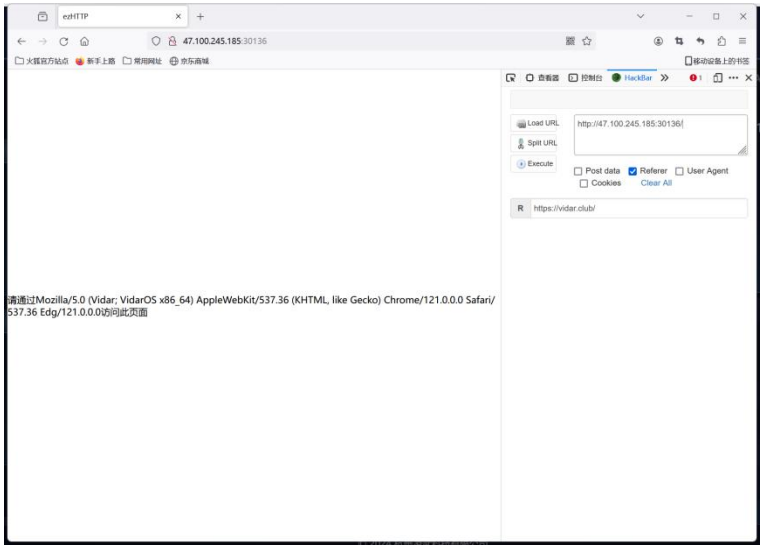
HGAME 2024　WEEK 1　wp

Written by FCowardB

1. ezhttp:

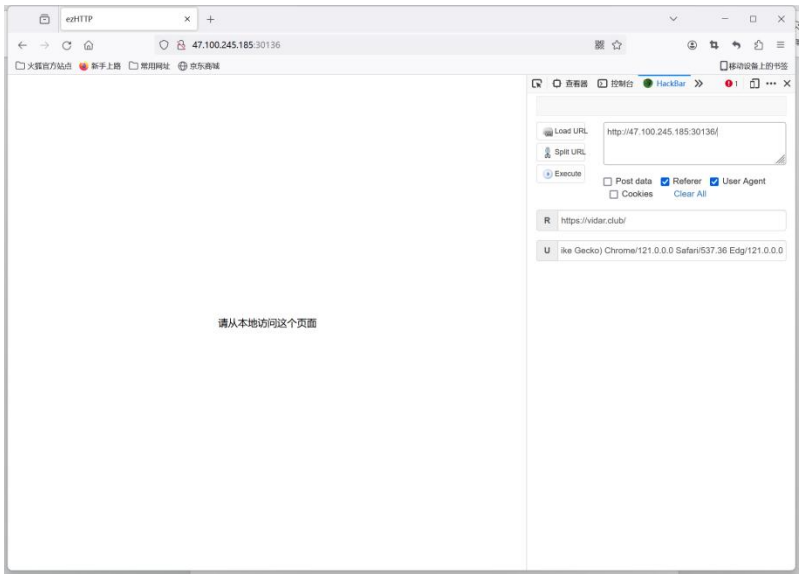
打开靶机提示要在 vidar.club 打开靶机，根据 http 协议，需要在 header 中添加 Referer 字段

利用 firefox 的 hackbar 直接添加



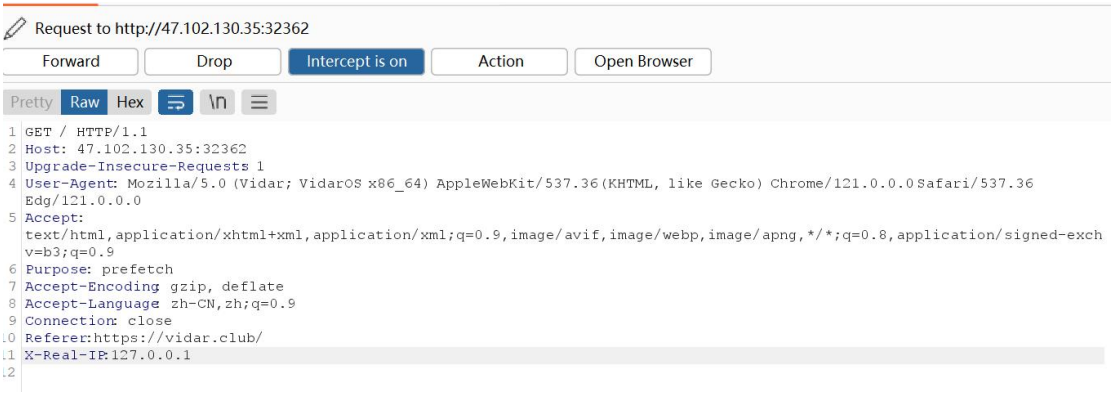
又提示：请通过 Mozilla/5.0 (Vidar; VidarOS x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0 访问此页面

