输入http://111.200.241.244:43009



F12打开查看器

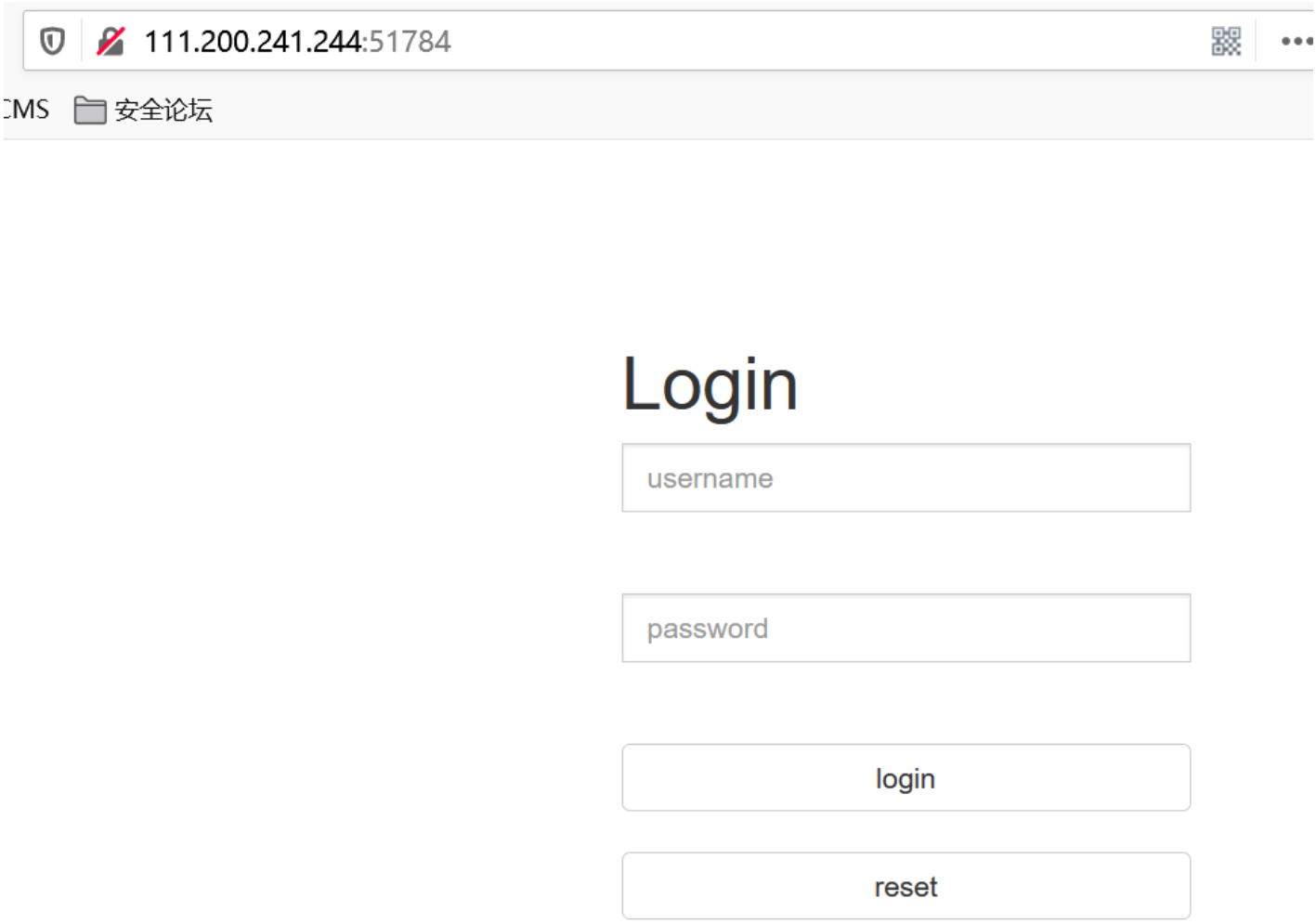
将disabled=""直接删除后刷新浏览器，出现flag



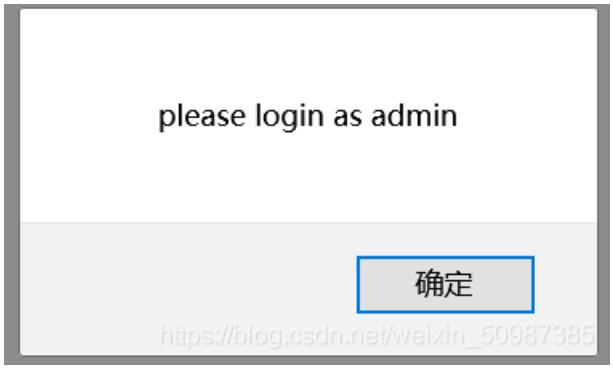
Flag=cyberpeace{6f82232dee55378d7c642dc5251281e8}

006 weak_auth

输入http://111.200.241.244:51784，出现登录页面



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}

Flag=cyberpeace{160e7678f803e05ca1aa65dfb93409cf}

007 simple_php

