****SQL注入****

**SQL注入基本介绍**  
不管用什么语言编写的Web应用，它们都用一个共同点，具有交互性并且多数是数据库驱动。在网络中，数据库驱动的Web应用随处可见，由此而存在的SQL注入是影响企业运营且最具破坏性的漏洞之一  
结构化查询语言（Structured Query Language，缩写：SQL），是一种特殊的编程语言，用于数据库中的标准数据查询语言。SQL 是一门 ANSI 的标准计算机语言，用来访问和操作[数据库系统](http://www.ichunqiu.com/courses/277" \t "https://bbs.ichunqiu.com/_blank)。SQL 语句用于取回和更新数据库中的数据。SQL 可与数据库程序协同工作，比如 MS Access、DB2、Informix、MS SQL Server、Oracle、Sybase 以及其他数据库系统。SQL注入（SQL Injection）是一种常见的[WEB安全漏洞](http://www.ichunqiu.com/course/475?bbs" \t "https://www.cnblogs.com/ichunqiu/p/_blank)，攻击者利用这个问题，可以访问或修改数据，或者利用潜在的数据库漏洞进行攻击。是一种通过操作输入来修改后台SQL语句达到代码执行进行攻击目的的技术。  
  
**SQL注入产生原因**  
构造动态字符串是一种编程技术，它允许开发人员在运行过程中动态构造SQL语句。开发人员可以使用动态SQL来创建通用、灵活的应用。动态SQL语句是在执行过程中构造的，它根据不同的条件产生不同的SQL语句。当开发人员在运行过程中需要根据不同的查询标准来决定提取什么字段(如SELECT语句)，或者根据不同的条件来选择不同的查询表时，动态构造SQL语句会非常有用。  
针对SQL注入的攻击行为可描述为通过在用户可控参数中注入SQL语法，破坏原有SQL结构，达到编写程序时意料之外结果的攻击行为。其成因可以归结为以下两个原因叠加造成的：  
  
1. 程序编写者在处理应用程序和数据库交互时，使用字符串拼接的方式构造SQL语句  
2. 未对用户可控参数进行足够的过滤便将参数内容拼接进入到SQL语句中  
SQL注入攻击方式

SQL注入的攻击方式根据应用程序处理数据库返回内容的不同，可以分为可显注入、报错注入和盲注：1、可显注入：攻击者可以直接在当前界面内容中获取想要获得的内容  
  
2、报错注入：数据库查询返回结果并没有在页面中显示，但是应用程序将数据库报错信息打印到了页面中，所以攻击者可以构造数据库报错语句，从报错信息中获取想要获得的内容  
  
3、盲注：数据库查询结果无法从直观页面中获取，攻击者通过使用数据库逻辑或使数据库库执行延时等方法获取想要获得的内容

**如何进行SQL注入攻击**

**编写注入点**

1.使用if语句来先判断一下变量是否初始化

<?php

if(isset($\_GET["ichunqiu"])){

}

?>

2.连接数据库。通过 mysql\_connect() 函数完成

mysql\_connect(servername,username,password);

servername       规定要连接的服务器。默认是"localhost:3306"。

username        规定登录所使用的用户名。默认值是拥有服务器进程的用户的名称。

password        规定登录所用的密码。默认是 ""。

3.选择一个数据库

mysql\_select\_db(database,connection)

database        必需。规定要选择的数据库。

connection        规定 MySQL 连接。如果未指定，则使用上一个连接。

4.执行MySQL 查询

mysql\_query(query,connection)

query        必需。规定要发送的 SQL 查询。

connection        规定 SQL 连接标识符。如果未规定，则使用上一个打开的连接。

5.对结果进行处理

mysql\_fetch\_array(data,array\_type)

data        可选。规定要使用的数据指针。该数据指针是 mysql\_query() 函数产生的结果。

array\_type

可选。规定返回哪种结果。可能的值：

MYSQL\_ASSOC - 关联数组

MYSQL\_NUM - 数字数组

MYSQL\_BOTH - 默认。同时产生关联和数字数组

创建数据库，创建表，创建列，插入数据。

**寻找及确认SQL注入**

**1、推理测试法**  
寻找SQL注入漏洞有一种很简单的方法，就是通过发送特殊的数据来触发异常。  
首先需要了解数据是通过什么方式进行输入

1.1 GET请求：该请求在URL中发送参数。

1.2 POST请求：数据被包含在请求体中。

1.3 其他注入型数据：HTTP请求的其他内容也可能会触发SQL注入漏洞。

2、数据库错误（以MySQL为例）

在参数后面加个单引号 select \* from users where id = 1'

