PKAV-EDU

《SQL注入基础·基础篇1》

SQL
注入
系列

BY
Verkey

从一个故事开始

- 从前，有一盏神奇的灯，叫阿拉丁神灯。这盏神灯历经几千年，孕育出了一个神灯精灵，名叫神灯士。这个神灯精灵诞生不久，灵智还不高，但是他可以用咒语操控神灯，让神灯变出各种各样的东西。
- 有一天，一只黑狐狸找到了神灯精灵，想让神灯精灵满足他一个愿望。神灯精灵很爽快的答应了。神灯精灵对狐狸说，你想要什么，只要你说出名字，我就念咒把它变出来。大家都知道，在童话故事里，狐狸一般都是很狡猾的。所以狐狸想了想，说：“衣服汽车城堡”。神灯精灵听完后，对着神灯念咒语：“吧啦吧啦，衣服汽车城堡”。神灯震了震，冒出一阵烟，但是什么都没出现。神灯士说：“神灯里面没有衣服汽车城堡”这样东西，所以你的愿望也没实现，你可以再说一样东西。
- 下面就请大家思考下，狐狸要怎么样说，才能实现衣服、汽车、城堡的愿望？

神灯士与狐狸的故事

Part1
- 数据库基础概念

Part2
- SQL注入漏洞的形成

Part3
- SQL注入在渗透测试过程中的作用

Part4
- 常见的SQL注入过程

主要内容

数据(Data) 图像、语音、文字等

- 在计算机系统中，各种字母、数字符号的组合、语音、图形、图像等统称为数据。

数据库(Database) Access、MSSQL、Oracle、SQLITE、MySQL等

- 数据库是按照数据结构来组织、存储和管理数据的“仓库”。

数据库管理系统(DBMS) Access、MSSQL、Oracle、SQLITE、MySQL等

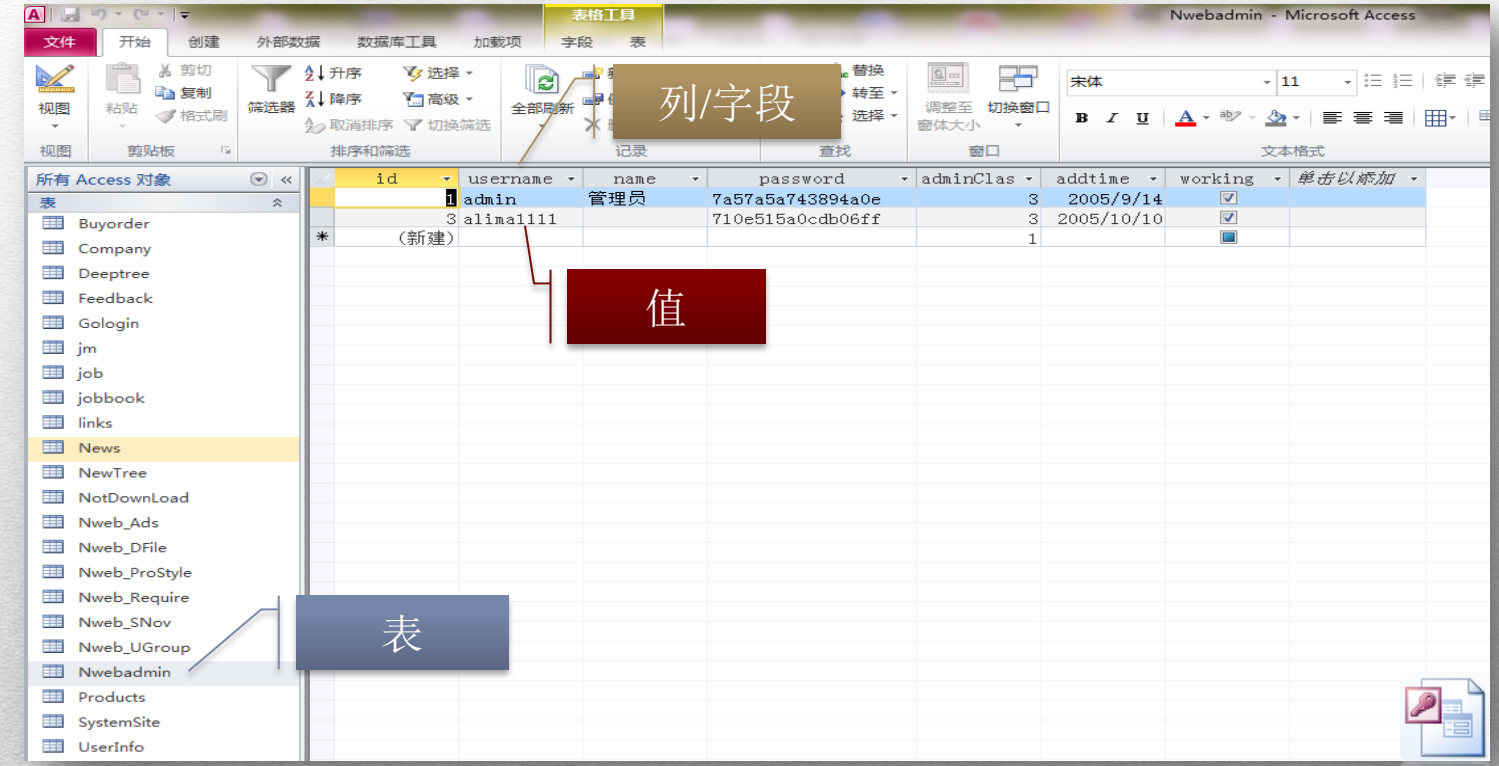
- 数据库管理系统(database management system)是一种操纵和管理数据库的软件，用于建立、使用和维护数据库。它对数据库进行统一的管理和控制，以保证数据库的安全性和完整性。