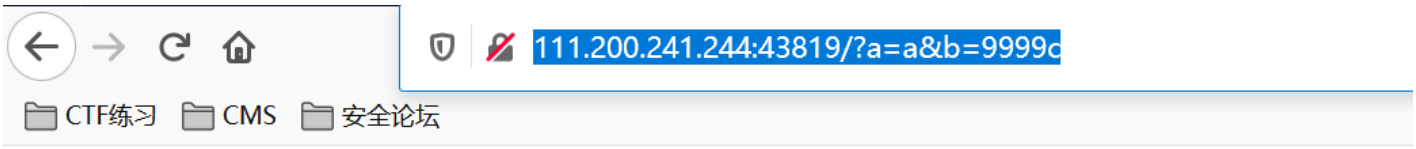
输入http://111.200.241.244:43819，查看到源码

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
<?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}

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
<?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

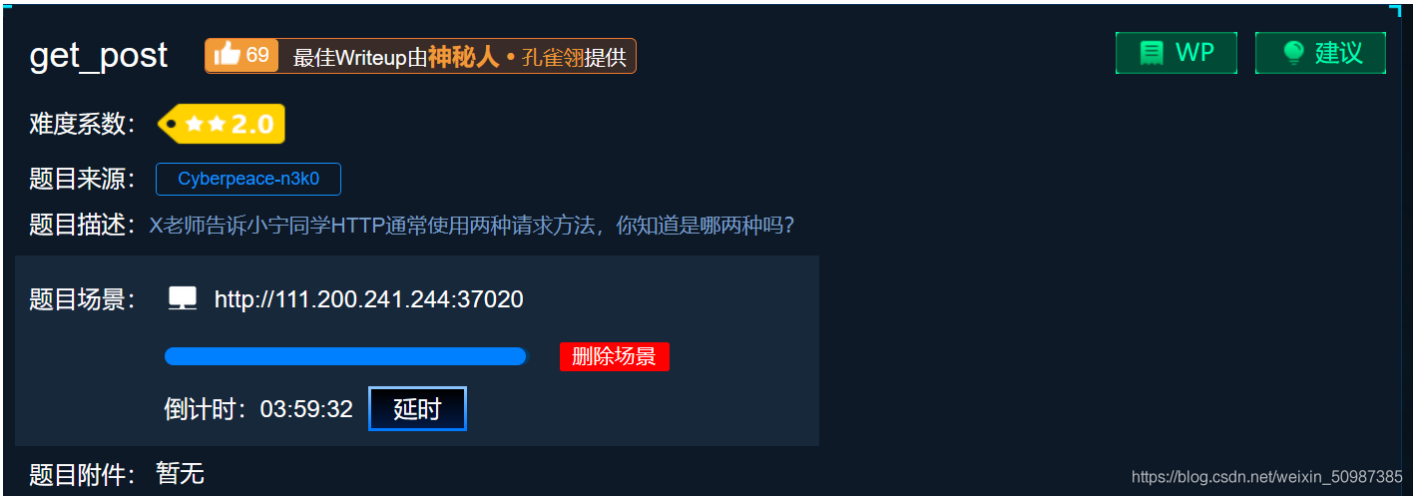
'a' 这是一个字符串类型。0 是数字类型。使用 == 宽松比较，此时发生类型转换。字符串和数字比较，是将字符串转换为数字然后进行比较的。

