《漏洞利用及渗透测试基础》实验报告

姓名：蒋薇 学号：2110957 班级： 张健老师班

**实验名称：**

SQL盲注

SQL盲注是一种利用应用程序对SQL注入漏洞的攻击技术，攻击者通过构造恶意输入数据，然后发送给应用程序，如果应用程序没有对输入数据进行充分的验证和过滤，就会将恶意数据直接传递给数据库执行，从而导致数据库受到攻击。SQL盲注攻击可以通过不断尝试来获取数据库中的敏感信息，例如用户名、密码、信用卡号等。攻击者可以利用盲注技术来逐步获取数据库中的信息，最终实现对目标系统的完全控制。为了防止SQL盲注攻击，应用程序需要对输入数据进行充分的验证和过滤，同时采用安全的SQL语句执行方式，例如使用参数化查询。

**实验要求：**

通过手工盲注攻击演示，了解SQL盲注攻击的原理和实现方式，并掌握如何利用SQL盲注漏洞来获取敏感信息。

实验环境：

* 操作系统：Windows 10
* 虚拟机：VMware Workstation 16 Pro
* 漏洞测试平台：DVWA 1.10（Damn Vulnerable Web Application）

**实验过程：**

1、下载并安装DVWA

首先，我们需要下载并安装DVWA漏洞测试平台。可以在官网上下载最新的版本，也可以在Github上下载源代码进行安装。

安装过程中需要配置数据库信息，可以选择使用自带的SQLite数据库或者其他数据库，例如MySQL。

2、登录DVWA

安装完成后，打开浏览器，输入DVWA的地址，进入登录界面。输入用户名和密码（默认为admin和password），登录到DVWA主界面。

3、设置安全等级为low

为了方便演示和测试，我们需要将DVWA的安全等级设置为low。在DVWA主界面上方的导航栏中，选择“DVWA Security”页面，在“Security level”中选择“low”，然后点击“submit”按钮保存设置。

4、进入SQL注入页面

在DVWA主界面上方的导航栏中，选择“SQL Injection”页面。在页面中，我们可以看到一个输入框和一个“submit”按钮。

5、尝试手工注入

现在我们可以开始手工注入攻击。我们先在输入框中输入一个单引号（'）并点击“submit”按钮，查看页面的返回结果。

可以看到页面返回了一个SQL错误信息，这表明输入的数据被直接拼接到了SQL语句中，存在SQL注入漏洞。

接下来，我们需要尝试构造恶意输入数据，利用盲注技术来获取数据库中的信息。这里我们以获取数据库名为例进行演示。

我们可以通过构造如下的注入语句来尝试获取数据库名：

' union select database(),null#

在注入语句中，我们使用了union关键字将两条SQL语句拼接在一起，第一条SQL语句是获取当前数据库名的语句，第二条SQL语句是填充注入点的占位符。

在执行上述语句后，页面返回了一个包含数据库名的结果，表明我们成功利用盲注技术获取了数据库名。

6、进一步尝试获取其他信息

通过类似的方法，我们可以进一步尝试获取数据库中的其他信息，例如表名、列名、数据等。这里我们以获取user表中的用户名和密码为例进行演示。

首先，我们需要确定user表的表名和列名。通过构造如下的注入语句，我们可以获取user表的表名：

' union select table\_name,null from information\_schema.tables where table\_schema=database()#

在上述语句中，我们使用了information\_schema.tables系统表来获取当前数据库中的表信息，其中table\_schema=database()表示获取当前数据库中的表信息。

执行上述语句后，页面返回了一个包含user表名的结果，表明我们成功获取了user表的表名。

接下来，我们需要确定user表中的用户名和密码列名。通过构造如下的注入语句，我们可以获取user表中的列名：

' union select column\_name,null from information\_schema.columns where table\_name='user'#

在上述语句中，我们使用了information\_schema.columns系统表来获取user表中的列信息，其中table\_name='user’表示获取user表中的列信息。

执行上述语句后，页面返回了一个包含用户名和密码列名的结果，表明我们成功获取了user表中的列名。

最后，我们可以通过构造如下的注入语句，获取user表中的用户名和密码：

' union select user,password from user#

在上述语句中，我们直接从user表中获取了用户名和密码信息。

执行上述语句后，页面返回了一个包含用户名和密码的结果，表明我们成功获取了user表中的敏感信息。

**心得体会：**

通过本次实验，了解了SQL盲注攻击的原理和实现方式，掌握了如何利用SQL盲注漏洞来获取敏感信息。