

攻防世界web新手区（持续更新）

原创

梳刘海的杰瑞 于 2020-04-24 21:19:51 发布 162 收藏

文章标签：[web](#)

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_45664911/article/details/105439354

版权



[web](#) 专栏收录该内容

12 篇文章 0 订阅

订阅专栏

[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。

如题目所示：鼠标右键不能用，如果查看代码的话可以使用键盘

```
ctrl+shift+i  
ctrl+u
```

(我按F12没有用)

```
<h1>FLAG is not here</h1>  
  
<!-- cyberpeace {3ca31ab8d997400b3c4f74ed8794b081} -->  
  
</body>  
</html>
```

robots

Robots协议，学名叫：The Robots Exclusion Protocol，就搜索引擎抓取网站内容的范围作了约定，包括网站是否希望被搜索引擎抓取，哪些内容不允许被抓取，把这些内容放到一个纯文本文件robots.txt里，然后放到站点的根目录下。爬虫抓取网站内容前会先抓取robots.txt，据此“自觉地”抓取或者不抓取该网页内容，其目的是保护网站数据和敏感信息、确保用户个人信息和隐私不被侵犯。

robots.txt文本文件必须存放在站点的根目录

猜想, flag应该在robots.txt中, 对robots.txt进行访问, 在网址后面加上/robots.txt

```
← → ↻ ⓘ 不安全 | 159.138.137.79:59357/robots.txt

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

再对flag...进行访问

```
← → ↻ ⓘ 不安全 | 159.138.137.79:59357/f1ag_1s_h3re.php

cyberpeace{f0c39e52fbee37fb2600ea8880c0a207}
```

User-agent: 表示允许所有搜索引擎蜘蛛来爬行抓取, 也可以把去掉, 改为特定某一个或者某些搜索引擎蜘蛛来爬行抓取, 如百度是Baiduspider, 谷歌是Googlebot。

back up

php的备份有两种: `.php~`和`.php.bak`
如果网站存在备份文件, 在地址栏最末加上`/index.php~`或`/index.php.bak`, 即可得到备份文件

添加了.php.bak.后自动下载了个文件, 用记事本打开发现flag