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。

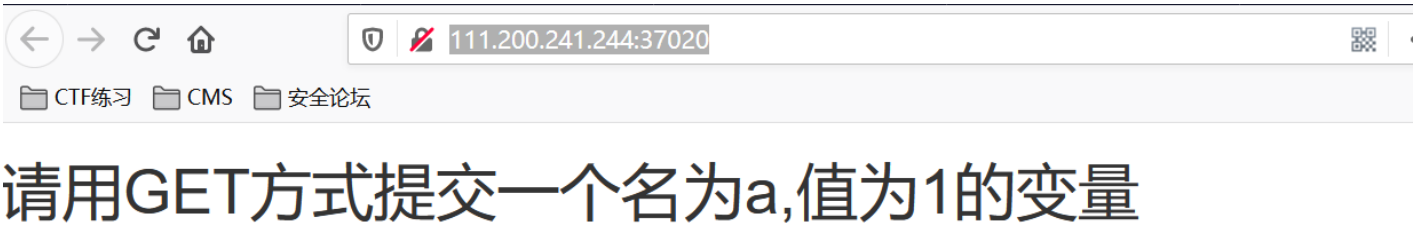
运算步骤二：最后比较0是否等于0，结果为真。

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

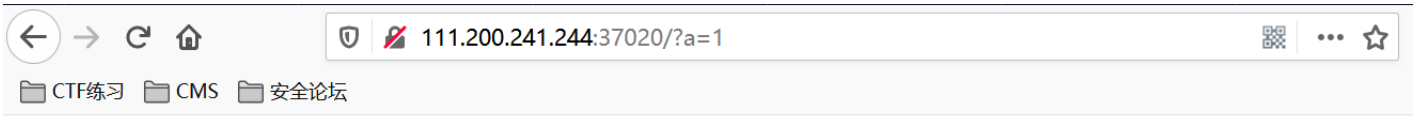
008 get_post



打开url=http://111.200.241.244:37020/



