GKCTF web-老八小超市儿 解题思路writeup

原创

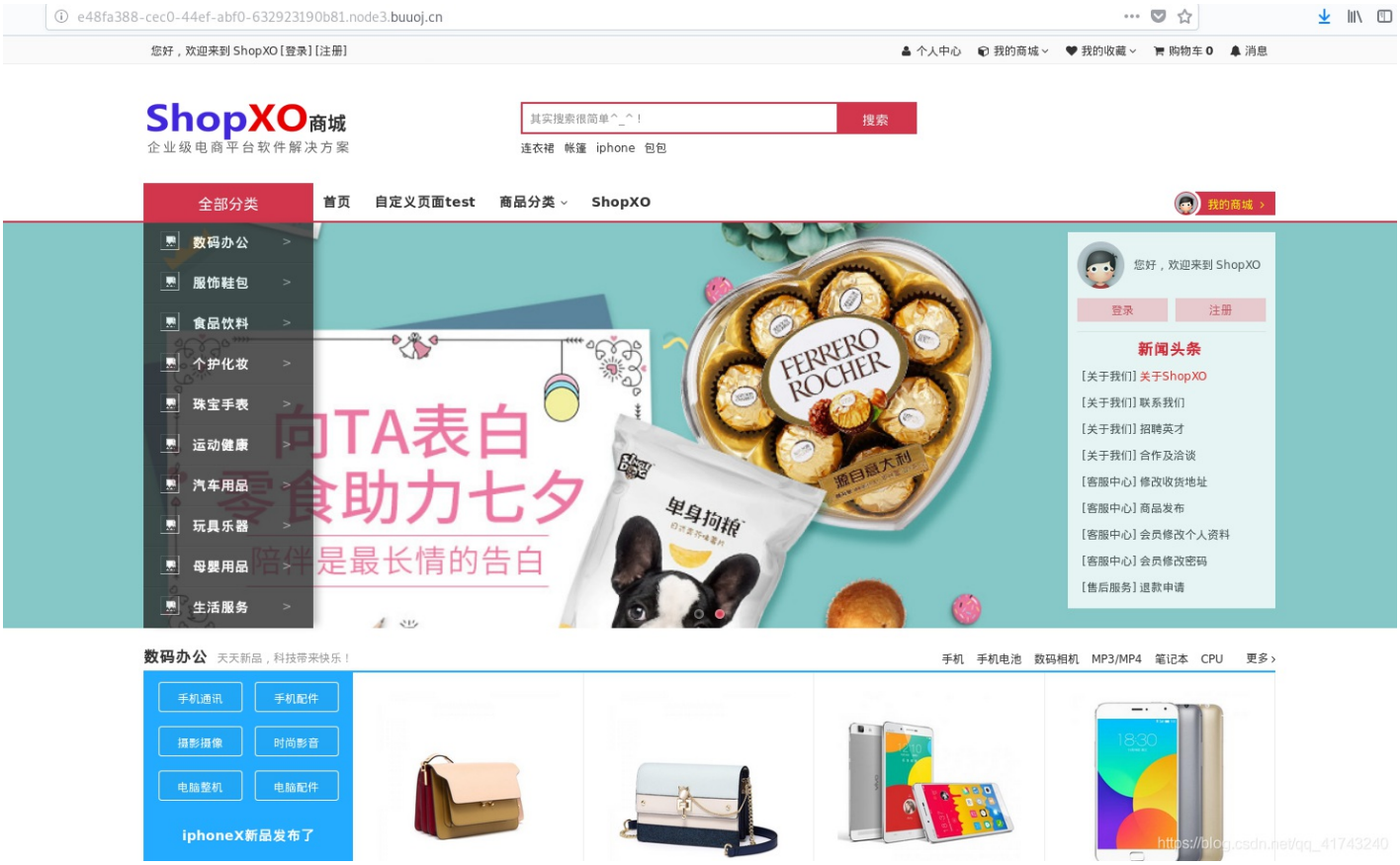
0kaml 于 2020-05-24 23:10:48 发布 933 收藏 1
分类专栏： CTF WEB 文章标签： 信息安全

本文链接：https://blog.csdn.net/qq_41743240/article/details/106320735

CTF 同时被 2 个专栏收录
12 篇文章 0 订阅
订阅专栏

WEB
4 篇文章 0 订阅
订阅专栏

打开题目



一看就知道是个CMS,我们试着搜索一下ShopXO企业级免费开源商城系统的漏洞,可以知道一个后台的文件上传漏洞

利用方法链接

http://www.nctry.com/1660.html

之后查看flag,会发现是假的,但从中可以知道真实flag在root目录下,访问root目录没有权限

查看根目录的flag.hint可以知道一个线索:

Sun May 24 07:51:26 2020 Get The RooT,The Date Is Useful!

然后查看根目录的auto.sh可以知道一个线索,每60秒会调用一个makeflaghint.py文件重新生成flag.hint,所以auto.sh调用makeflaghint.py是root权限,我们可以直接修改makeflaghint.py的内容执行cat /root/flag获取flag