```
<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>
```

https://blog.csdn.net/weixin_45664911

cookie

为什么会有cookie

Web应用程序是使用HTTP协议传输数据的。HTTP协议是无状态的协议。一旦数据交换完毕，客户端与服务器端的连接就会关闭，再次交换数据需要建立新的连接。这就意味着服务器无法从连接上跟踪会话。你可能会这样的经历，登陆一个网站的时候会提醒你要不要记住账户和密码，这样下次来你就不用再次输入账号密码了。这就是cookie的作用，当我们再次访问的时候，方便服务器直接根据我们的cookie来直接取上一次取过的东西(对于每一个cookie服务器会对这个cookie存储上一次我们拿过的数据，下一次对于同一个cookie的时候，就直接在这里取)

什么是Cookie

Cookie是由服务器端生成，发送给User-Agent（一般是浏览器），（服务器告诉浏览器设置一下cookie），浏览器自动会将Cookie以key/value保存到某个目录下的文本文件内，下次请求同一网站时也会自动发送该Cookie给服务器，即添加在请求头部（前提是浏览器设置为启用cookie）。

Cookie就是一个小型文件（浏览器对cookie的内存大小是有限制的-----用来记录一些信息）

cookie的一些基本信息可以查看这篇博客（<https://segmentfault.com/a/1190000016248401>）

根据博客看，我利用浏览器对他进行了查看

你知道什么是cookie吗?

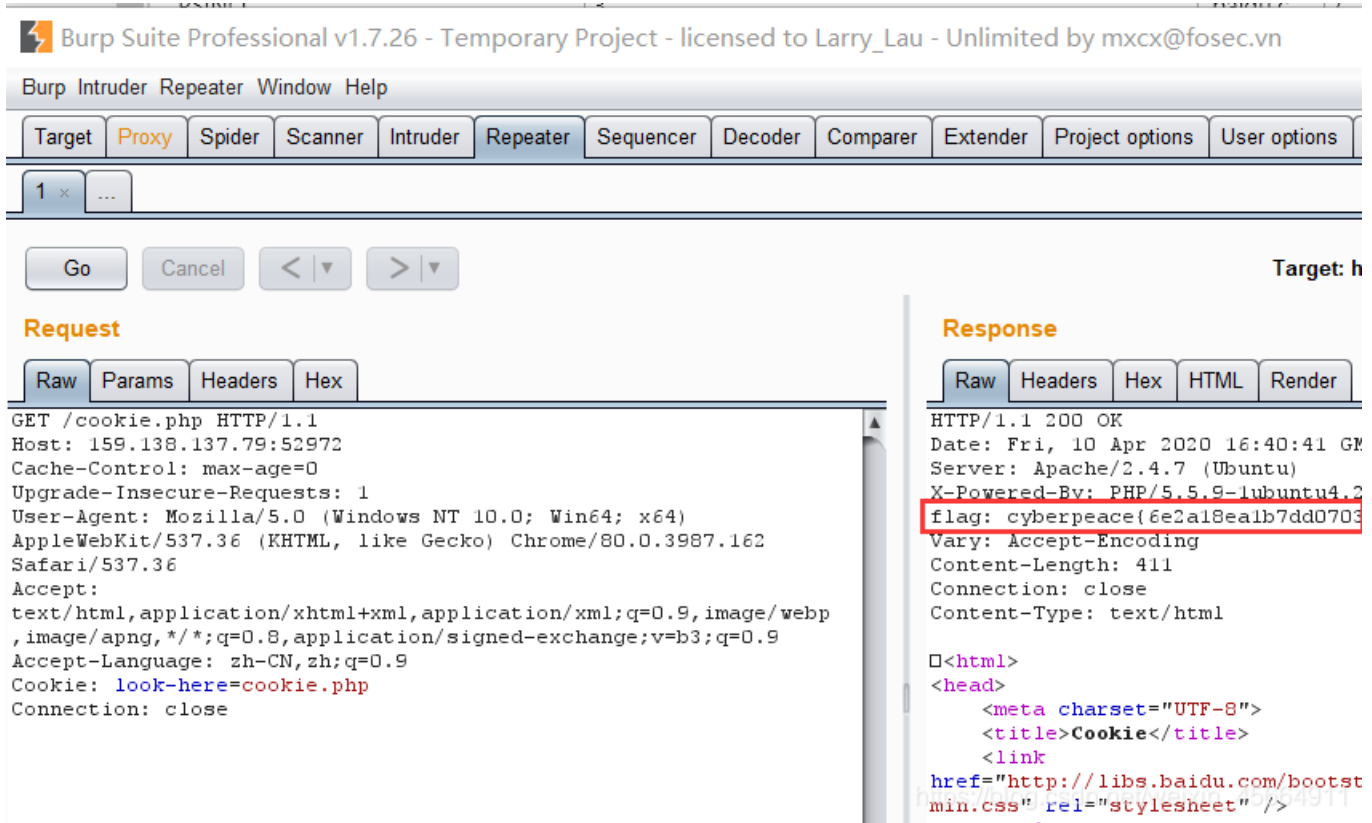
| Name | Value |
|----------------------|-------------------------------------|
| MCITY | -315%3A317%3A |
| delPer | 0 |
| H_PS_PSSID | 1447_31120_21087_31186_30904_31218_ |
| PSTM | 1565088070 |
| PSINO | 3 |
| BIDUPSID | A33DCAC79DE5DDFB9F833D3C18163B5I |
| BAIDUID | A33DCAC79DE5DDFB9F833D3C18163B5I |
| BDORZ | B490B5EBF6F3CD402E515D22BCDA1598 |
| BDRCVFR[feWj1Vr5u3D] | I67x6TjHwwYf0 |
| ZD_ENTRY | baidu |
| look-here | cookie.php |
| __cfduid | d351a924e50c66077fed33fdbd0b544471 |
| BDUSS | nZxM1o0eE9RLUpBakpaUXR6UkMxOUU: |

https://blog.csdn.net/weixin_45664911

发现一个cookie.php的文件，对它进行访问

See the http response

做到cookie的题目，再加上看到response就能联想到抓包



Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x ...

Go Cancel < >

Request

Raw Params Headers Hex