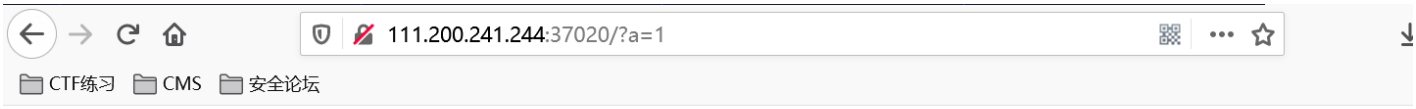
将a=1输入得到



请用GET方式提交一个名为a,值为1的变量

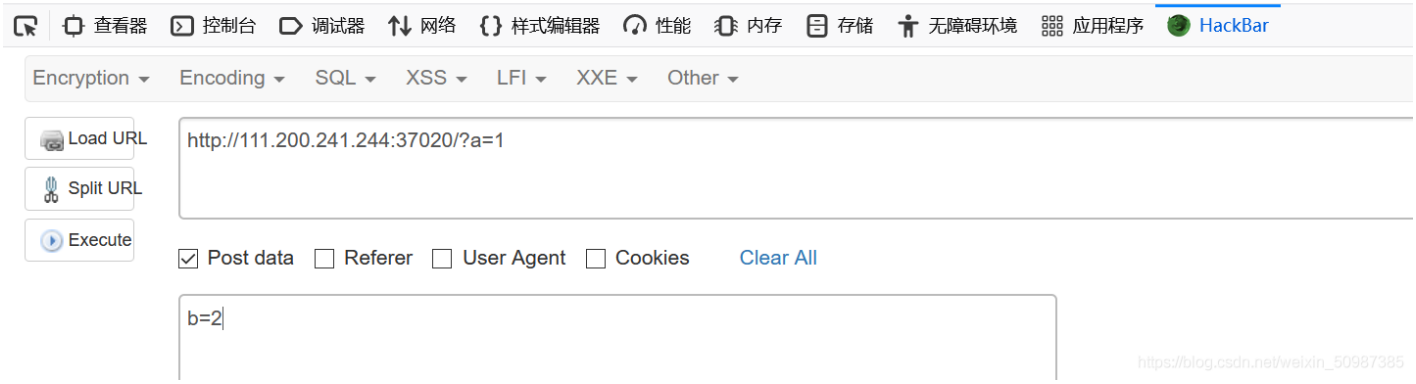
请再以POST方式随便提交一个名为b,值为2的变量

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



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。

