

攻防世界xff_referer解析

原创

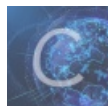
[nwpuhkp](#) 于 2021-10-30 10:35:11 发布 140 收藏

分类专栏: [web 攻防世界](#) 文章标签: [web php](#)

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/chlet/article/details/121047423>

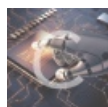
版权



[web](#) 同时被 2 个专栏收录

1 篇文章 0 订阅

订阅专栏



[攻防世界](#)

3 篇文章 0 订阅

订阅专栏

攻防世界xff_referer解析

xff_referer

👍 173

最佳Writeup由 **话求 · DengZ** 提供

难度系数: ★★ 2.0

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。

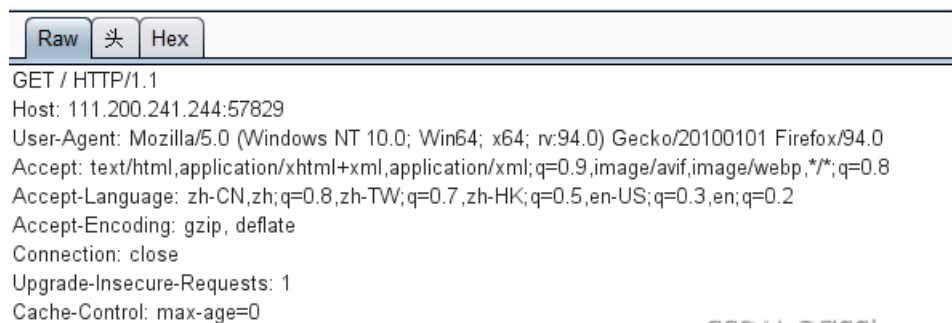
题目场景: [点击获取在线场景](#)

题目附件: 暂无

ip地址必须为123.123.123.123

获取场景后发现，要求IP为123.123.123.123；

可以使用火狐浏览器的X-Forwarded-For插件；
这里使用Burpsuit；



CSDN @755long

抓到请求信息；
在host后添加X-Forwarded-For:123.123.123.123；

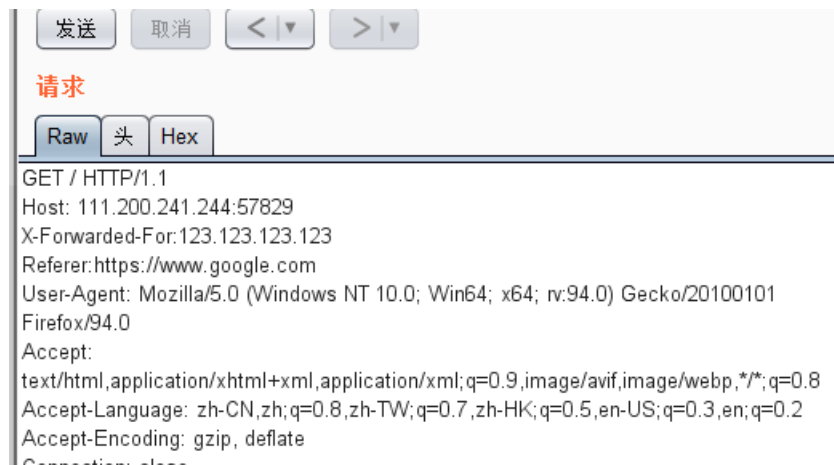


在重发器中发送；

```
}
</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><
```

发现有了另一个限制；

要求来自谷歌；



Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

CSDN @7SSlong

在X-Forwarded-For:123.123.123.123后面加上Referer:https://www.google.com;

响应

Raw 头 Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 29 Oct 2021 05:56:16 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>
<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{00d718277bcc2e5603be581be7122
4d2}";</script></body>
</html>
```

CSDN @7SSlong

得到flag;

cyberpeace{00d718277bcc2e5603be581be71224d2}