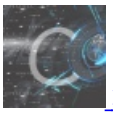
攻防世界-Web篇

原创

写代码的猿 于 2020-11-09 22:36:59 发布 194 收藏

分类专栏： 攻防世界总结 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_43454872/article/details/109587328



攻防世界-Web新手篇

1.题目描述 cookie

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？

2.题目场景

http://220.249.52.133:37857

3.WriteUp解题思路

cookie通俗的讲是类型为“小型文本文件”，是某些网站为了辨别用户身份，进行Session跟踪而储存在用户本地终端上的数据（通常经过加密），由用户客户端计算机暂时或永久保存的信息 。

方法一:

根据题目的提示可知：首先按F12，查看源代码，在存储中找到cookie的Values发现values中有一个cookie.php，所以访问http://220.249.52.133:37857/cookie.php的值，发现页面的提示信息为：See the http response（查看http响应),所以查看NetWork(网络)查看消息头：

```
Keep-Alive
Content-Encoding
 gzip
Content-Length
 253
Content-Type
 text/html
Date
 Mon, 09 Nov 2020 13:59:49 GMT
flag:cyberpeace{5d1fe9f081aa84c92a4691cd384e27a9}

Keep-Alive
 timeout=5, max=100
Server
 Apache/2.4.7 (Ubuntu)
Vary
 Accept-Encoding
X-Powered-By
 PHP/5.5.9-1ubuntu4.26
```

这样就得到了flag

方法二：

利用Burp Suite进行网络抓包。