




# CTF Web学习（一）----基础篇及头文件修改、隐藏

原创

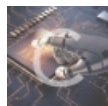
网络猿  于 2021-01-10 16:42:42 发布  971  收藏 16

分类专栏: [我的CTF Web学习之路](#) 文章标签: [php](#) [python](#) [数据库](#) [网络安全](#)

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\\_36451824/article/details/112426297](https://blog.csdn.net/qq_36451824/article/details/112426297)

版权



[我的CTF Web学习之路](#) 专栏收录该内容

4 篇文章 1 订阅

订阅专栏

## CTF Web学习（一）

基础篇及头文件修改、隐藏

---

CTF Web学习目录链接

[CTF Web学习（一）：基础篇及头文件修改、隐藏](#)

[CTF Web学习（二）：代码审计、burp suite应用](#)

[CTF Web学习（三）：python脚本的编写及应用](#)

[CTF Web学习（四）：SQL注入](#)

文章目录

## CTF Web学习（一）

### 前言

#### 一、直接查看源代码

##### （一）F12看代码

- 1、bugku web1题
- 2、bugku web2题

#### 二、头文件、属性、隐藏等

##### （一）input限制输入长度

- 1、修改maxlength属性

##### （二）修改头文件

- 1、修改User Agent属性
- 2、修改Accept-Language属性
- 3、修改cookie
- 4、头文件里藏flag
- 5、域名解析
- 6、修改Referer
- 7、修改X-Forwarded-For

##### （三）各种隐藏

- 1、302隐藏
- 2、js隐藏

#### 三、传参

##### （一）get传参

- 1、基础篇

##### （二）post传参

- 1、基础篇

### 总结

---

## 前言

CTF Web的题型，按照目前我的理解，就是玩网站，拿到自己想要的东西，就像CTF比赛一样，拿flag、key及其他隐藏信息，而在现实生活中，可能就是拿数据库权限，拿服务器权限等等。而本篇主要是从零基础开始学习，如果有大佬发现问题，还望即使指正。

---

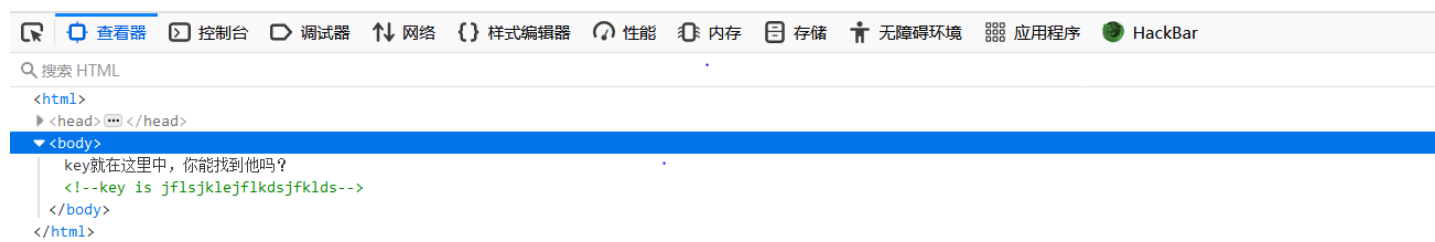
## 一、直接查看源代码

### （一）F12看代码

#### 1、bugku web1题

链接: [http://lab1.xseclab.com/base1\\_4a4d993ed7bd7d467b27af52d2aaa800/index.php](http://lab1.xseclab.com/base1_4a4d993ed7bd7d467b27af52d2aaa800/index.php)

WriteUp: 直接F12



[https://blog.csdn.net/qq\\_36451824](https://blog.csdn.net/qq_36451824)

## 2、bugku web2题

链接: <http://123.206.87.240:8002/web2/>

WriteUp: 和上题一样, 直接F12

## 二、头文件、属性、隐藏等

### (一) input限制输入长度

#### 1、修改maxlength属性

1、<http://123.206.87.240:8002/yanzhengma/>

2、[http://lab1.xseclab.com/base10\\_0b4e4866096913ac9c3a2272dde27215/index.php](http://lab1.xseclab.com/base10_0b4e4866096913ac9c3a2272dde27215/index.php)

