hackme的web部分水题writeup集合

原创

cggwz 于 2020-10-31 10:07:31 发布 161 收藏

分类专栏： CTF hackme题解 文章标签： hackme writeup 抓包 aaencode js

本文链接：https://blog.csdn.net/cggwz/article/details/109398286

简单介绍，hackme是提供ctf基础题的一个很好的网站，网站链接如下：

网站链接

这次把web部分的头几个没什么值得说的题说一下，因为太短了，单独发一篇博客不值得。

hide and seek

几乎每个平台都有这道题，直接右击查看源代码即可看到flag。目的就是教会我们查看网页源代码。应平台要求，flag就不提供了。

scoreboard

网页源代码里是没有的，也没有很多的提示，那么只能说flag在服务器端或者在数据包里，起码不在客户端。scoreboard页面可以和服务器端沟通的只有登录按钮和提交flag的按钮。我们先尝试抓包，建议使用burp suite，非常好用。wireshark也可以完成这一题，不过做后面的题可能不太方便，主要是wireshark不能发包。开始抓包就可以做各种尝试，关闭浏览器重新打开页面（因为浏览器有缓存，如果不关闭不会发新的内容），登录退出，在提交flag框内随便提交一串字符串。最后在提交字符串的响应包的头部发现flag。

这道题主要是教我们抓包以及告诉我们包的头部可能会包含信息。

homepage

提示比较明显，问我们有没有检查代码。所以我们就在网页源代码里寻找js代码，可以发现code.js，点开发现是一堆颜表情，这就是aaencode，直接google，有很多解码的网页，解码后得到一段代码，然后直接运行，浏览器按F12可以打开调试器，然后运行，可以得到一个二维码，用手机扫一下就可以得到flag。

这道题主要是让我们了解aaencode，以及js代码的调试。

总结

这三道题，不仅入门，而且并没有什么过多的步骤，所以放在一起。