攻防世界新手区

原创

H0ne 于 2021-02-07 16:15:05 发布 2034 收藏 1

文章标签： web

本文链接：https://blog.csdn.net/qq_53142368/article/details/113740252

学习目标：

做自己喜欢的事

学习内容：

攻防世界新手区练习

学习时间：

2021年2月6日

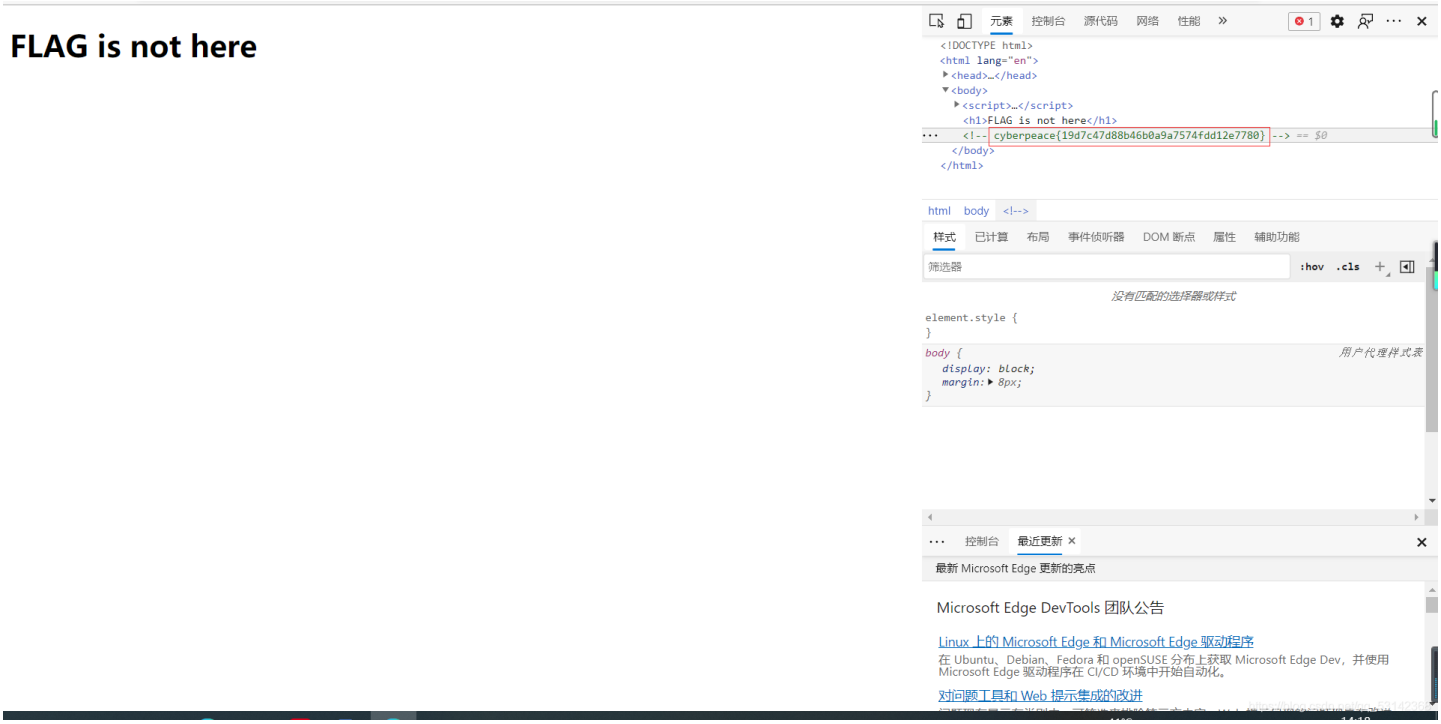
学习产出：

1.

