【墨子学院Writeup】用火狐插件ModifyHeader或者burpsuit来伪造Referer(来源页)获取flag(KEY)

原创

iqiqiya 于 2018-05-23 17:55:21 发布 4170 收藏 2
分类专栏： ------墨者学院CTF 我的CTF之路 杂七杂八经验 我的CTF进阶之路 文章标签： 用火狐插件ModifyHeader或者burpsuit来伪造 burpsuit来伪造Referer(来源页) 【墨子学院Writeup】

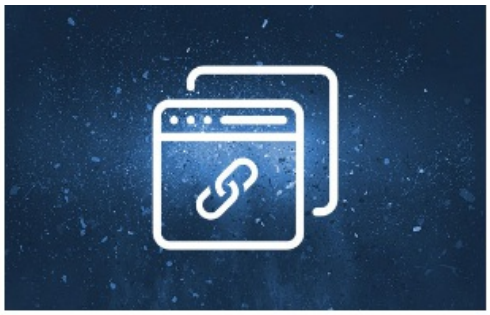

------墨者学院CTF 同时被 3 个专栏收录
3 篇文章 0 订阅
订阅专栏


我的CTF之路
92 篇文章 5 订阅
订阅专栏


杂七杂八经验
122 篇文章 1 订阅
订阅专栏

有好多种方法　但都是通过伪装Referer

本文只介绍两种



来源页伪造

难易程度：★ ★
增加经验：60 (完成可获得经验值)
消耗墨币：免费

分类：网络安全
标签：浏览器 抓包

提交KEY　放弃

IP地址：219.153.49.228　端口：47799　协议：http　其他：无　[点击访问]

靶场介绍　解题思路　防御方案

登录 > 点击启动靶场环境 > 访问靶场 > 解题找到KEY > 提交KEY > 发表解题思路 > 完成

背景介绍

安全工程师“墨者”在访问一个网页时，提示只能通过另一个页面跳转的方式访问，这该如何办？

实训目标

1、了解浏览器的使用；
2、了解数据包的发送；
3、了解抓包工具的使用，能够进行抓包改包，如burpsuite等；
（掌握：达到能够独立完成使用的程度
了解：达到知晓其作用的程度不要求熟练运用）

解题方向

解题方向

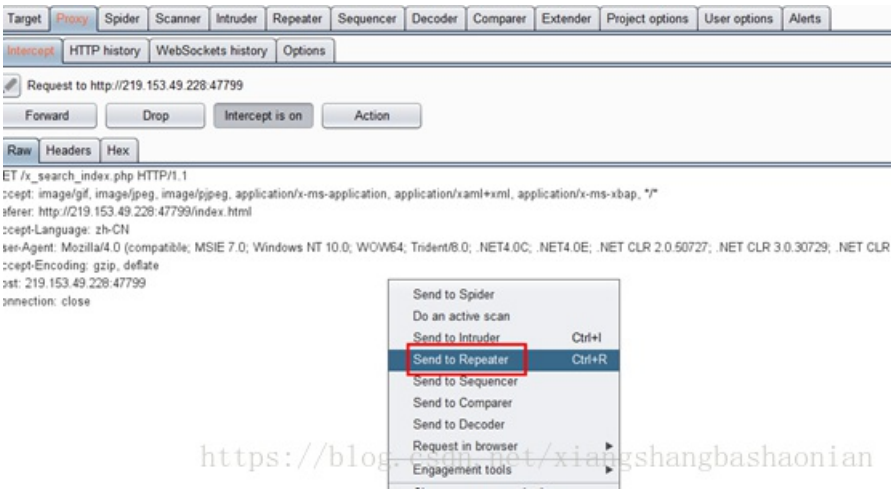
充分理解题目，referer伪造！

先看看题目

页面上有一个按钮

点击会提示当前页面只允许从google.com访问　猜测需要burp抓包　根据上边提示加上Referer: google.com就可以啦

可是需要注意了　这里是个坑　必须是http://www.google.com才可以。。。



恭喜成功伪造来源页！
KEY:

mozhe50e6fba2b50dc90ef292b5f2f75

注意：还可以用火狐插件Modify header进行构造