```
GET /cookie.php HTTP/1.1
Host: 159.138.137.79:52972
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.162
Safari/537.36
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
Accept-Language: zh-CN,zh;q=0.9
Cookie: look-here=cookie.php
Connection: close
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 10 Apr 2020 16:40:41 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.2
flag: cyberpeace{6e2a18ealb7dd0703}
Vary: Accept-Encoding
Content-Length: 411
Connection: close
Content-Type: text/html

<html>
<head>
<meta charset="UTF-8">
<title>Cookie</title>
<link
href="http://libs.baidu.com/bootst
min.css" rel="stylesheet"/>
```

成功得到flag

其实刚开始用bp对网页进行抓包的时候就能看到里面有cookie.php



Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options

Intercept HTTP history WebSockets history Options

Request to http://159.138.137.79:52972

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
GET /cookie.php HTTP/1.1
Host: 159.138.137.79:52972
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applic
Accept-Language: zh-CN,zh;q=0.9
Cookie: look-here=cookie.php
Connection: close
```

disabled button

打开开发者工具，进入查看器

方法一：将disable删除

方法二：将disable改成“disable=false”



```
<html>
  <head>
    <meta charset="UTF-8">
    <title>一个不能按的按钮</title>
    <link href="http://libs.baidu.com/bootstrap/3.0.3/css/b...>
    <style>...</style>
  </head>
  <body>
    <h3>一个不能按的按钮</h3>
    <form action method="post"> == $0
      <input disabled class="btn btn-default" style="height:
    </form>
  </body>
</html>
```

https://blog.csdn.net/weixin_45664911

一个不能按的按钮

cyberpeace{1e3214042ec2f78}

更改后flag就可以单击了

```
js中设置按钮可点击与不可点击，默认是可点击的
(1)设置按钮内不可点击
document.getElementById("bt1").disabled=true;
(2)设置按钮可点击
document.getElementById("bt1").disabled=false;
```