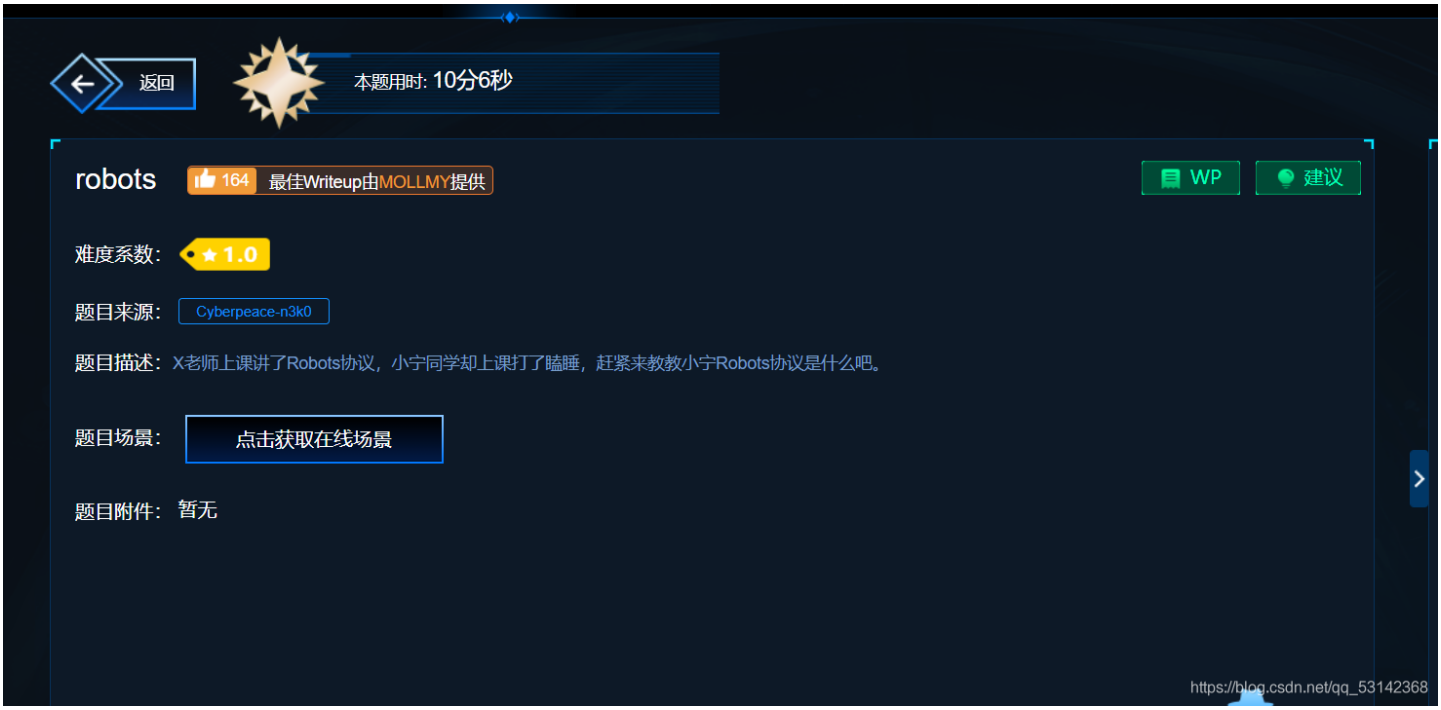
打开后会出现

FLAG is not here

查看其HTML



2.



首先需要了解啥是robot协议

Robots协议的详解

Robots协议是Web站点和搜索引擎爬虫交互的一种方式，Robots.txt是存放在站点根目录下的一个纯文本文件。该文件可以指定搜索引擎爬虫只抓取指定的内容，或者是禁止搜索引擎爬虫抓取网站的部分或全部内容。当一个搜索引擎爬虫访问一个站点时，它会首先检查该站点根目录下是否存在robots.txt，如果存在，搜索引擎爬虫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，那么搜索引擎爬虫就沿着链接抓取。

另外，robots.txt必须放置在一个站点的根目录下，而且文件名必须全部小写。如果搜索引擎爬虫要访问的网站地址是http：//www.w3.org/，那么robots.txt文件必须能够通过http：//www.w3.org/robots.txt打开并看到里面的内容。

