

# 攻防世界 web xff\_referer

原创

AKalone 于 2019-10-26 10:39:08 发布 2357 收藏 3

分类专栏: [攻防世界](#) 文章标签: [攻防世界](#) [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/shidonghang/article/details/102737570>

版权



[攻防世界](#) 专栏收录该内容

13 篇文章 0 订阅

订阅专栏

## xff\_referer

### 题目

xff\_referer 👍 14 最佳Writeup由 [话求](#) • [DengZ](#) 提供

难度系数: ★ 1.0

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。

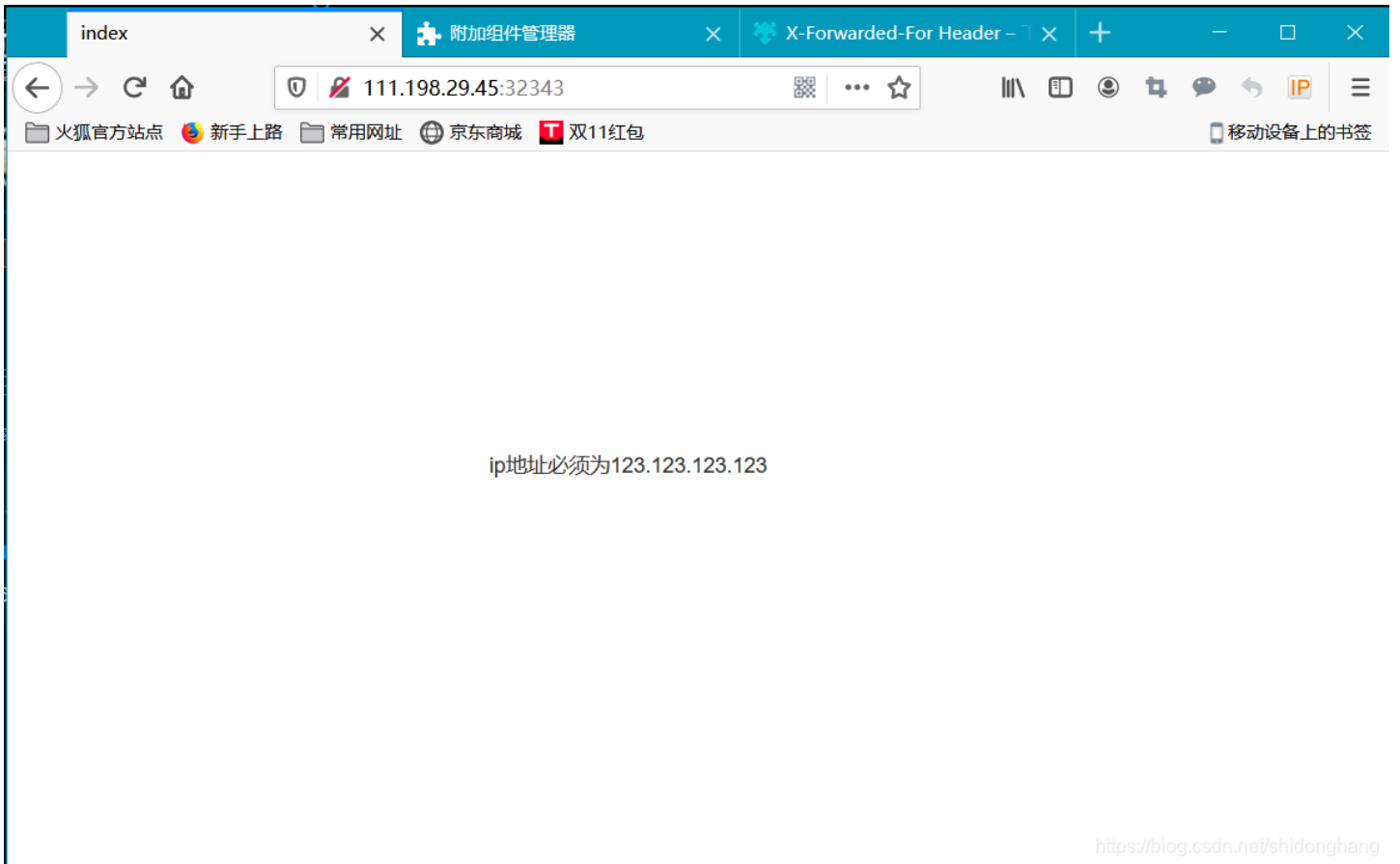
题目场景:  删除场景

倒计时: 03:56:24 延时

题目附件: 暂无

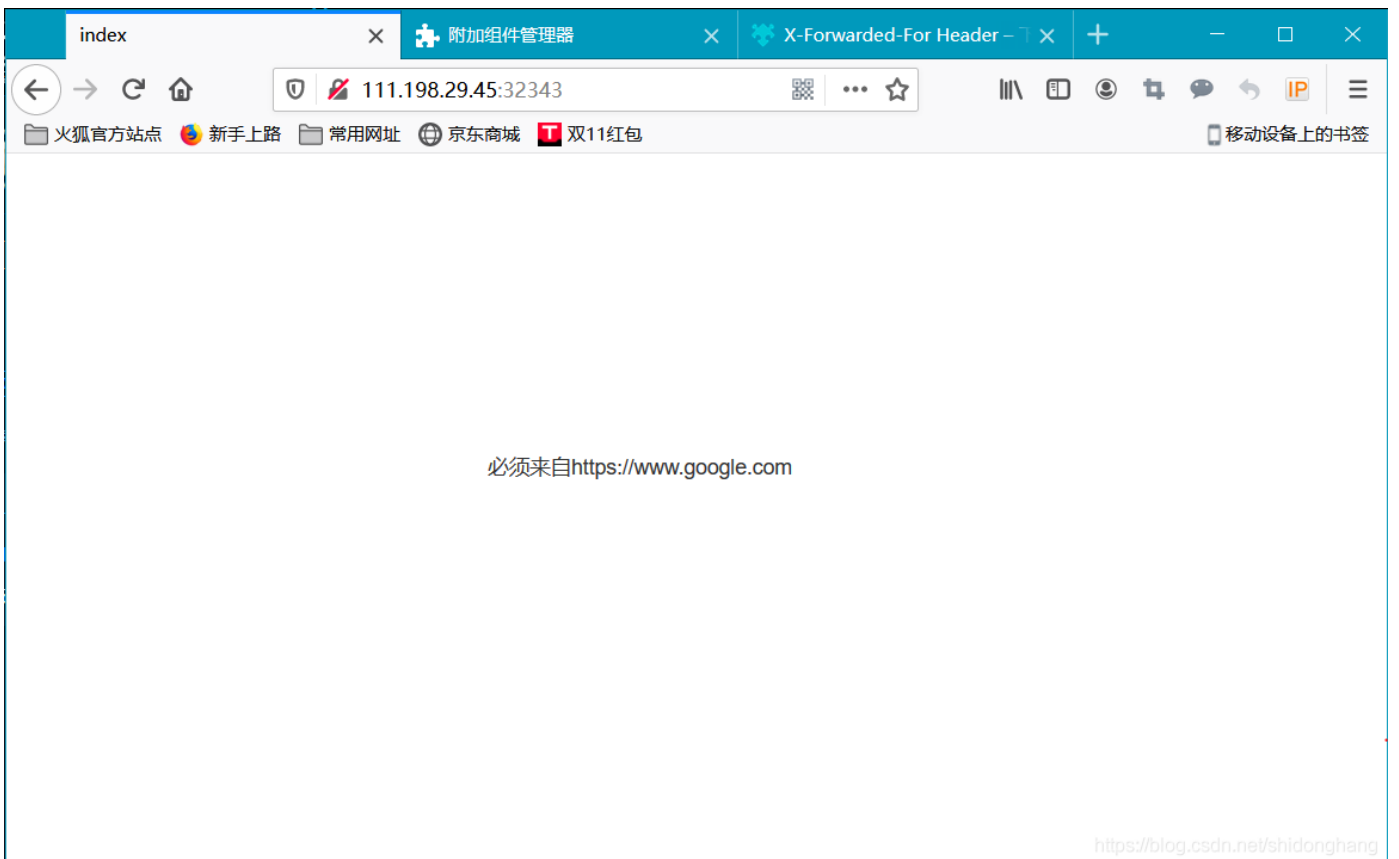
<https://blog.csdn.net/shidonghang>

### 场景



## 过程

- 使用火狐的X-Forwarded-For Header来更改IP为123.123.123.123。



- 重新编辑报文，在最下面加入Cache-Control:max-age=0，再发送。

新请求

取消 发送

方法 GET 网址 http://111.198.29.45:32343/

请求头:

```
Host: 111.198.29.45:32343
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: keep-alive
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 123.123.123.123
Cache-Control: max-age=0
```

<https://blog.csdn.net/shidonghang>

- 从响应载荷下面一长串中可以找到flag。

消息头 Cookie 参数 响应 耗时 堆栈跟踪

预览

ip地址必须为123.123.123.123

▼ 响应载荷 (payload)

```
3 <!-- U!r-8 -->
4 </title>
5 http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />
6
7
8 in-left:auto;
9 in-right:auto;
10 in-top:200px;
11 h:20em;
12
13
14
15
16 址必须为123.123.123.123</p>
17 .getElementById("demo").innerHTML="必须来自https://www.google.com";</script><script>document.getElementById("demo").innerHTML="cyberpeace{954dabc349420a085daf1938bf2aa64c}";</script><
18
19
```

<https://blog.csdn.net/shidonghang>