不知道为什么，当我改成disable=false后flag是无法点击的

weak auth

Login

https://blog.csdn.net/weixin_45664911

看到这个页面我先拿万能密码试了一下 (admin/' or '1'='1)
不成功

weak.php

159.138.137.79:55731 显示
password error

确定

https://blog.csdn.net/weixin_45664911

查看源码，弱口令进行爆破
弱口令字典

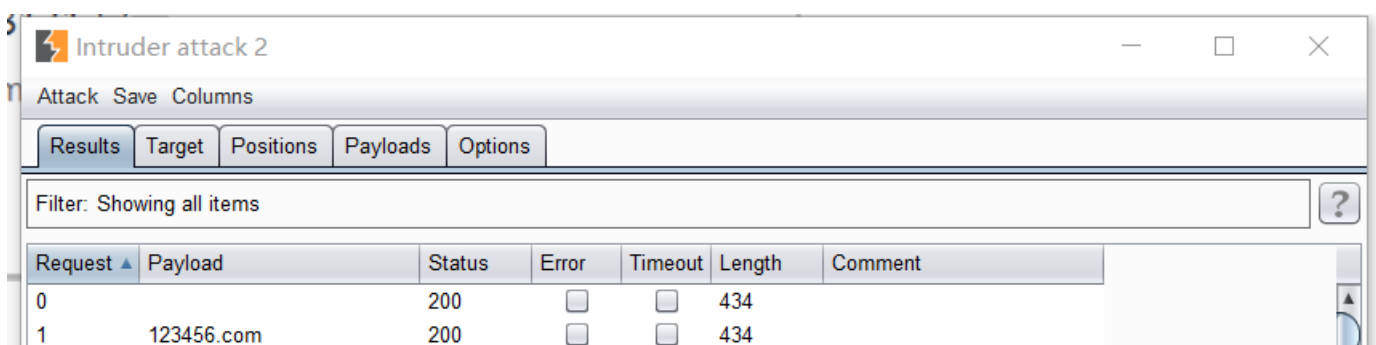
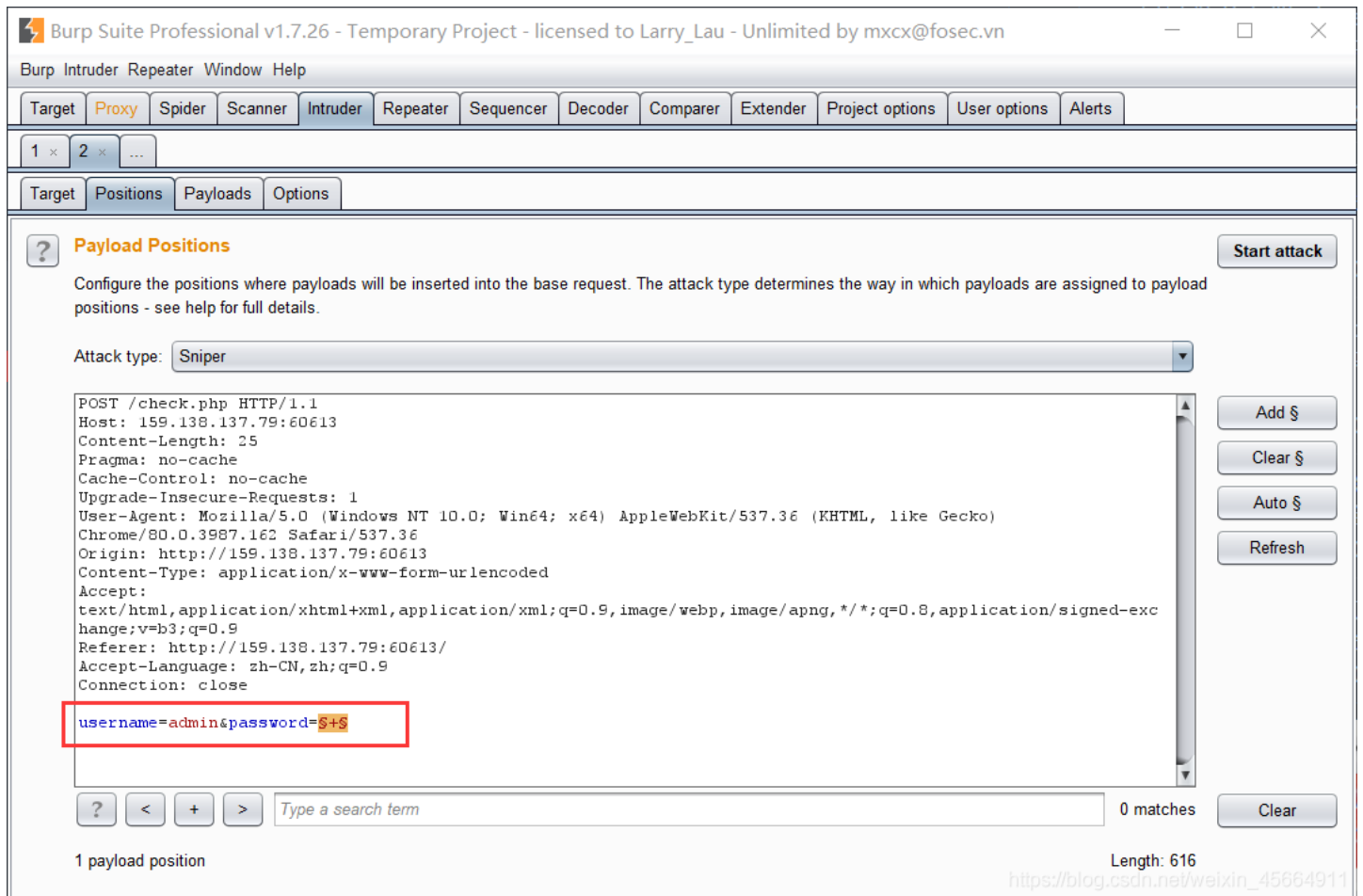
https://github.com/rootphantomer/Blasting_dictionary