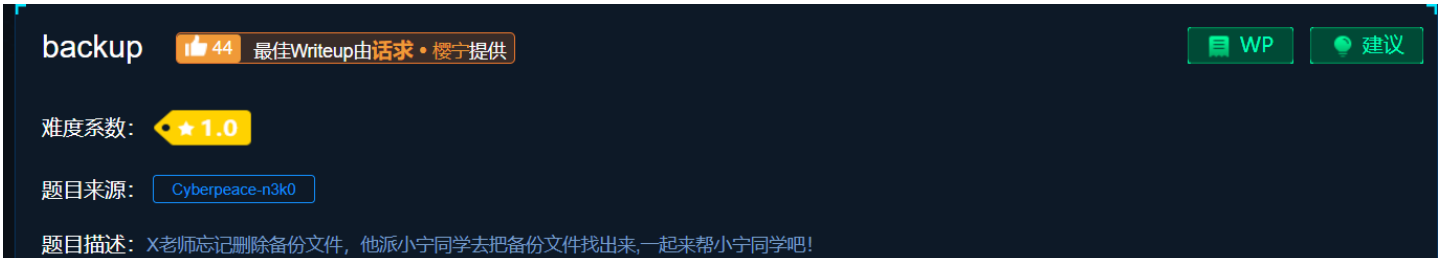
在其后缀加入robots.txt后得到


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


然后在URL后面加入f1ag_1s_h3re.php

cyberpeace{931158a597f5509c33f90e9e81325d13}

3.

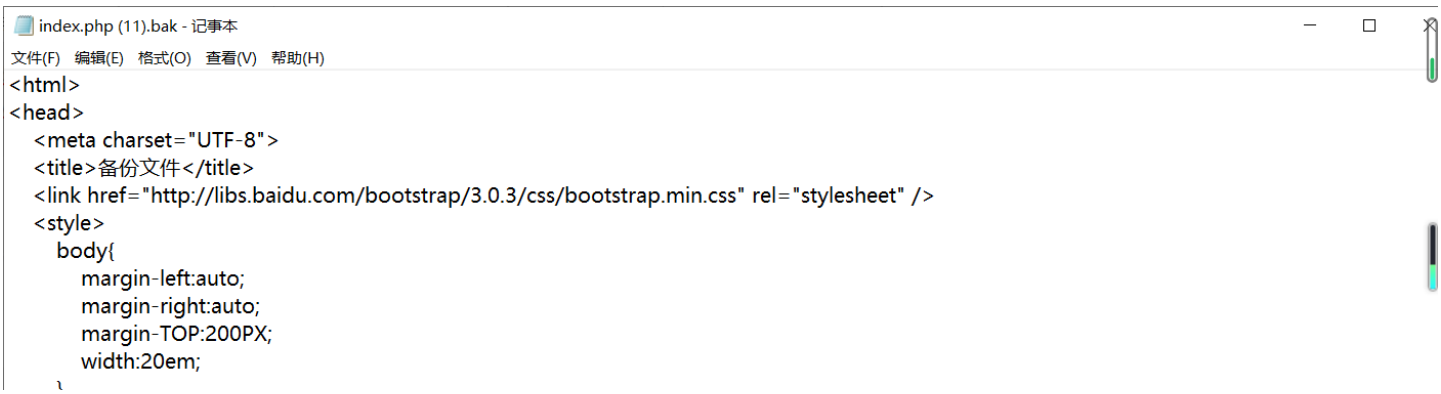


打开后

首先需要了解啥是index.php备份文件名

所以在URL后面加上index.php.bak

发现bak文件直接打不开，所以需要在 bak文件所在的文件夹中用记事本的形式打开，查看他的HTML



```
    </style>
</head>
<body>
<h3>你知道index.php的备份文件名吗？ </h3>
<?php
$flag="Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}"
?>
</body>
</html>
```

第 8 行，第 30 列　100%　Windows (CRLF)　UTF-8

找到cyberspace

4.

