

BugkuCTF web12_本地管理员 writeup

原创

Mitch311 于 2020-12-21 18:21:10 发布 802 收藏 1

分类专栏: CTF 文章标签: unctf

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/Mitchell_Donovan/article/details/111480321

版权



[CTF 专栏收录该内容](#)

51 篇文章 3 订阅

订阅专栏

web12_本地管理员

[原题链接](#)

key:base64解码+XFF伪造请求头

①查看源代码发现了线索, 拿去base64解码得到字符串'test123'

管理员系统

Username:

Password:

Submit Reset



②猜测用户名admin, 密码test123, 尝试登陆, 发现登陆失败

管理员系统

Username: admin

Password:

Submit Reset

IP禁止访问, 请联系本地管理员登陆, IP已被记录.

https://blog.csdn.net/Mitchell_Donovan

③题干反复强调"本地", 可以想到用伪造XFF请求头来访问

④burpsuite抓包，送到repeater，然后在请求头部 Headers 添加 X-Forwarded-For:127.0.0.1，go一下即可得到flag