结构化查询语言(SQL) DQL、DDL、DML、TCL、DCL

- 结构化查询语言(Structured Query Language)简称SQL，结构化查询语言是一种数据库查询和程序设计语言，用于存取数据以及查询、更新和管理关系数据库系统。

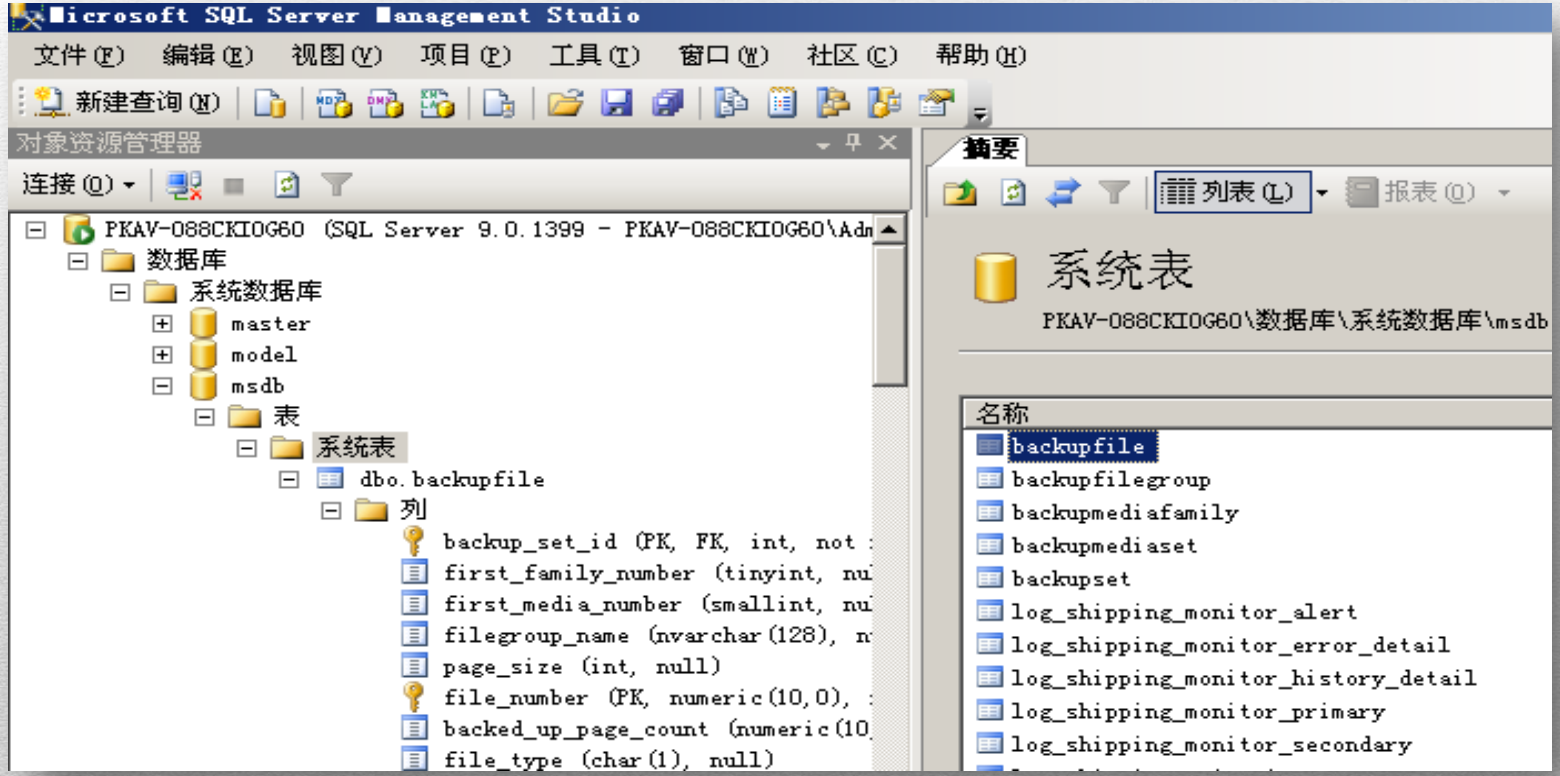
数据库基础概念

- 这是一个Access数据库



一个简单的Acess数据库示例

- 这是一个SQL Server 2005的数据库：



SQL Server数据库示例

- 静态网页：

  html或者htm，是一种静态的页面格式，不需要服务器解析其中的脚本。由浏览器如(IE、Chrome等)解析。

  1.不依赖数据库

  2.灵活性差，制作、更新、维护麻烦