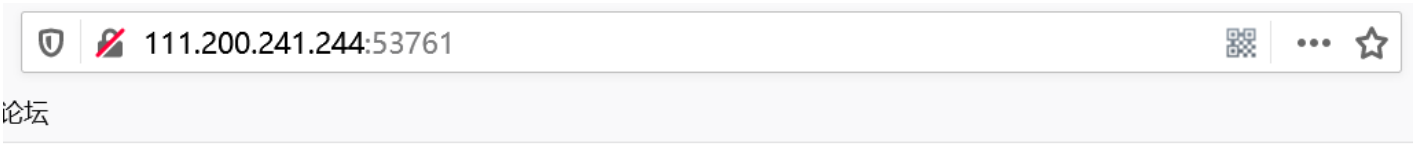
【解题思路】

火狐浏览器插件hackbar

burpsuite伪造

场景题开启后如下所示

打开url链接

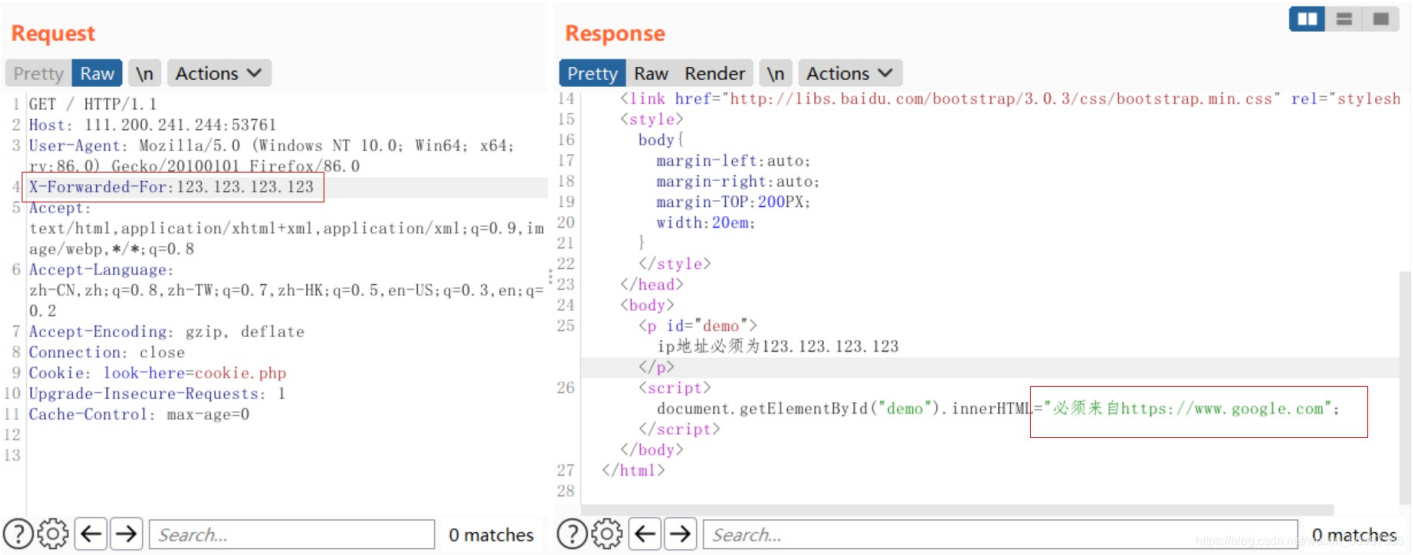


论坛

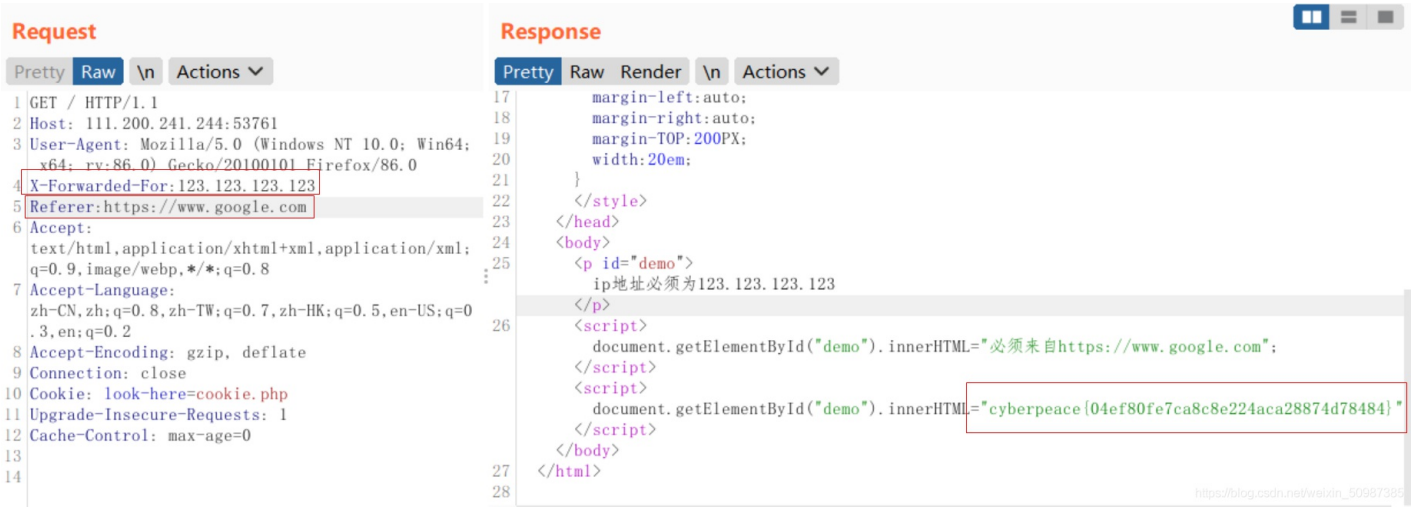
ip地址必须为123.123.123.123

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。



