




CTF | CTF-Web 捉迷藏

原创

大青呐  于 2019-07-10 13:52:41 发布  867  收藏 2

分类专栏: [CTF-Web实验](#) [CTF-Web实验](#) 文章标签: [CTF-Web](#)

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/qq_42646885/article/details/95321970

版权



[CTF-Web实验](#) 同时被 2 个专栏收录

9 篇文章 0 订阅

订阅专栏

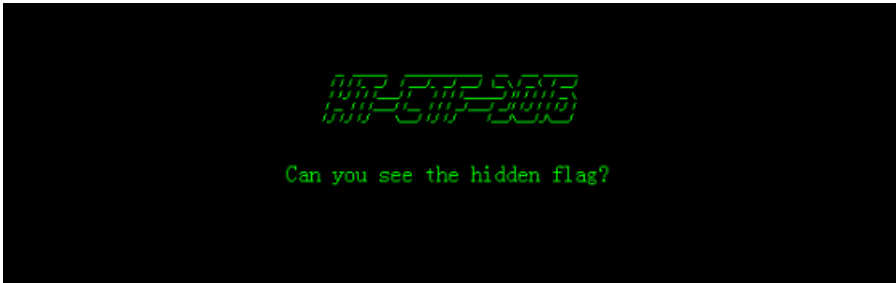


[CTF-Web实验](#)

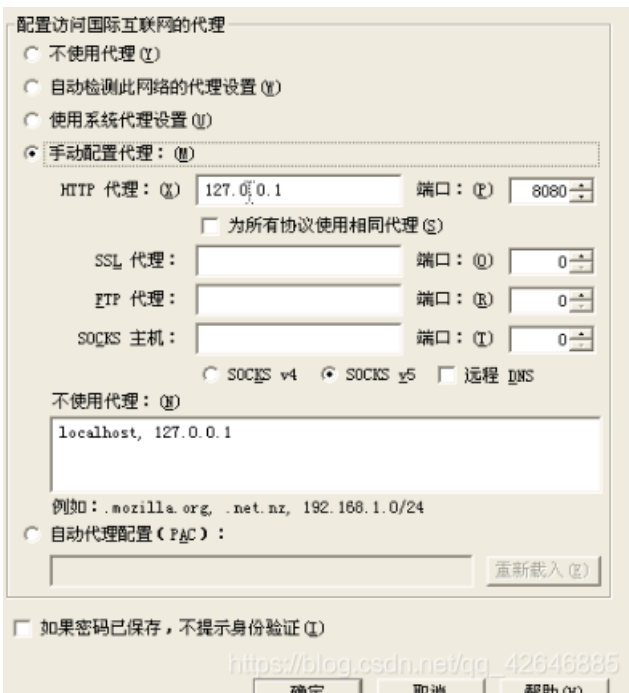
4 篇文章 0 订阅

订阅专栏

打开网址, 看到如下页面。

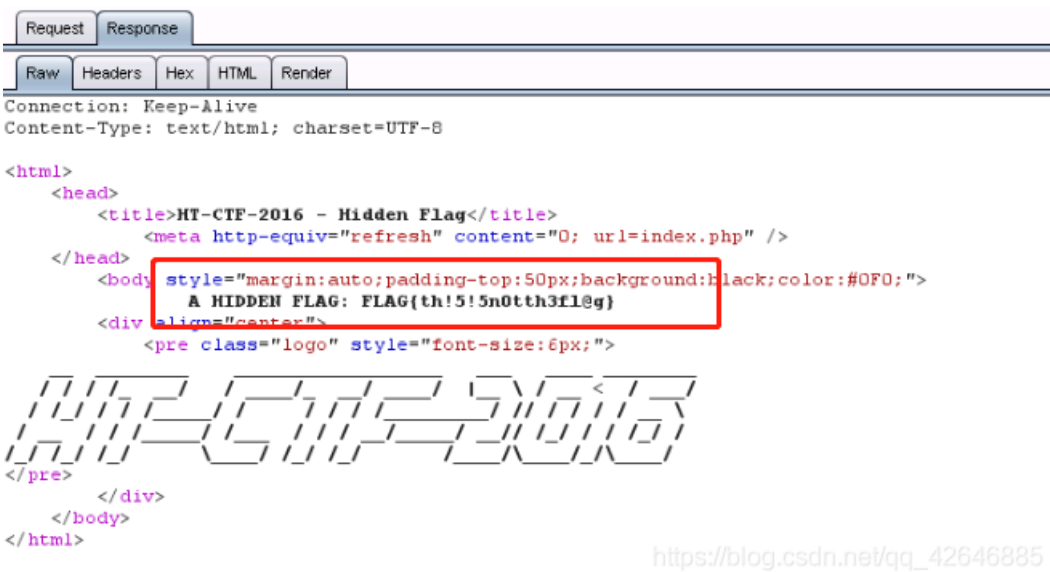


先查看源代码, 发现页面还有一个表格和一个链接。



点击确定后，打开burpsuite,在Proxy-Intercept-点击Intercept on。

在浏览器访问10.1.1.219:20111/Index.php，再查看History，打开详细看到flag的信息。



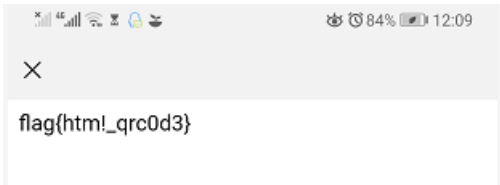
除此之外，开始的时候检查中间table有什么东西，找到控制table颜色的样改为白色：



看到table变成了一个二维码。



用微信扫描二维码后出现Key。



不过这个flag是个幌子。。。

实验总结：该实验比较简单，主要是要会使用burpsuite抓包。

burpsuit使用参考：[工具 | Burpsuite简介及使用](#)