WriteUp: 上面两道题就是修改input的maxlength参数, 或者直接删除即可



53+77=?  验证

查看器 控制台 调试器 网络 样式编辑器

搜索 HTML

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "ht
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
  <body>
    <span id="code" class="code" style="background: rgb(80, 104, 2
    <input class="input" type="text" maxlength="123">
    <button id="check">验证</button>
  <div style="text-align:center;">
    <script src="js/jquery-1.12.3.min.js"></script>
    <script type="text/javascript" src="js/code.js"></script>
  </body>
</html>
```



提交

数字太小了!

查看器 控制台 调试器 网络 样式编辑器 性能 内网

搜索 HTML

```
<html>
  <head>
  <body>
    <form action="" method="post">
      <input type="text" maxlength="123" name="v">
    </form>
  </body>
</html>
```

## (二) 修改头文件

### 1、修改User Agent属性

1、[http://lab1.xseclab.com/base6\\_6082c908819e105c378eb93b6631c4d3/index.php](http://lab1.xseclab.com/base6_6082c908819e105c378eb93b6631c4d3/index.php)

提示：只允许使用HAHA浏览器，请下载HAHA浏览器访问！

WriteUp：提示需要用HAHA浏览器，说是下载，其实就没有这个浏览器，因此想到需要修改User Agent。可以用HackBar直接修改，也可以用burp suite 修改User Agent，结果一样。



注：如果用火狐的HackBar，需要用2.1.3之前的版本，之后版本是要收费的，不能execute。[HackBar2.1.3下载地址](#)，添加后记得把自动更新关闭，否则会升级的。

## 2、修改Accept-Language属性

1、[http://lab1.xseclab.com/base1\\_0ef337f3afbe42d5619d7a36c19c20ab/index.php](http://lab1.xseclab.com/base1_0ef337f3afbe42d5619d7a36c19c20ab/index.php)

提示：only for Foreigner

WriteUp：使用burp suite修改语言Accept-Language，只要不是中文就行。

```
GET /base1_0ef337f3afbe42d5619d7a36c19c20ab/index.php HTTP/1.1
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
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
Upgrade-Insecure-Requests: 1
```

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

改为：us-Ch,us;q=0.8,en-US;q=0.3,en;q=0.2

## 3、修改cookie

1、[http://lab1.xseclab.com/base9\\_ab629d778e3a29540dfd60f2e548a5eb/index.php](http://lab1.xseclab.com/base9_ab629d778e3a29540dfd60f2e548a5eb/index.php)

提示：必须要登陆才能得到key

WriteUp: burp suite修改cookie的值，让Login=1，就□了