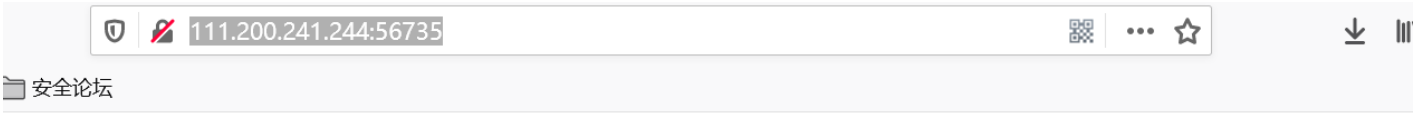
再添加Referer:https://www.google.com



返回flag= cyberpeace{04ef80fe7ca8c8e224aca28874d78484}

010 webshell

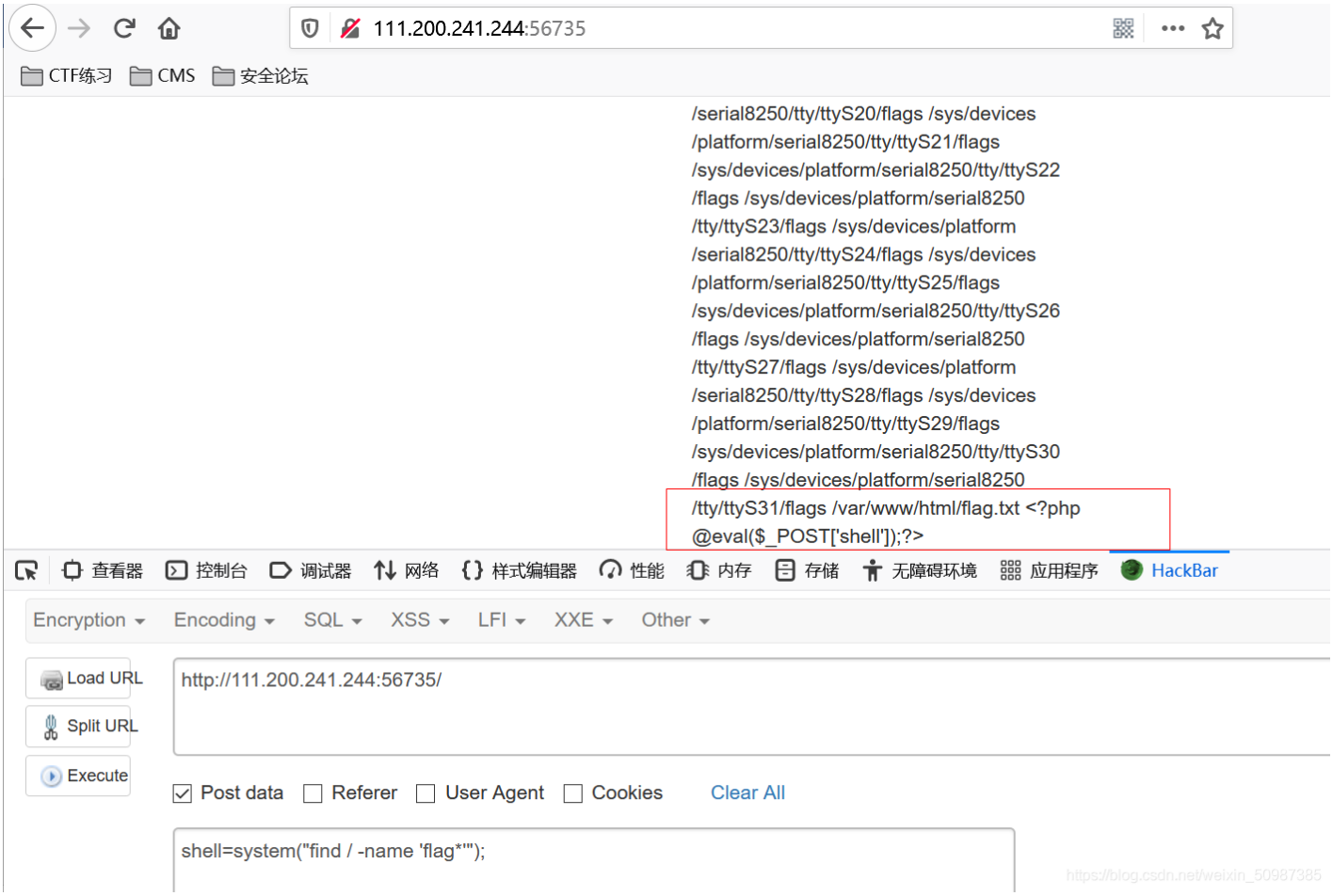
打开http://111.200.241.244:56735/



你会使用webshell吗?

