XCTF攻防世界练习区-web题-backup

原创

不愿透露姓名的菜鸟 于 2019-09-19 17:01:31 发布 416 收藏
分类专栏： CTF

本文链接：https://blog.csdn.net/Homewm/article/details/101027414

0x05.cookie

【题目描述】

X老师告诉小宁他在cookie里放了些东西，小宁疑惑地想：‘这是夹心饼干的意思吗？

【目标】

掌握有关cookie的知识。

Cookie是当主机访问Web服务器时，是由Web服务器创建的，将信息存储在用户计算机上的文件。一般网络用户习惯用其复数形式 Cookies，指某些网站为了辨别用户身份、进行Session 跟踪而存储在用户本地终端上的数据，而这些数据通常会经过加密处理。

cookie就是服务端为了让用户不在每次访问需要登录的页面都要登录一次，而生成的一种证明身份的数据。服务器可以设置或读取Cookies中包含信息，借此维护用户跟服务器会话中的状态。cookie中常常包含了一些敏感消息：用户名、计算机名、使用的浏览器和曾经访问的网站等，当得到没有过期的cookie时就能绕过登录甚至做更多的事。

【解题思路】

思路一：

你知道什么是cookie吗？

（1）简单的构造链接：http://111.198.29.45:34019/cookie.php

（2） 查看页面元素-网络 找到消息头中的flag。在查看消息头中cookie的时候就会留意到flag内容。

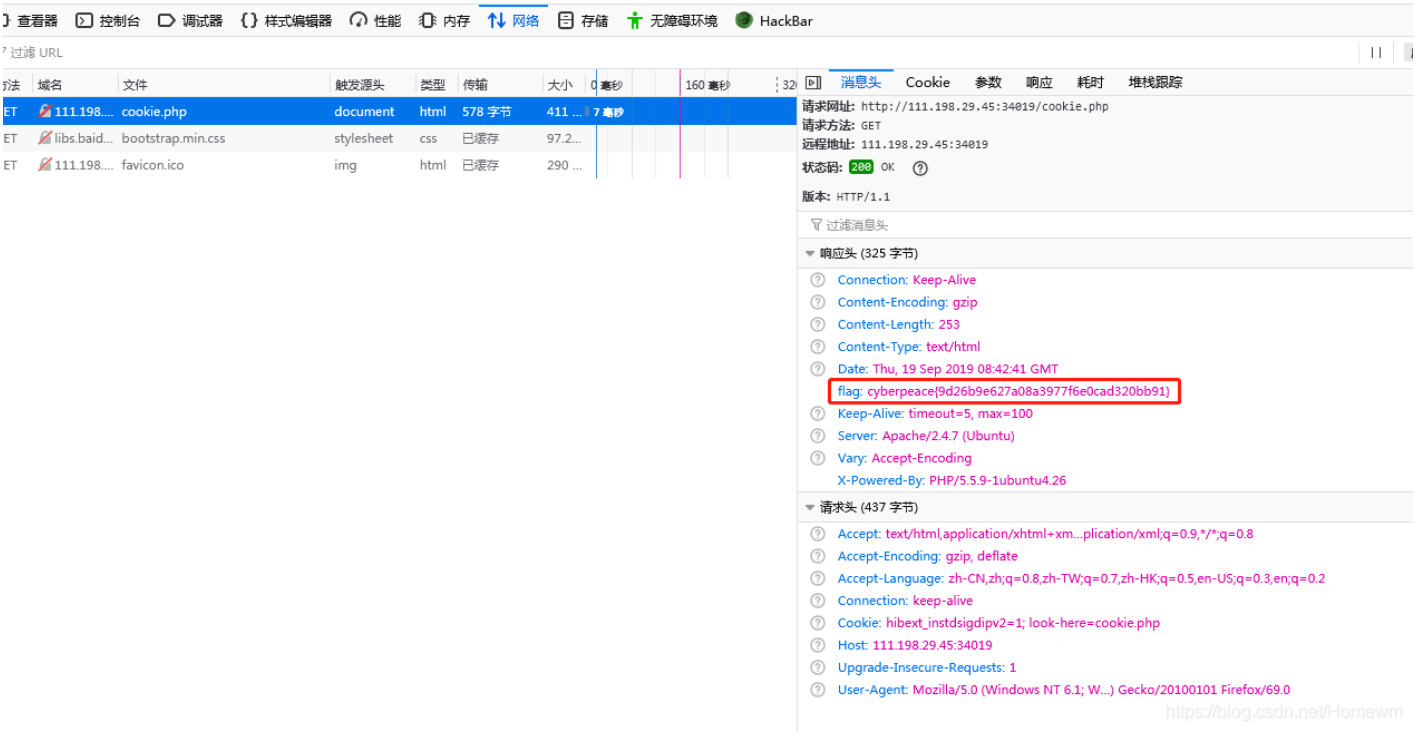
思路二：

第二步使用Chrome安装了Live HTTP Headers插件查看http header消息。能直接看到flag信息。

思路三：

使用burpsuite抓包和重放，就能直接得到flag。详细信息参考https://blog.csdn.net/God_XiangYu/article/details/100612961

See the http response



参考链接：

https://blog.csdn.net/God_XiangYu/article/details/100612961

再次让我很佩服上述链接的这位同学，writeup写的真的是太详细和方法真的是太多了，还有总结，真的很值得关注。