```
GET /base9_ab629d778e3a29540dfd60f2e548a5eb/index.php HTTP/1.1
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
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: Login=0
Upgrade-Insecure-Requests: 1
```

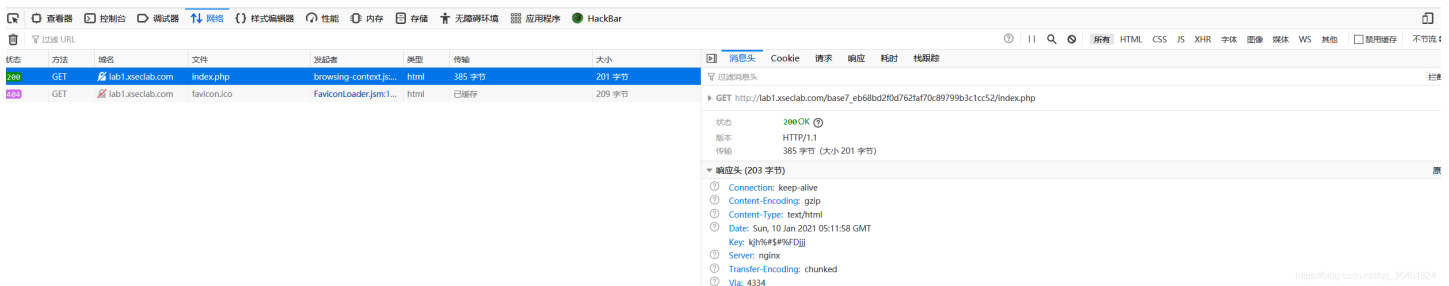
[https://blog.csdn.net/qq\\_36451824](https://blog.csdn.net/qq_36451824)

## 4、头文件里藏flag

1、[http://lab1.xseclab.com/base7\\_eb68bd2f0d762faf70c89799b3c1cc52/index.php](http://lab1.xseclab.com/base7_eb68bd2f0d762faf70c89799b3c1cc52/index.php)

提示：Key就在这里，猜猜这里是哪里呢？(Web找key加强版)

WriteUp: 用浏览器网络或者burp suite跟踪查看头文件



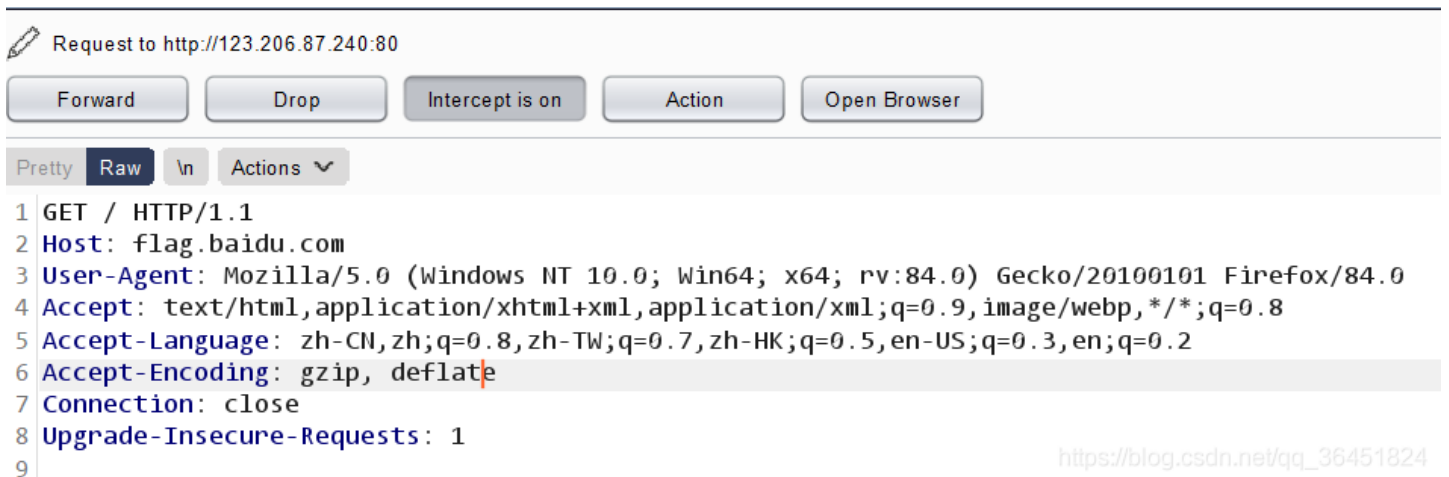
2、<http://123.206.87.240:9009/hd.php>

WriteUp: 该题和上面一样，用burp suite跟踪即可

## 5、域名解析

1、听说把flag.baidu.com解析到123.206.87.240就能拿到flag

WriteUp: 用burp suite修改Host属性为flag.baidu.com即可



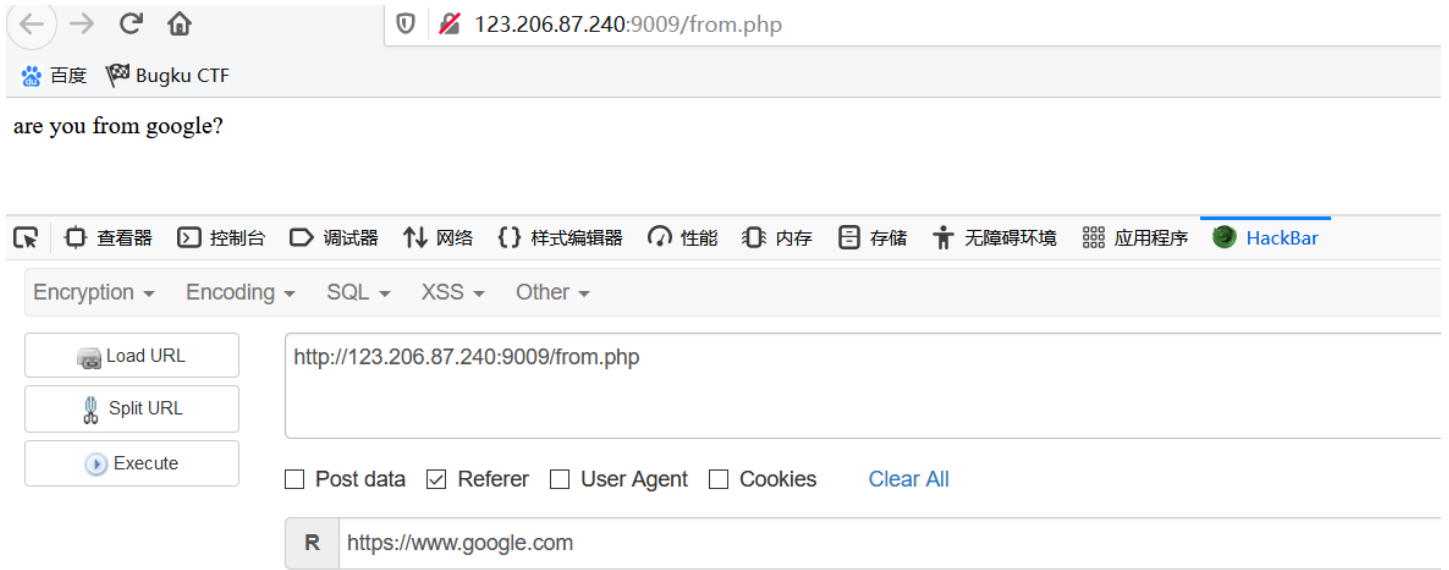