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

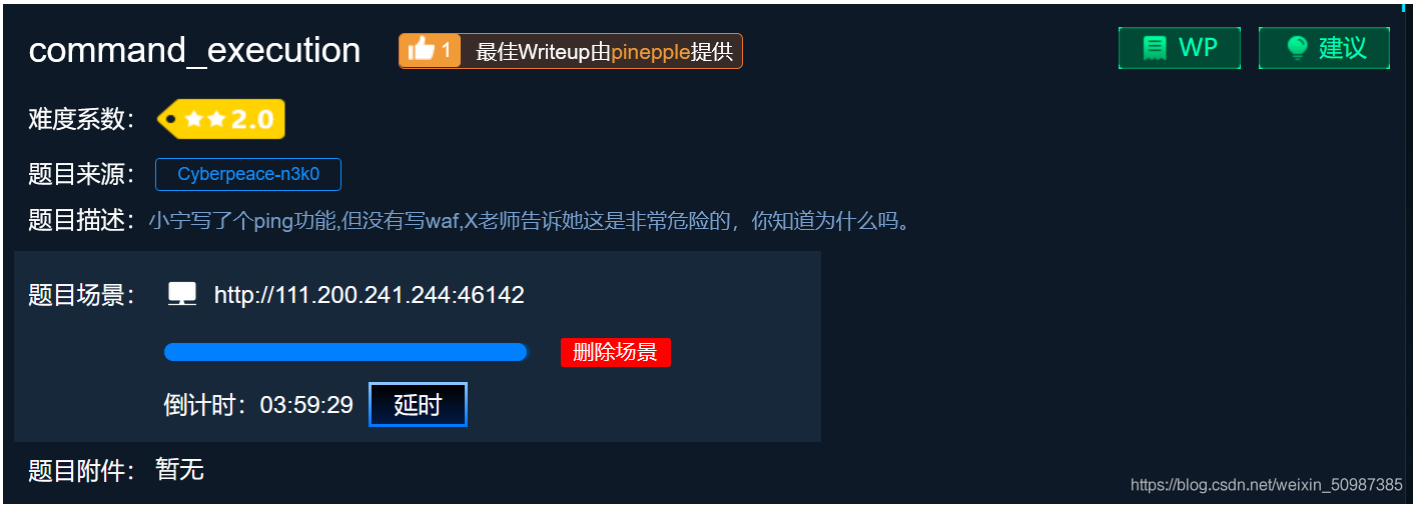
利用hackbar传递shell,令shell=system("find / -name 'flag*'");查找所有与flag相关文件



