10、XCTF xff_referer

原创

山兔1 于 2021-09-16 23:38:09 发布 164 收藏

分类专栏： CTF 文章标签： http

本文链接：https://blog.csdn.net/m0_53008479/article/details/120339977

`X` 老师告诉小宁其实 `xff` 和 `referer` 是可以伪造的。

拦截数据包，修改数据包。

```
X-Forwarded-For: 123.123.123.123
```

这个必须加在 `http` 的请求头。

得到：

必须来自 `https://www.google.com`

再在请求头加上 `Referer: https://www.google.com`

得到 `flag`，

基础知识：

`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。

简单地说， `xff` 是告诉服务器当前请求者的最终 `ip` 的 `http` 请求头字段

通常可以直接通过修改 `http` 头中的 `X-Forwarded-For` 字段来仿造请求的最终 `ip` 。

`HTTP` 来源地址（ `referer` ，或 `HTTPreferer` ）

是 `HTTP` 表头的一个字段，用来表示从哪儿链接到当前的网页，采用的格式是 `URL` 。换句话说，借着 `HTTP` 来源地址，当前的网页可以检查访客从哪里而来，这也常被用来对付伪造的跨网站请求。

简单的讲， `referer` 就是告诉服务器当前访问者是从哪个 `url` 地址跳转到自己的，跟 `xff` 一样， `referer` 也可直接修改。