[https://blog.csdn.net/qq\\_36451824](https://blog.csdn.net/qq_36451824)

## 6、修改Referer

你从哪里来? are you from google?

1、<http://123.206.87.240:9009/from.php>

WriteUp: 修改或者添加referer为: <https://www.google.com>



are you from google?

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序 HackBar

Encryption Encoding SQL XSS Other

Load URL Split URL Execute

Post data  Referer  User Agent  Cookies Clear All

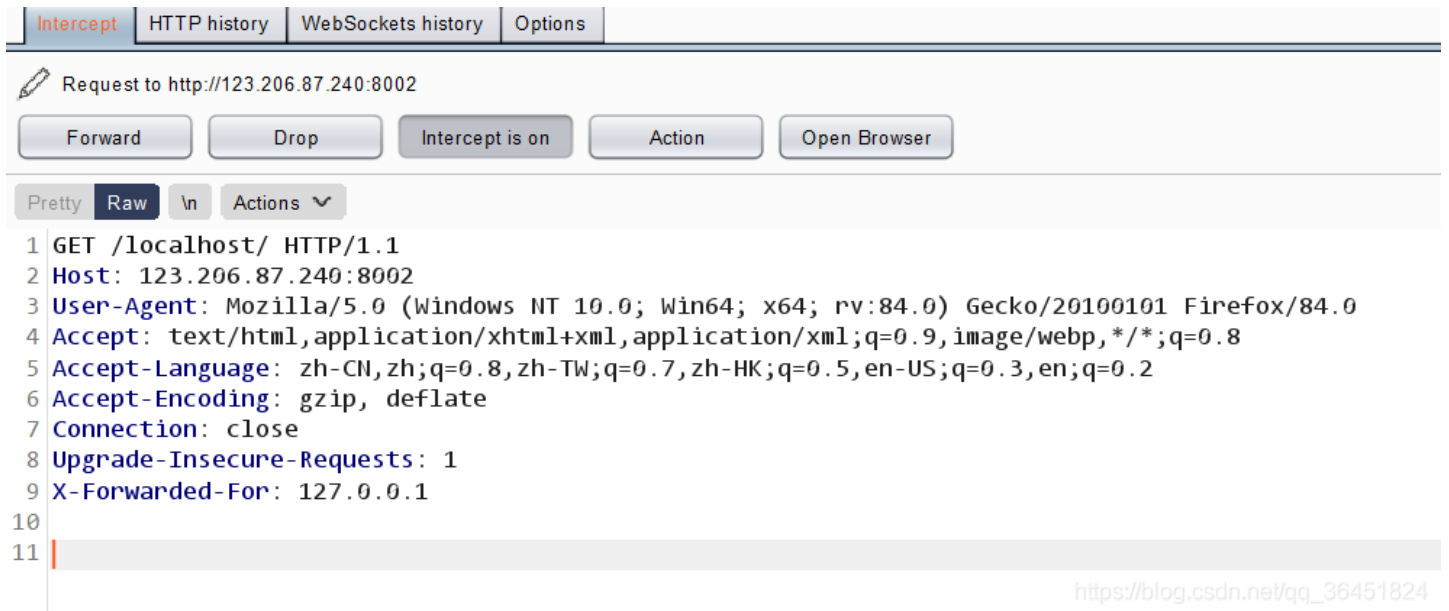
R <https://www.google.com>

[https://blog.csdn.net/qq\\_36451824](https://blog.csdn.net/qq_36451824)

## 7、修改X-Forwarded-For

1、<http://123.206.87.240:8002/localhost/>

WriteUp: 提示本地管理员, 修改X-Forwarded-For: 127.0.0.1



Intercept HTTP history WebSockets history Options

Request to <http://123.206.87.240:8002>

Forward Drop Intercept is on Action Open Browser

Pretty Raw ln Actions

