

# GKCTF web-老八小超市儿 解题思路writeup

原创

Okaml 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](#)

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/qq\\_41743240/article/details/106320735](https://blog.csdn.net/qq_41743240/article/details/106320735)

版权



[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

您好, 欢迎来到 ShopXO [登录] [注册]

个人中心 我的商城 我的收藏 购物车 消息

ShopXO 商城  
企业级电商平台软件解决方案

其实搜索很简单^\_^!

连衣裙 帐篷 iphone 包包

全部分类 首页 自定义页面test 商品分类 ShopXO 我的商城

您好, 欢迎来到 ShopXO

登录 注册

新闻头条

- [关于我们] 关于ShopXO
- [关于我们] 联系我们
- [关于我们] 招聘英才
- [关于我们] 合作及洽谈
- [客服中心] 修改收货地址
- [客服中心] 商品发布
- [客服中心] 会员修改个人资料
- [客服中心] 会员修改密码
- [售后服务] 退款申请

数码办公 天天新品, 科技带来快乐!

手机 手机电池 数码相机 MP3/MP4 笔记本 CPU 更多

手机通讯 手机配件 摄影摄像 时尚影音 电脑整机 电脑配件

iphoneX新品发布了

单身狗粮

向TA表白 零食助力七夕 陪伴是最长情的告白

https://blog.csdn.net/qq\_41743240

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