# 简介

应用程序在向后台数据库传递SQL（Structured Query Language，结构化查询语句）查询时，如果为攻击者提供了影响该查询的能力，就会引发SQL注入。

一个正常的PHP数据查询语句：

$conn = mysql\_connection($host, $username, $password)

$query = “select \* from users where user=’admin’ and passwd=’”

$query = $query.$\_GET[“passwd”].”’”；

$result = mysql\_query($query);

这里查询语句中的passwd是根据用户输入设定的，没有做任何的限定，攻击者可以利用这个修改查询语句。

# 分类

## SQL注入点

字符型

整数型

搜索型：like ‘’

## SQL注入攻击

没有正确的过滤转义字符

错误的类型处理：比如要求传入整数型，最终传入字符型

数据库服务器中的漏洞

SQL盲注：错误没有回显

条件响应：1=1 AND 1=2

条件性差错（select 1/0 from t1 where id=0;）

时间延迟

# 原理

正常的 SQL 语句：

select \* from users where id = 1;//正常情况不会把id写死，而是根据外部传入

动态的构造过程：

$query = "select \* from users where user='admin' and passwd='"

$query = $query.$\_GET["passwd"]."'";

利用动态构造构造注入语句：

不传入id数字，而是传入字符等非法字符

# 测试

简单的规则：发送以外数据来触发异常

识别Web应用的数据输入：

select \* from users where id =1 and 1=1; //TRUE and TRUE，返回正确结果

select \* from users where id =1 and 1=2;//TRUE and FALSE,返回空，SQL注入

了解哪种类型的请求会触发异常

检测服务器响应中的异常

# 利用与防御

## 不同数据库的SQL注入

### Access 的 SQL 注入

Access 注入猜解过程

猜解表名

猜解列名

猜解字段值长度

ASCII 逐字解码法猜解字段值

ASP+Access：

### MySQL 的 SQL 注入

### SQLServer 的 SQL 注入

有趣的出错信息

Group By 与 Having 查询

爆表名与字段名

爆数据记录

## 基于不同方法的条件语句的使用

### 基于时间

基于 Web 应用响应时间上的差异

基于时间（SQLServer）

有管理员访问权限

IF (system\_user = 'sa') WAITFOR DELAY '0:0:5' –-

IF (substring((select @@version), 25, 1) = 5) WARITFOR DELAY '0:5:15' –-

EXEC master..xp\_cmdshell 'ping -n 5 127.0.0.1'

有管理员访问权限，没有启动xp\_cmdshell,于 2005和 2008 版本

EXEC sp\_config 'show advanced options', 1;

GO

RECONFIGURE;EXEC sp\_configure 'xp\_cmdshell', 1;

2000版本

exec master..sp\_addextendedproc 'xp\_cmdshell', 'xplog70.dll'

基于时间（MySQL）

select benchmark(1000000),sha1('fooying'));

select sleep(5); (5.0.12 版本以上)

### 基于错误

根据指定位值的不同来触发不同的错误响应并提取位值

基于错误

/is\_srvrolemember('sysadmin')

/case when (system\_user = 'sa') then 1 else 0 end

### 基于内容

基于页面返回的不同 HTML 进行相关的判断

基于内容

%2B case when (system\_user = 'sa') then 1 else 0 end

//%2B相当于+

## 其他SQL注入利用手法

### 万能密码

'or'= 'or'

sql = "select \* from users when username='"& name & "'and passwd='"&password & "'"

sql = "select \* from users when username='' or'='or" and passwd='admin'

假 or 真 or 假 and 假=假 or 真 or （假 and假）=假or真or假=（假or真）or假=真or假=真

### 字符转换与编码的处理

Declare 与 OX6e 编码

二次编码

/\*\*/替换空格

Declare 与 OX6e 编码

16进制编码

0x6e6574207573657220666f6f79696e67202f616464

declare @a sysname

select @a=<16进制代码>

exec master .dbo.xp\_cmdshell @a

## SQL注入的防御

### 基础与二次过滤

输入检查

特殊符号过滤

白名单与黑名单

### 不同语言的 SQL 防御

使用参数化语句

特殊符号过滤

白名单与黑名单

Java

使用?占位符进行构造查询语句

JSF(Java Server Faces) 的 输入验证类 javax.faces.validator

.NET

@parameter(SqlClient)

:parameter(OracleClient)

?(OleDb/Odbc)

Regular-Expression Validator 控件

Custom Validator 控件

PHP

?占位符(mysqli,MySql)

Pg\_query\_params()(mysqli,PostgreSQL)

冒号字符与?占位符(PEAR:MDB2)

冒号字符与?占位符(PDO)

Preg\_match 使用正则表达式执行匹配验证

Is\_<type>(input) 判断输入类型

Strlen(input) 判断输入长度

### 平台层的防御

Web 应用防火墙

URL 策略与页面层策略

数据库权限控制

额外的部署考虑