```
1 GET /localhost/ HTTP/1.1
2 Host: 123.206.87.240:8002
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 X-Forwarded-For: 127.0.0.1
10
11
```

[https://blog.csdn.net/qq\\_36451824](https://blog.csdn.net/qq_36451824)

### (三) 各种隐藏

#### 1、302隐藏

1、[http://lab1.xseclab.com/base8\\_0abd63aa54bef0464289d6a42465f354/index.php](http://lab1.xseclab.com/base8_0abd63aa54bef0464289d6a42465f354/index.php)

WriteUp: 点击链接发现提示key is not here!, 用burp suite截包或者网络发现有个302地址key\_is\_here\_now\_.php

状态	方法	域名	文件	发起者	类型	传输	大小
302	GET	lab1.xseclab.com	search_key.php	document	html	261 字节	16 字节
200	GET	hacklist.sinaapp.c...	index_no_key.php	document	html	162 字节	16 字节
404	GET	hacklist.sinaapp.c...	favicon.ico	FaviconLoader.jsm:1...	html	已缓存	209 字节

## 2、js隐藏

1、<http://123.206.87.240:8002/web3/>

WriteUp: 用调试器可以看到js代码

```
alert("flag就在这里");  
alert("来找找吧");  
<!--&#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;&#73;&#125;-->
```

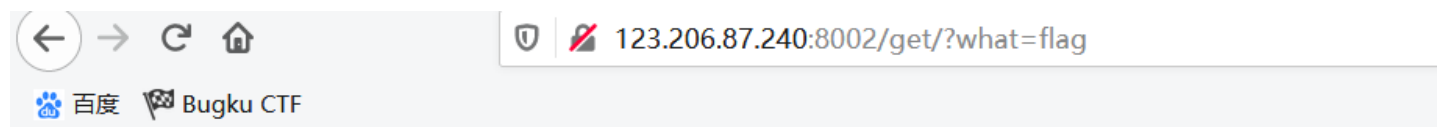
解码得KEY{J2sa42ahJK-HS11lll}





```
$what=$_GET['what']; #取what的值
echo $what;
if($what=='flag') #如果what==fLag
echo 'flag{****}'; #给出fLag
```

WriteUp: 上面这种就为最基础的get传参赋值, 小白可以这样理解, get就是取网址问号之后的参数和值。即网址后面加上?what=flag就行了。



```
$what=$_GET['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
flagflag{bugku_get_su8kej2en}
```



## (二) post传参

### 1、基础篇

1、http://123.206.87.240:8002/post/

提示:

```
$what=$_POST['what']; #取what的值
echo $what;
if($what=='flag') #如果what==fLag
echo 'flag{****}'; #给出fLag
```

WriteUp: 上面这种就为最基础的post传参赋值。即post值为what=flag就行了。

The image shows a browser window with a shell script and a Burp Suite interface. The browser address bar shows the URL `123.206.87.240:8002/post/`. The shell script is as follows:

```
$what=$_POST['what'];  
echo $what;  
if($what=='flag')  
echo 'flag{****}';  
flagflag{bugku_get_ssseint67se}
```

The Burp Suite interface shows the URL `http://123.206.87.240:8002/post/` and the post data `what=flag`. The interface includes a toolbar with icons for '查看器' (Viewer), '控制台' (Console), '调试器' (Debugger), '网络' (Network), '样式编辑器' (Style Editor), '性能' (Performance), '内存' (Memory), '存储' (Storage), and '无障碍环境' (Accessibility). Below the toolbar are dropdown menus for 'Encryption', 'Encoding', 'SQL', 'XSS', and 'Other'. On the left side, there are buttons for 'Load URL', 'Split URL', and 'Execute'. On the right side, there are checkboxes for 'Post data', 'Referer', 'User Agent', and 'Cookies', along with a 'Clear All' button. The URL `https://blog.csdn.net/qq_36451824` is visible in the bottom right corner.

## 总结

其实做CTF Web的题型时，拿上题，可做以下步骤：

- 1、看看题目有没有明显的提示，包括页面展示和网址
- 2、右键查看源代码
- 3、网络跟踪或者burp suite截包看有没有头文件或者隐藏信息
- 4、需要简单审计代码

以上即为本次学习的自我总结，如果有不恰之处，还望大佬指出。如果文章中存在侵权或者未经授权等现象，还望私聊我。