首先需要了解啥是cookie协议

你知道什么是cookie吗?

cookie（储存在用户本地终端上的数据）

编辑 讨论 7 上传视频

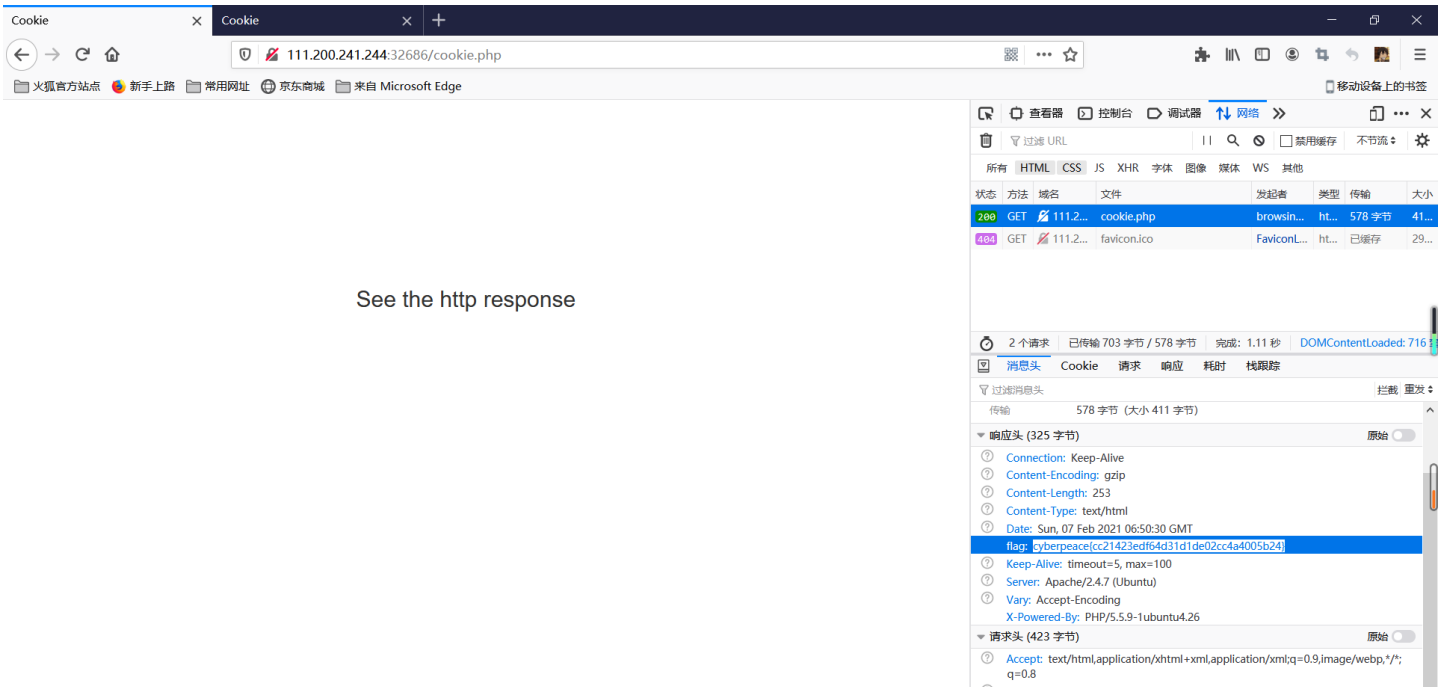
本词条由"科普中国"科学百科词条编写与应用工作项目 审核 。

Cookie，有时也用其复数形式 Cookies。类型为"**小型文本文件**"，是某些网站为了辨别用户身份，进行Session跟踪而储存在用户本地终端上的数据（通常经过加密），由用户客户端计算机暂时或永久保存的信息 [1] 。

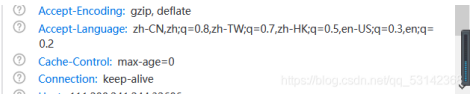
所以在URL上加上cookie.php得到结果是

See the http response

看到这种情况看到提示说查看response，响应头就一定藏着flag



See the http response

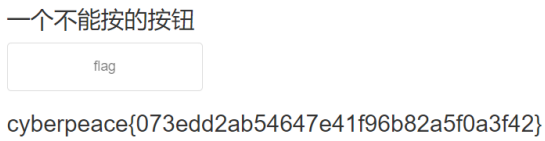

Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Cache-Control: max-age=0
Connection: keep-alive

5.


disabled_button
62 最佳Writeup由沐一清提供
WP
建议
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，然后给了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?
题目场景：
http://111.200.241.244:47644
删除场景
倒计时：03:59:25
延时
题目附件：
暂无
题目已答对
分享wp点赞赚金币哦
马上去写
https://blog.csdn.net/qq_53142368

