

攻防世界WEB进阶之Cat

原创

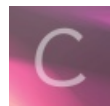
置顶 [harry_c](#) 于 2019-08-05 13:12:59 发布 6266 收藏 5

分类专栏: [攻防世界](#) 文章标签: [攻防世界](#) [web进阶](#) [cat](#) [安全](#) [渗透](#)

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/harry_c/article/details/98482494

版权



[攻防世界](#) 专栏收录该内容

29 篇文章 2 订阅

订阅专栏

攻防世界WEB进阶之Cat

第一步: 分析

第二步: 实操

第三步: 答案

第一步: 分析

难度系数: 2星

题目来源: XCTF 4th-WHCTF-2017

题目描述: 抓住那只猫

首先题给出的信息抓住那只猫, 没有任何提示性, 题目来源为XCTF, 点击场景, 打开为一个输入页面:

提示输入域名, 测试题给的域名loli.club, 无任何响应, 但是查询的内容出现在搜索框中为get请求, 再测试127.0.0.1, 巧了, 返回对应的ping值, 说明这是一个功能框, 输入对应的ip会ping到对应连接情况。

第二步: 实操

尝试执行命令, 127.0.0.1&&dir、127.0.0.1&&ls、127.0.0.1|ls均被屏蔽, 所以无法入手, 至此, 没有收获到任何东西, 唯一收获到的是网站使用的是url编码能够传入。随便输入不同的url编码值, 编码在我之前的一篇博文中有提

供: https://blog.csdn.net/harry_c/article/details/97913194

当输入边界值%80时系统产生报错, 看到报错心中窃喜, 是否为突破口。

通过对报错信息的仔细查找, 似乎找到了网站的绝对地址, 窃喜使用地址访问未果, 百度找到方法应该要加@输入 @/opt/api/dnsapi/views.py果然再一次出现了报错信息, 想必距离答案越来越近了, 在查找cat、database、XCTF等关键词, 哈哈找到关于database的内容:

继续查询url=@/opt/api/database.sqlite3

第三步: 答案

继续搜索关键词找到类似于flag的形式

经过数次尝试最终锁定答案。

至此最终flag为: WHCTF{yooooo_Such_A_G00D_@}