【墨者学院writeup】浏览器信息伪造之User-Agent及NetType微信网络检测破解

原创

iqiqiya 于 2018-05-21 19:13:29 发布 3866 收藏 3
分类专栏： 我的CTF之路 杂七杂八经验 ------墨者学院CTF 我的CTF进阶之路 文章标签： 墨者学院writeup 浏览器信息伪造 浏览器信息伪造writeup NetType微信网络检测
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/xiangshangbashaonian/article/details/80396328
版权


我的CTF之路 同时被 3 个专栏收录
92 篇文章 5 订阅
订阅专栏


杂七杂八经验
122 篇文章 1 订阅
订阅专栏


------墨者学院CTF
3 篇文章 0 订阅
订阅专栏

题目地址：

http://219.153.49.228:48756/

题目介绍：

用到的知识：

User-Agent（用户代理）字符串是Web浏览器用于声明自身型号版本并随HTTP请求发送给Web服务器的字符串，在Web服务器上可以获取到该字符串。

从微信6.0开始，其内嵌的浏览器在UserAgent字符串中增加了NetType字段用于标识客户端（手机）当前的网络环境，经测试，该字段至少有以下3个取值：

NetType/WIFI

NetType/2G

NetType/3G+

分别对应于Wifi、2G、3G以上网络环境。因此，Web服务器可以据此识别客户端网络环境并提供有针对性的内容。

附测试数据：

iPhone 5 / iOS 8.0 / Wifi

Mozilla/5.0 (iPhone; CPU iPhone OS 8_0 likeMac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12A365MicroMessenger/6.0 NetType/WIFI

iPhone 5 / iOS 8.0 / 2G

Mozilla/5.0 (iPhone; CPU iPhone OS 8_0 like Mac OS X)AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12A365 MicroMessenger/6.0NetType/2G

iPhone 5 / iOS 8.0 / 3G

Mozilla/5.0 (iPhone; CPU iPhone OS 8_0 likeMac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12A365 MicroMessenger/6.0NetType/3G+

解题思路：

我们只需用下边这段User-Agent替换burpsuit抓到的重新发包即可得到KEY值

0x001：

打开burpsuite并设置浏览器代理127.0.0.1:8080>>浏览器先访问http://219.153.49.228:48756/

0x002：

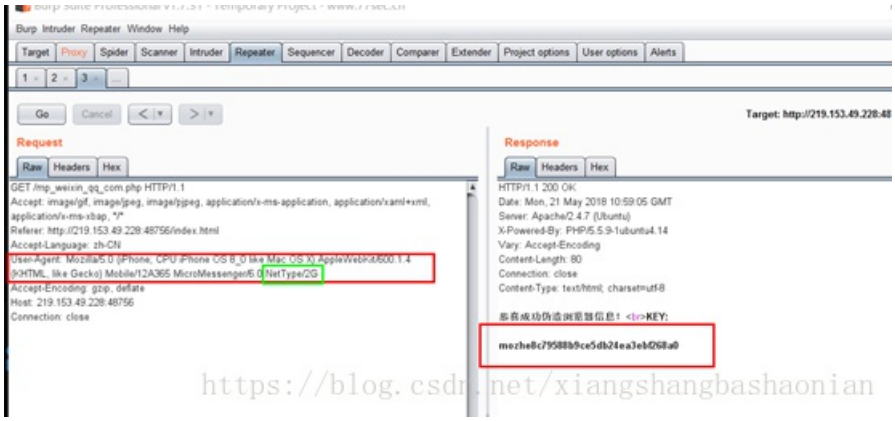
在点击下方微信图文也就是这个链接http://219.153.49.228:43656/mp_weixin_qq_com.php进行拦截包-->右键发送给repeater伪造

0x003：

将user-agent修改为下方的User-Agent 点击GO即可

---------- ---我是分割线----------

User-Agent: Mozilla/5.0 (iPhone; CPU iPhoneOS 8_0 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12A365MicroMessenger/6.0 NetType/2G



恭喜成功伪造浏览器信息！
KEY:

mozhe8c79588b9ce5db24ea3ebf268a0

参考资料：https://blog.csdn.net/lilin_emcc/article/details/40145113

tips:利用火狐插件Default User Agent也可以

创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