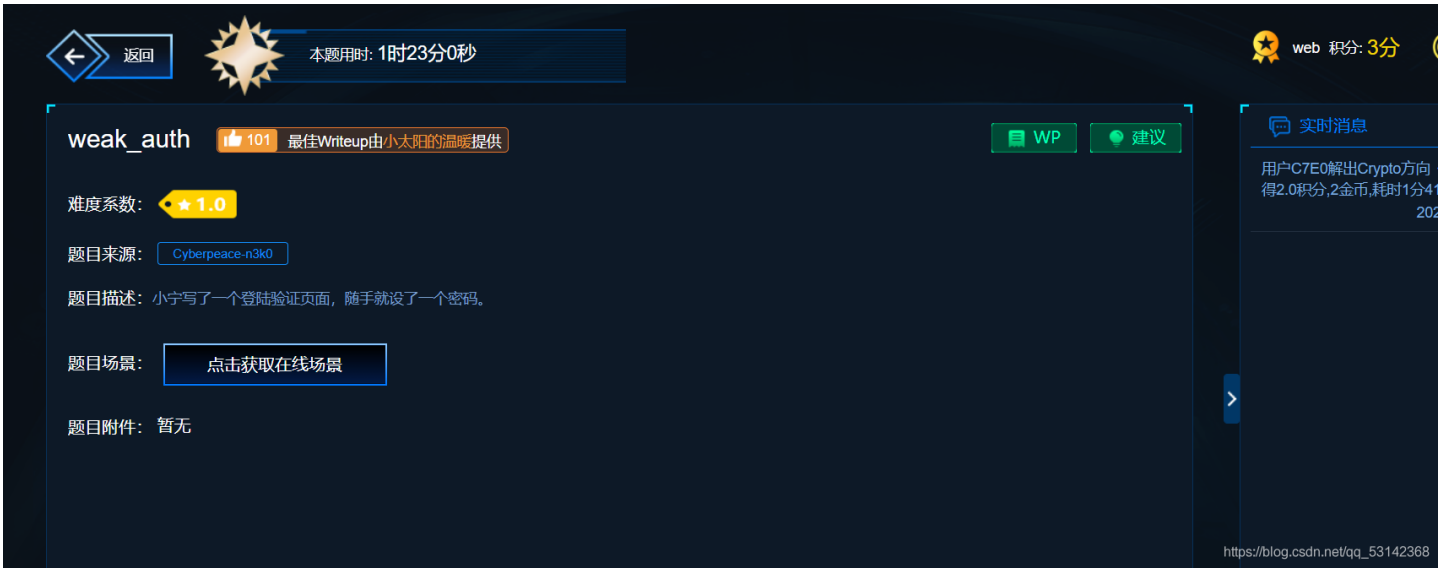
发现点不了这个flag

发现有一个disabled，disabled属性可设置或返回是否禁用单选按钮。所以删掉disabled属性

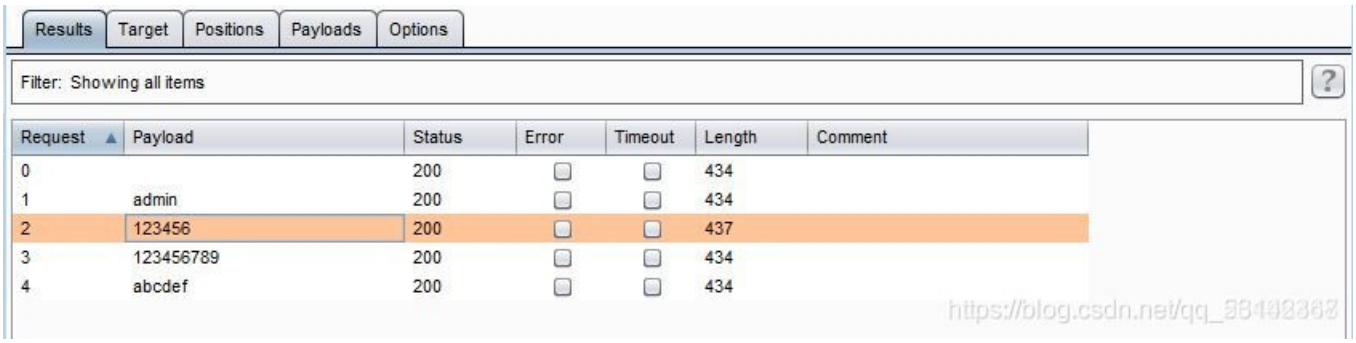


cyberpeace{073edd2ab54647e41f96b82a5f0a3f42}

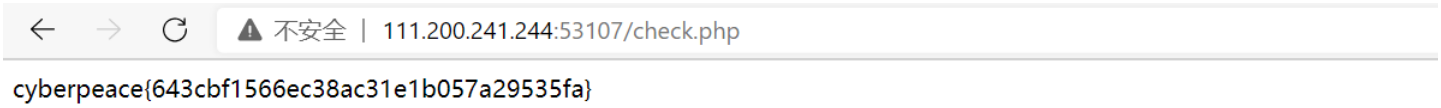
6.



随便登陆，提示说要admin登陆
查看HTML没看到重要信息，所以就需要暴力破解了