很容易看出这是 nser-agent 头，再次利用 hackbar 修改 ua 头

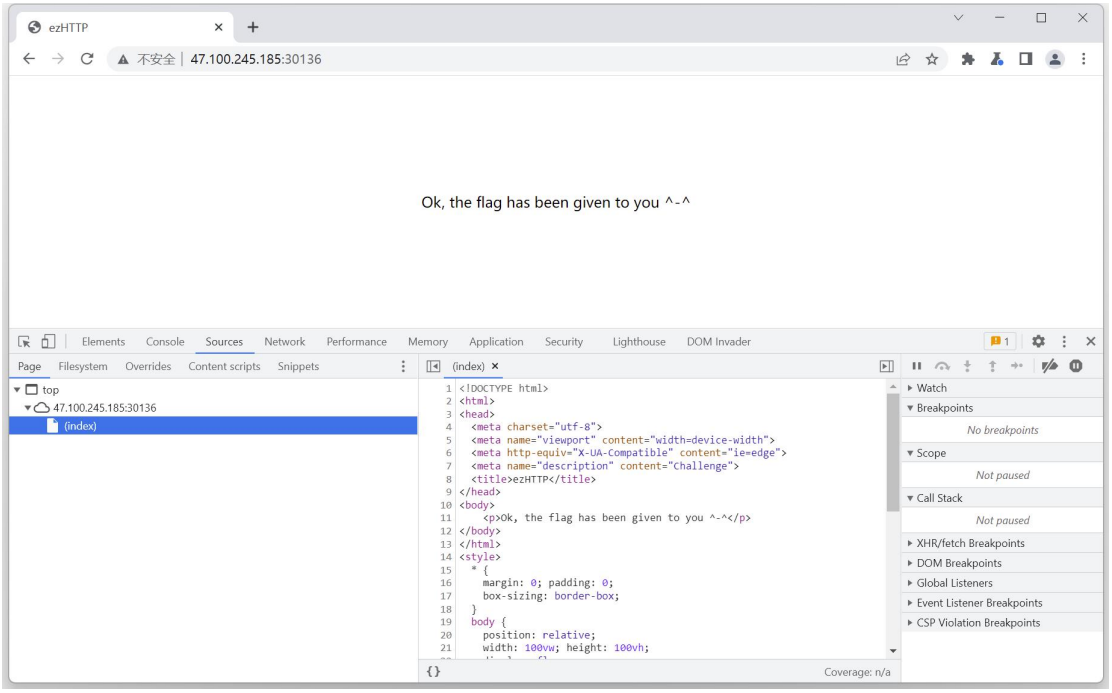


提示要从本地访问页面，
X-Forwarded-For（XFF）是用来识别通过 HTTP 代理或负载均衡方式连接到 Web 服务器的客户端最原始的 IP 地址的 HTTP 请求头字段

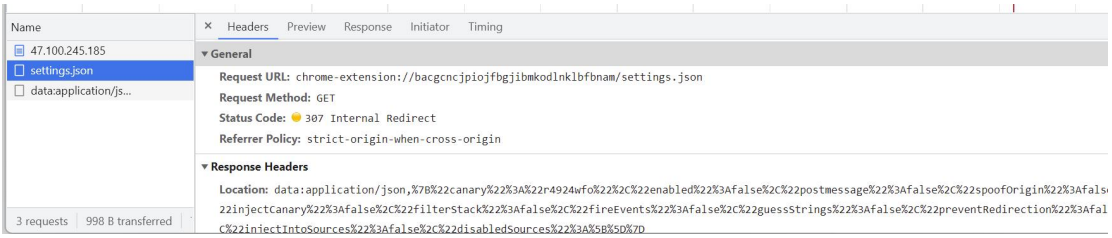
所以需要添加 XFF 字段，利用 bp 添加 XFF 发现不行，再查找资料发现很多字段都可以标志本地访问
[CTF 题目中伪造 IP 方法_ctf 伪装 127.0.0.1-CSDN 博客]
需要使用 bp 反复尝试(非常浪费时间,每次都需要重新输入 Referer 和 UA 字段)
反复尝试发现 X-real-ip 字段有效



之后提示 flag is given to you
但是页面中并没有显示，猜测可能在源代码或者响应头里



源代码中没有发现
但



查阅资料 JSON Web Token 说是 header payload 通常是 base64 编码的 josn 字符串，所以通过 base64 解码 payload 部分得到

{ “F14g” : “hgame{HTTP_!s_1mP0rT4nt}”

2.