  3.交互性交差，在功能方面有较大的限制

  4.安全，不存在SQL注入漏洞

- 动态网页：

  asp、aspx、php、jsp等，由相应的脚本引擎来解释执行，根据指令生成静态网页。

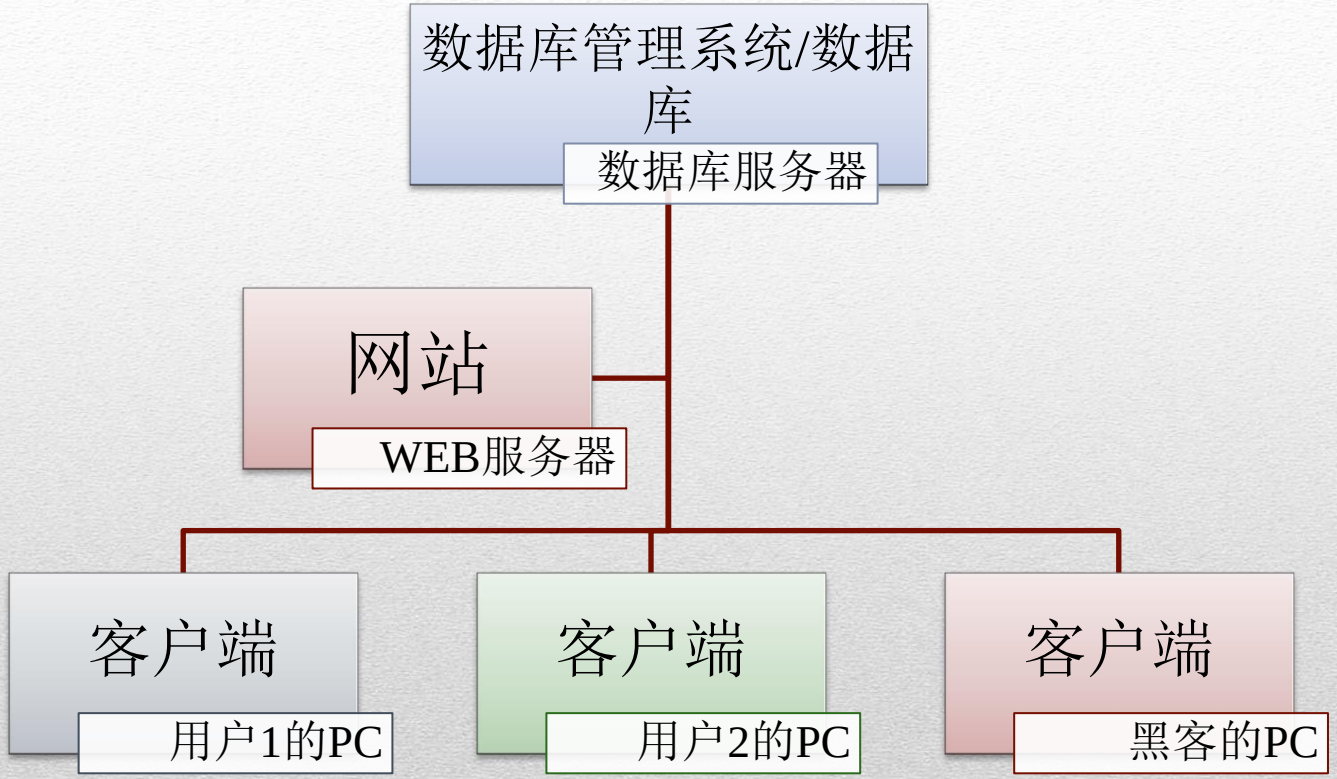
  1.依赖数据库

  2.灵活性好，维护简便

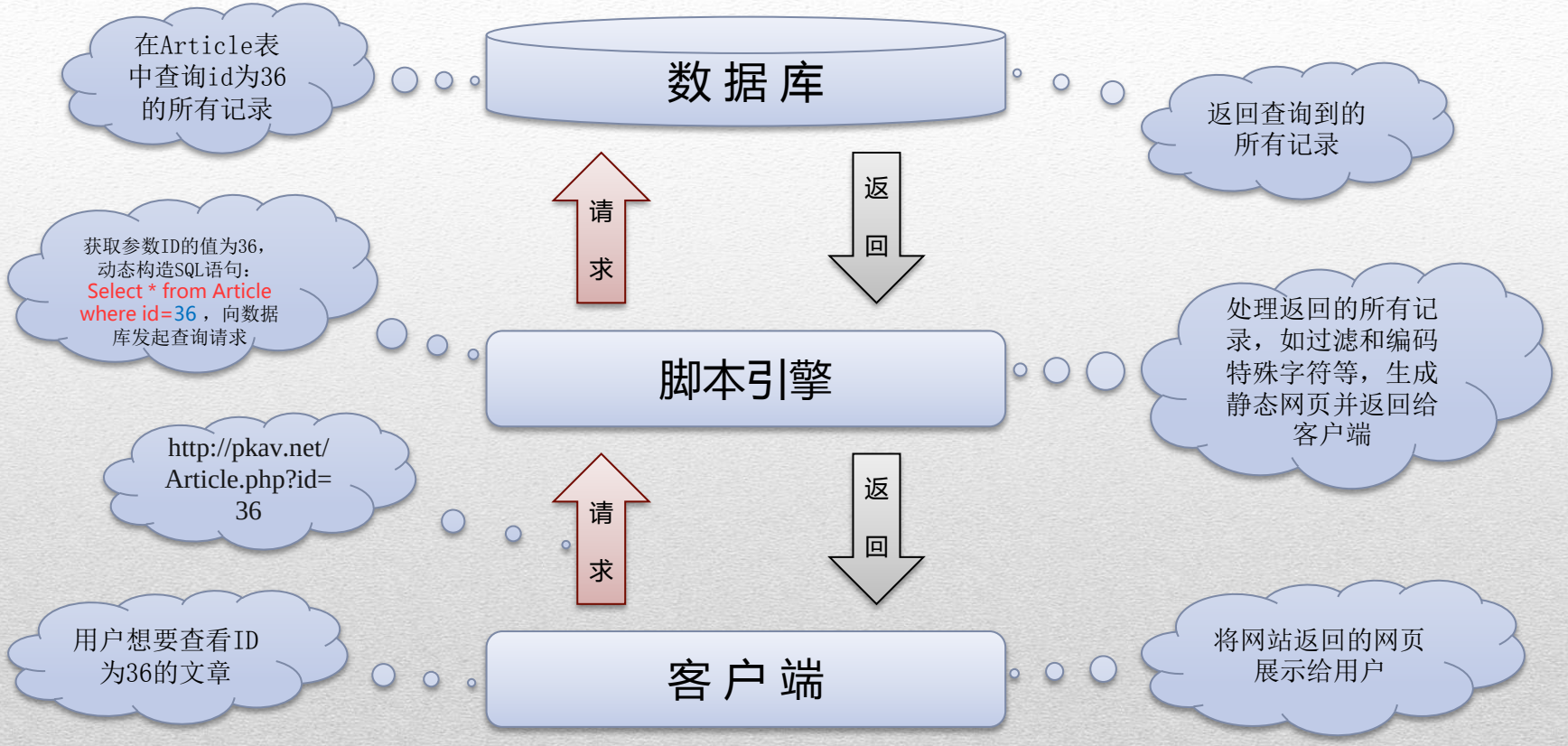
  3.交互性好，功能强大

  4.存在安全风险，可能存在SQL注入漏洞

为什么要使用数据库？


数据库管理系统/数据库
数据库服务器
网站
WEB服务器
客户端
用户1的PC
客户端
用户2的PC
客户端
黑客的PC

一个简单的拓扑图



SQL注入漏洞是怎么样形成的？

- 示例演示:

http://localhost/example/sqli/Article.php?id=2&type=1

- 思考提问:

SQL注入漏洞的成因是什么?

- SQL注入漏洞的成因:

数据与代码未严格分离；用户提交的参数数据未做充分检查过滤即被代入到SQL命令中，改变了原有SQL命令的“语义”，且成功被数据库执行。

实例讲解-SQL注入漏洞是怎么样形成的？

- SQL注入的定义:

很多应用程序都使用数据库来存储信息。SQL命令就是前端应用程序和后端数据库之间的接口。攻击者可利用应用程序根据提交的数据动态生成SQL命令的特性，在URL、表单域，或者其他的输入域中输入自己的SQL命令，改变SQL命令的操作，将被修改的SQL命令注入到后端数据库引擎执行。

- SQL注入的危害:

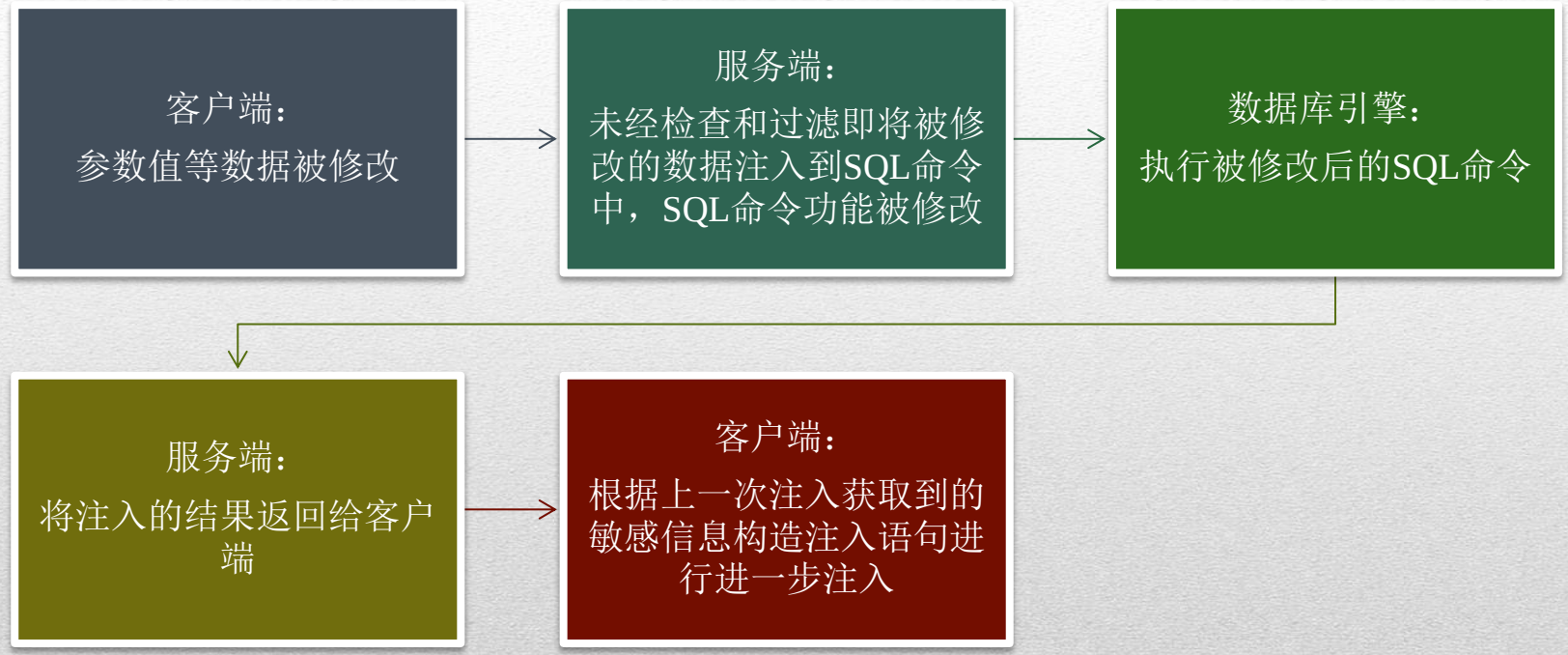
这些危害包括但不局限于：

A. 数据库信息泄漏：数据库中存放的用户的隐私信息的泄露。
B. 网页篡改：通过操作数据库对特定网页进行篡改。
C. 网站被挂马，传播恶意软件：修改数据库一些字段的值，嵌入网马链接，进行挂马攻击。
D. 数据库被恶意操作：数据库服务器被攻击，数据库的系统管理员帐户被窜改。
E. 服务器被远程控制，被安装后门。经由数据库服务器提供的操作系统支持，让黑客得以修改或控制操作系统。
F. 破坏硬盘数据，瘫痪全系统。

一些类型的数据库系统能够让SQL指令操作文件系统，这使得SQL注入的危害被进一步放大。

- 绕过登录验证：使用万能密码登录网站后台等。
- 获取敏感数据：获取网站管理员帐号、密码等。
- 文件系统操作：列目录，读取、写入文件等。
- 注册表操作：读取、写入、删除注册表等。
- 执行系统命令：远程执行命令。

SQL注入在渗透测试过程中的作用


客户端：
参数值等数据被修改
服务端：
未经检查和过滤即将被修改的数据注入到SQL命令中，SQL命令功能被修改
数据库引擎：
执行被修改后的SQL命令
服务端：
将注入的结果返回给客户端
客户端：
根据上一次注入获取到的敏感信息构造注入语句进行进一步注入

常见的SQL注入过程

多问多想多做

THANKS~ ☺

“Update 工资 Set Money=Money *”. $_GET[‘努力’];

PKAV-EDU