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <title>weak auth</title>
6 </head>
7 <body>
8
9 <script>alert('please login as admin');</script><!--maybe you need a dictionary-->
10
11
12 </body>
13 </html>
```

如果用其他用户名登录的话，会显示以下弹窗，则推断用户名是admin



bp抓包——action——send to intruder——position（在password上加上符号\$，则过会字典代替尝试的是password而不是admin）——payloads——add 字典——start attack



| | | | | | |
|---|-------------|-----|--------------------------|--------------------------|-----|
| 2 | 123123 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 434 |
| 3 | idc123!@# | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 434 |
| 4 | 123 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 434 |
| 5 | aaa123!@# | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 434 |
| 6 | qq123.com | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 434 |
| 7 | 123456 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 437 |
| 8 | wantian##*(| 200 | <input type="checkbox"/> | <input type="checkbox"/> | 434 |
| 9 | qwe123 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 434 |

Request Response

Raw Params Headers Hex

```
POST /check.php HTTP/1.1
Host: 159.138.137.79:60613
Content-Length: 30
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/80.0.3987.162 Safari/537.36
Origin: http://159.138.137.79:60613
Content-Type: application/x-www-form-urlencoded
```

得出来密码是123456，再次登录得flag

cyberpeace{2b284f9f31b4daaab584cb4e0c4bae90}

bp使用博客: <https://blog.csdn.net/u011781521/article/details/54772795>

simple 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;
}
?>
```

简单分析代码可知，当赋值a,b满足条件时就可以得到flag1+flag2

条件一

```
if($a==0 and $a){
    echo $flag1;
}
```

参数a==0并且a为真时输出flag1

条件二


```
if(is_numeric($b)){
    exit();
}
if($b>1234){
    echo $flag2;
}
```

第一个：如果b是数字或者数字字符串则退出

第二个：当b>1234,输出flag2

首先对于a的话，我们可以直接传一个字母a进去，因为a是没有赋值的，所以通过比较，字符串'a'==0是true的。并且a也是true的。

对于b来说，赋值1235a,则b就不是数字串了。而且1235a会自动转换为1235大于1234



当然也有其他的方法，可以看flag是否完整来看赋值是否正确

知识点

1. PHP中“==”和“===”

“==”在进行比较的时候，会先将字符串类型转化成相同，再比较。

当一个数值和字符串进行比较的时候，会将字符串转换成数值

“===”在进行比较的时候，会先判断两种字符串的类型是否相等，再比较

例：“admin”==0 比较的时候，会将admin转化成数值，强制转化,由于admin是字符串，转化的结果是0自然和0相等；

“1admin”==1 比较的时候会将1admin转化成数值,结果为1；

而“admin1”==1 却等于错误，也就是“admin1”被转化成了0；

2. is_numeric() 函数

is_numeric(b)表示b为数字或者数字字符串的时候，is_numeric的值为真

3. PHP弱类型

php一个数字和一个字符串进行比较或者进行运算时，PHP会把字符串转换成数字再进行比较。PHP转换的规则的是：若字符串以数字开头，则取开头数字作为转换结果，若无则输出，纯字母被转换为0。若字符串以字母开头，也输出0