

攻防世界WEB新手入门10 xff_referer

原创

[EliAyase](#) 于 2020-08-05 09:43:37 发布 283 收藏 1

分类专栏: [攻防世界](#) 文章标签: [web 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_39787312/article/details/107793211

版权



[攻防世界](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

攻防世界WEB新手入门10 xff_referer

题目信息

WriteUp

题目信息

xff_referer  73 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

https://blog.csdn.net/qq_39787312

WriteUp

打开链接后看到如下信息

ip地址必须为123.123.123.123

结合题目可知需要伪造XFF。

打开burpsuite进行抓包

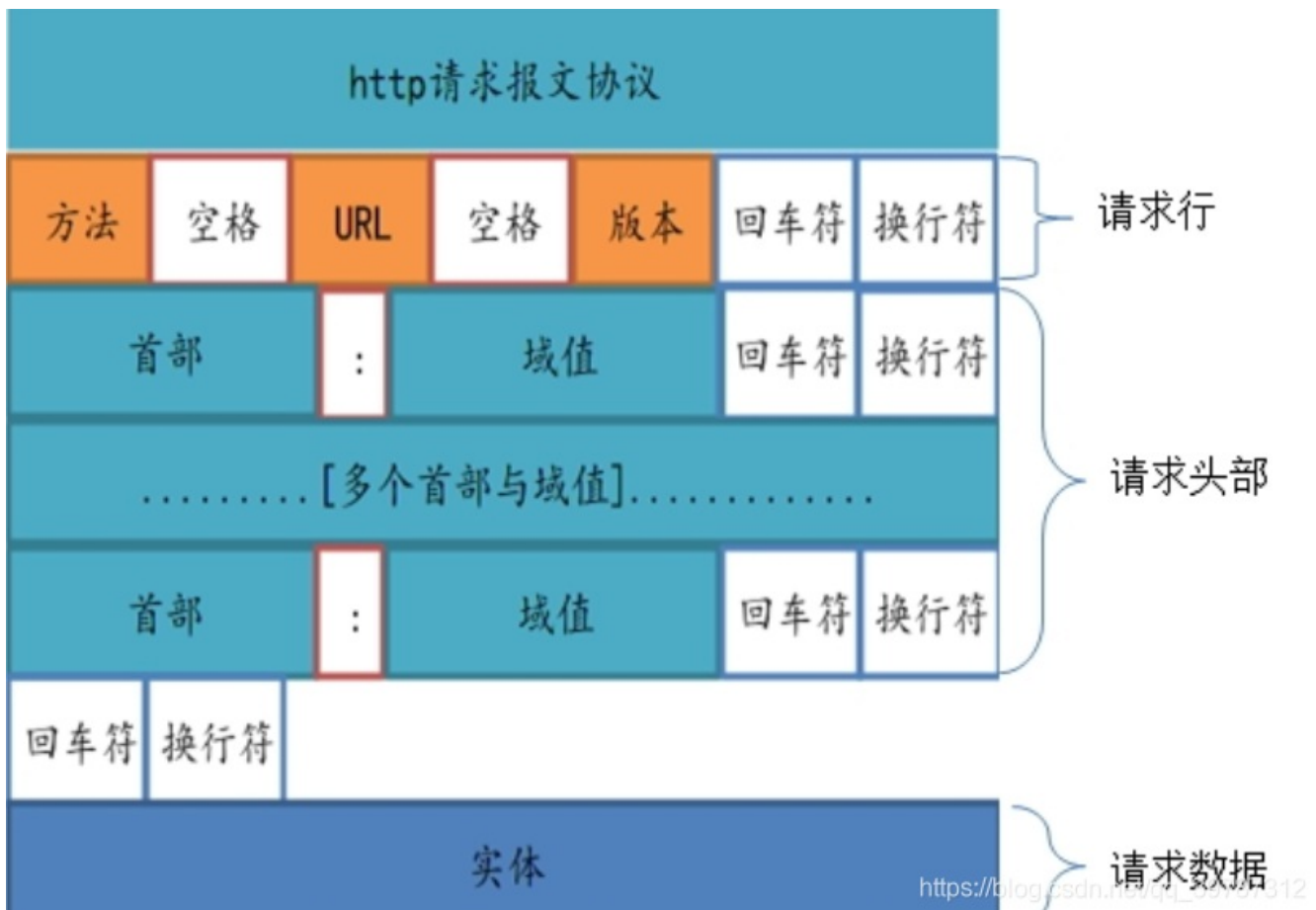
```
1 GET / HTTP/1.1
2 X-Forwarded-For: 123.123.123.123
3 Host: 220.249.52.133:52387
4 Pragma: no-cache
5 Cache-Control: no-cache
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; ;
8 Accept: text/html,application/xhtml+xml,application/javascript;q=0.9,*/*;q=0.8
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8
11 Connection: close
12
```

在包头添加XFF信息

```
X-Forwarded-For: 123.123.123.123
```

发送以后发现没有响应

咨询大佬以后得到回复：http报文结束时需要两行空白行



至于burpsuite抓包时只有一行空白且能正常响应的原因暂时未知。

在响应包后多加一行空白即可正常响应。

响应页面如下:

必须来自<https://www.google.com>

再添加Referer

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

```
1 GET / HTTP/1.1
2 X-Forwarded-For: 123.123.123.123
3 Referer: https://www.google.com
4 Host: 220.249.52.133:52387
5 Cache-Control: max-age=0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Winr
8 Accept: text/html,application/xhtml+xml,appli
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8
11 Connection: close
12
13
```

https://blog.csdn.net/qq_39787312

发送即可得到flag