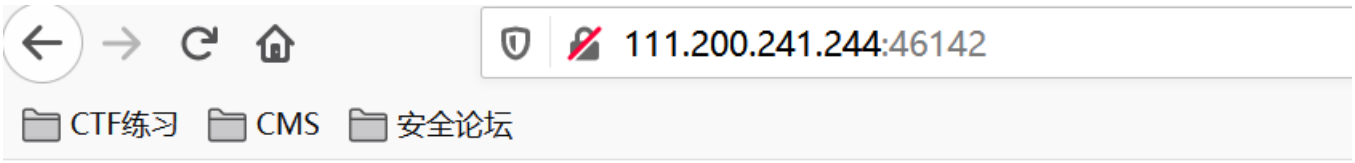
发现flag在flag.txt文件中

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

011 command_execution



输入url http://111.200.241.244:46142/

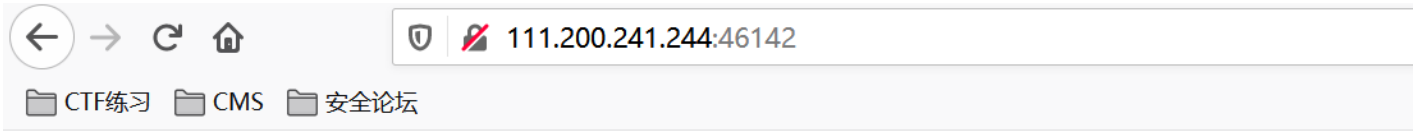


PING

请输入需要ping的地址

PING

先ping一下本机地址,ping 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=0.065 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
```


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

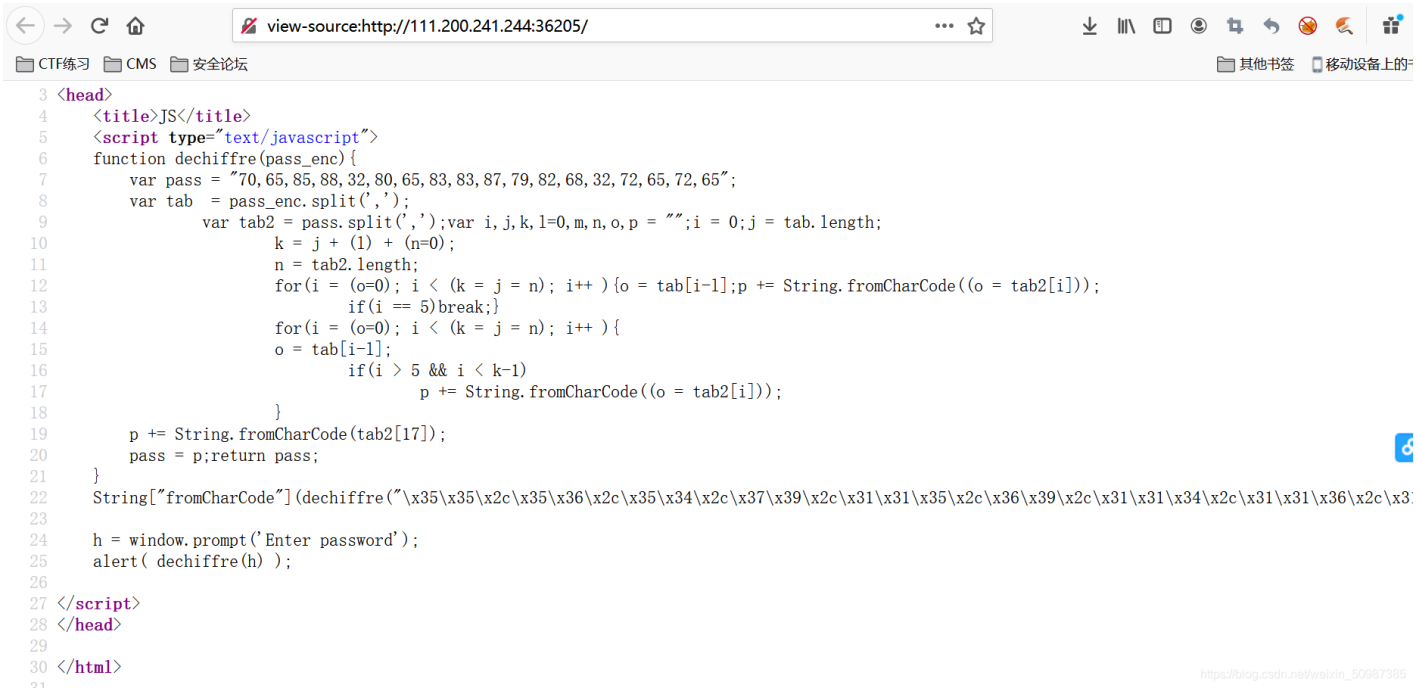
查看flag.txt文件内容，ping 127.0.0.1 | cat /home/flag.txt

获得flag = cyberpeace{bee31b2c250b75c0bdd12a3a1a40d960}

012 simple_js

进入题目场景

打开题目，弹出一个弹窗，提示输入密码，随便输入一个，之后查看源码，得到JS源代码，是一个解码函数。



分析源码，发现随便输入都会输出

pass="70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65"。

用python处理：

运行如下python代码：

```
a = [70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65]
for i in a:
    print(chr(i),end='')
```

输出结果：FAUX PASSWORD HAHA

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

\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

字符串转16进制 >>

16进制转字符串 >>

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

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}。