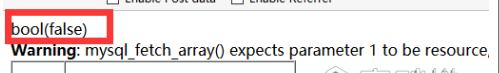


执行失败，所以mysql\_query()函数会返回一个布尔值，在下行代码中mysql\_fetch\_array($sql)将执行失败，并且PHP会显示一条警告信息，表明mysql\_fetch\_array()的第一个参数必须是个资源，而代码在实际运行中，给出的参数值却是一个布尔值。

$sql = mysql\_query($querry,$con);下一行加上

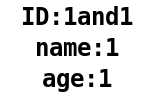
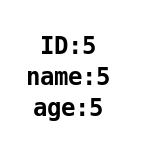
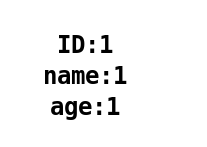
var\_dump($sql);

结果：



1. **and大法和or大法**  
   页面不返回任何错误信息，可以借助本方法来推断了，首先在参数后面加上 and 1=1和and 1=2看有什么不同，当and 1=1 返回了数据，而and 1=2没有，这证明1=1是一个为真的条件，前面的结果是true，true and true 所以没有任何问题，第二个 1=2 是个假条件， true and false还是false，所以并没有数据返回。

or就是或者，两个都为假，才会为假。就像在靶机实验时，把id改为1、2、3、4、5，都有返回，当id=6时是没有数据的。



3、加法和减法  
3.1需要区分一下数字型和字符串型：

3.2数字型：不需要使用单引号来表示

3.3其他类型：使用单引号来表示

综合上述，可以发现的例子是数字型的，这样就可以使用加法和减法来判断了。  
加法，在参数输入1+1，看看返回的数据是不是id等于2的结果，这里注意一下+号在SQL语句是有特效含义的，所以要对其进行url编码，最后也就是%2b。

**利用SQL注入**

要想发动[sql注入攻击](http://www.ichunqiu.com/courses/277" \t "https://bbs.ichunqiu.com/_blank)，就要知道正在使用的系统数据库，不然就没法提取重要的数据。  
首先从Web应用技术上就给提供了判断的线索：

ASP和.NET：Microsoft SQL Server

PHP：MySQL、PostgreSQL

Java：Oracle、MySQL  
Web容器也给提供了线索，比如安装IIS作为服务器平台，后台数据及很有可能是Microsoft SQL Server，而允许Apache和PHP的Linux服务器就很有可能使用开源的数据库，比如MySQL和PostgreSQL。  
**基于错误识别数据库**  
大多数情况下，要了解后台是什么数据库，只需要看一条详细的错误信息即可。比如判断事例中使用的数据库，加个单引号。

error:You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1

上面错误信息可以发现是Microsoft SQL Server，如果错误信息开头是ORA，就可以判断数据库是Oracle

**基于数字函数推断**

|  |  |
| --- | --- |
| 数据库服务器 | 函数 |
| Microsoft SQL Server | @@pack\_received、@@rowcount |
| MySQL | connection\_id()、last\_insert\_id()、row\_count() |
| Oracle | BITAND(1,1) |
| PostgreSQL | select EXTRACT(DOW FROM NOW()) |

connection\_id()不管它值多少，基本上都是正的，也就是为真，这里不存在insert语句，默认情况就是返回零，也就是假。  
那么如果and connection\_id()数据返回正常，and last\_insert\_id()不返回数据，就可以推断这是一个MySQL数据库了。

**UINON语句提取数据**  
UNION操作符可以合并两条或多条SELECT语句的查询结果，基本语法如下：

select column-1 column-2 from table-1

UNION

select column-1 column-2 from table-2

如果应用程序返回了第一条查询得到的数据，我们就可以在第一条查询后面注入一个UNION运算符来添加一个任意查询，来提取数据，当然在使用UNION之前必须要满足两个条件：

* 两个查询返回的列数必须相同
* 两个查询语句对于列返回的数据类型必须相同

第一个条件，可以使用NULL来尝试，由于NULL值会被转换成任何数据类型，所以不用管第二个条件。就是这样的一个个加上去进行尝试，直到不返回错误

而在靶机实验第1到第3时，我们就用到了UINON语句提取数据：IMG_256

**ORDER BY子句**

可以是用order by子句得到准确列数，使用order by子句可以帮助我们快速得到列数。

**枚举数据库**

枚举数据库并提取数据遵循一种层次化的方法，首先我们提取数据库名称，然后提取表，再到列，最后才是数据本身。要想获取远程数据库的表、列，就要访问专门保存描述各种数据库结构的表。通常将这些结构描述信息成为元数据。以MySQL为例，这些表都保存在information\_schema数据库中。