攻防世界WEB新手入门10 xff_referer

原创

EliAyase 于 2020-08-05 09:43:37 发布

分类专栏： 攻防世界 文章标签： web 安全

攻防世界WEB新手入门10 xff_referer

题目信息

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

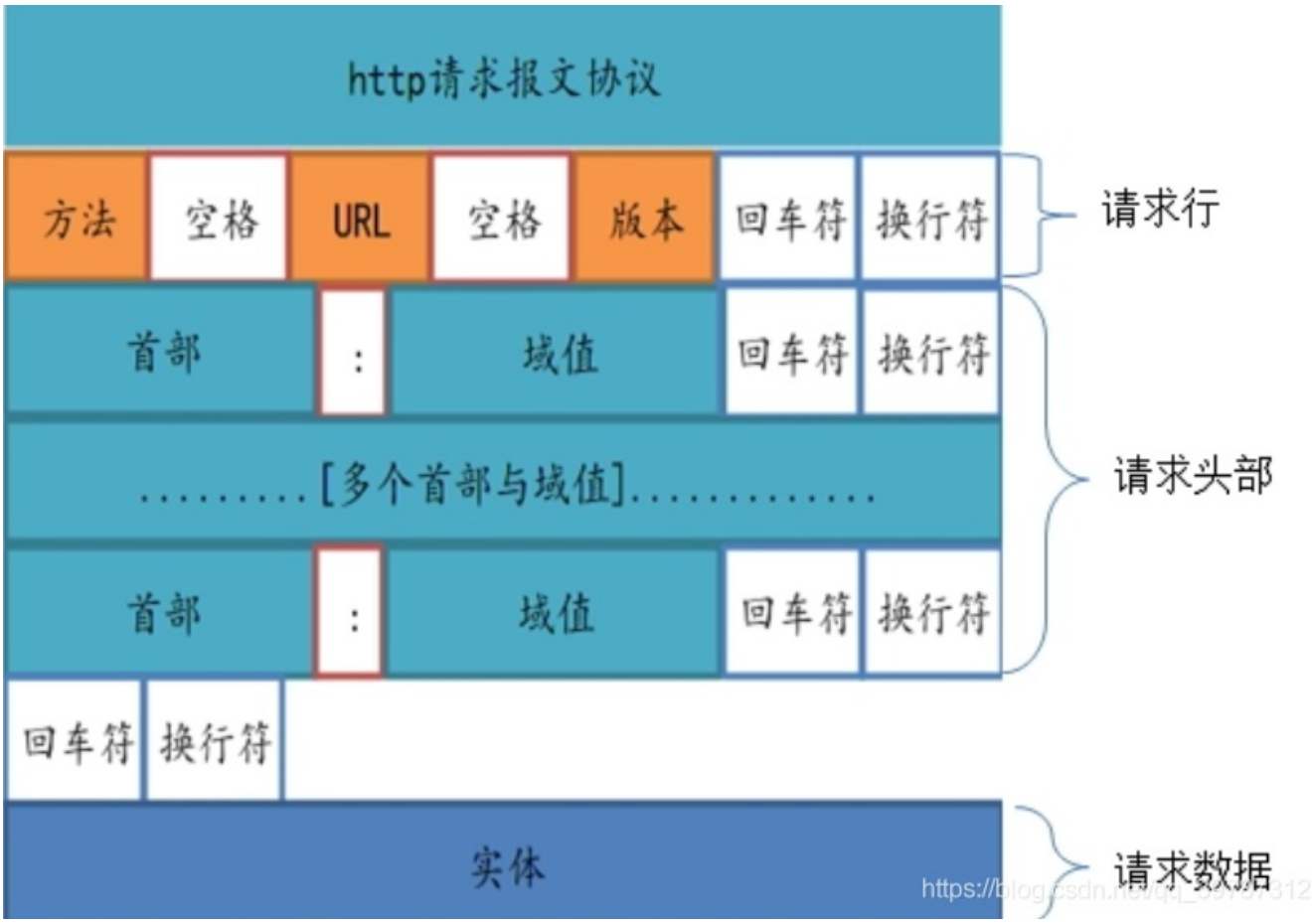
```
GET / HTTP/1.1
X-Forwarded-For: 123.123.123.123
Host: 220.249.52.133:52387
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; 
Accept: text/html,application/xhtml+xml,applicati
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8
Connection: close

```

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

发送即可得到flag