

攻防世界xff_referer

原创

ProbeN1 于 2021-01-24 10:51:57 发布 397 收藏 1

分类专栏: [CTF](#)

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/m0_51792282/article/details/112264410

版权



[CTF 专栏收录该内容](#)

11 篇文章 0 订阅

订阅专栏

X老师告诉小宁其实xff和referer是可以伪造的。

(1) X-Forwarded-For:简称XFF头, 它代表客户端, 也就是HTTP的请求端真实的IP, 只有在通过了HTTP代理或者负载均衡服务器时才会添加该项。xff是http的拓展头部, 作用是使Web服务器获取访问用户的IP真实地址(可伪造)。由于很多用户通过代理服务器进行访问, 服务器只能获取代理服务器的IP地址, 而xff的作用在于记录用户的真实IP, 以及代理服务器的IP。格式为:

X-Forwarded-For: 本机IP, 代理1IP, 代理2IP, 代理2IP

(2) HTTP 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, 告诉服务器我是从哪个页面链接过来的, 服务器基此可以获得一些信息用于处理。referer是http的拓展头部, 作用是记录当前请求页面的来源页面的地址。服务器使用referer确认访问来源, 如果referer内容不符合要求, 服务器可以拦截或者重定向请求。

Burp: 直接在请求头添加:

X-Forwarded-For:123.123.123.123

提示必须来自谷歌

再添加

Referer:https://www.google.com

出来了



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)