用到burp suite（需要Python环境),所以提前先下载Python环境



看到这个123456返回长度不一样，所以密码就是123456，账号就是admin



cyberpeace{643cbf1566ec38ac31e1b057a29535fa}

7.


```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;
}
?>
```

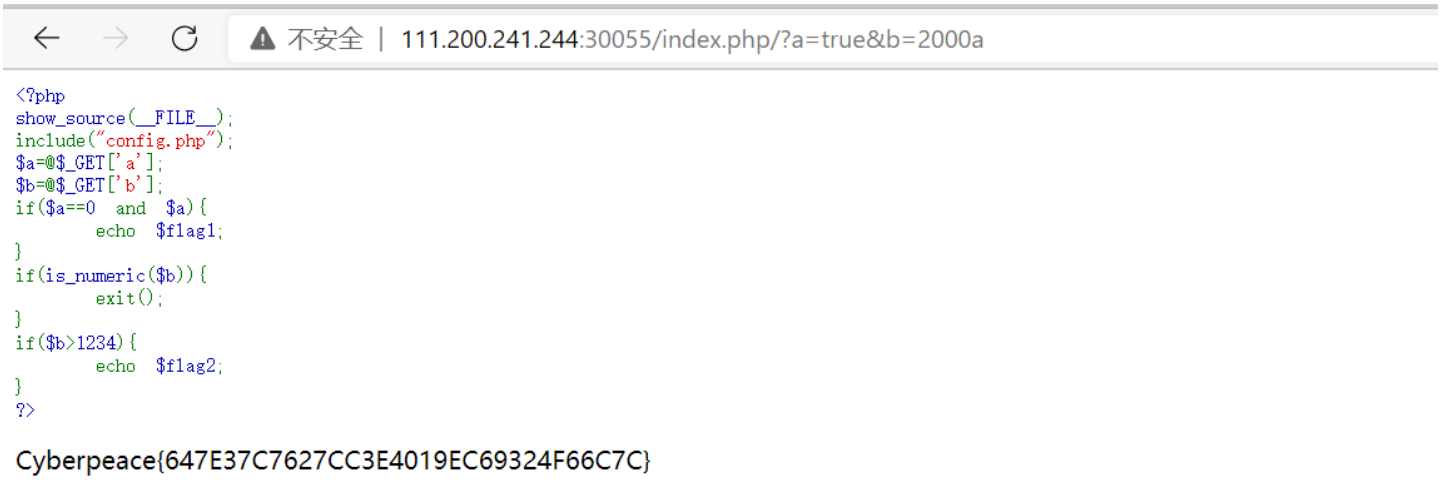
php中其中两种比较符号:

==：先将字符串类型转化成相同，再比较

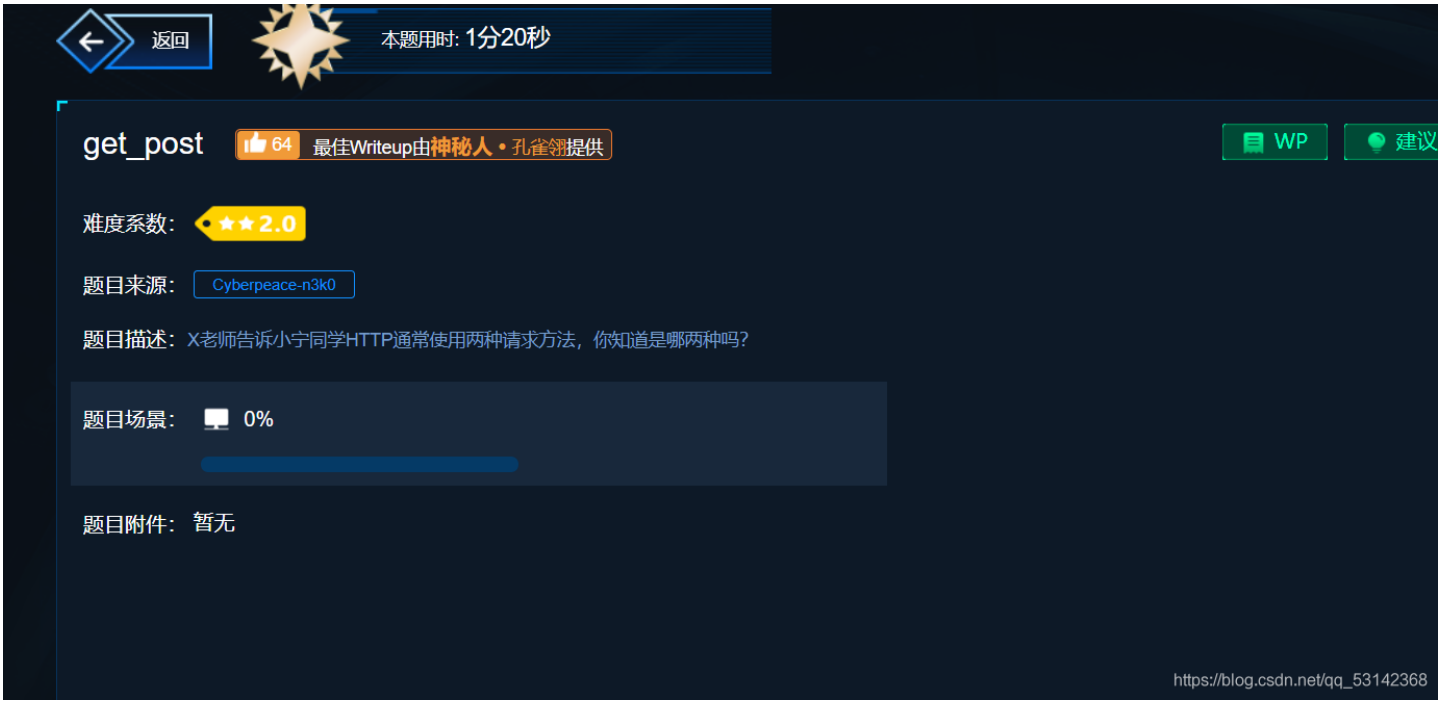
===：先判断两种字符串的类型是否相等，再比较

注：<、>、<=、>=都存在和==相同的弱类型，原理相同！！！

分析代码，需要满足$ a==0 and $b>1234,b还不能是数字
我们使a=true 当比较时true转换为0 输出前半段
b=2000a 比较时转换为2000>1234.输出后半段



8.



请用GET方式提交一个名为a,值为1的变量

这一看就是考get post呗

get方式提交即url上输入

post提交使用火狐浏览器(需要用到hackbar插件）

12.

打开页面后让你输入密码，（放心，你是不可能输入对的）
查看页面的源代码

```
<html>
<head>
    <title>JS</title>
    <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 + (l) + (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\x2c\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>
</head>

</html>
```

发现了重要的东西
有2c 明显是十六进制
将这些十六进制数转换成十进制后，
55,56,54,79,115,69,114,116,107,49,50
sacll处理后得到
Cyberpeace{786OsErtk12}

-
-
-

9，10，11题小白还没弄懂，等小白弄懂后，再在上面补充。*