

数据库基础

数据库基础

一、数据库管理系统

- (一) .数据库管理系统介绍
- (二) 关系型数据库管理系统
- (三) 非关系型数据库
- (四) 关系型数据库VS非关系型数据库

Mysql数据库简介

安装windows版本的mysql5.5

远程连接

二、MySql数据库简介

三、安全值守数据库常用语句

1.用户权限设置

- Mysql中用户是如何定义的
- 用户创建
- 用户删除
- 用户查询
- 权限级别介绍
- 查看用户权限赋予情况
- 用户授权

2.元数据查询

3.union查询详解

4.分组查询

5.字符串函数

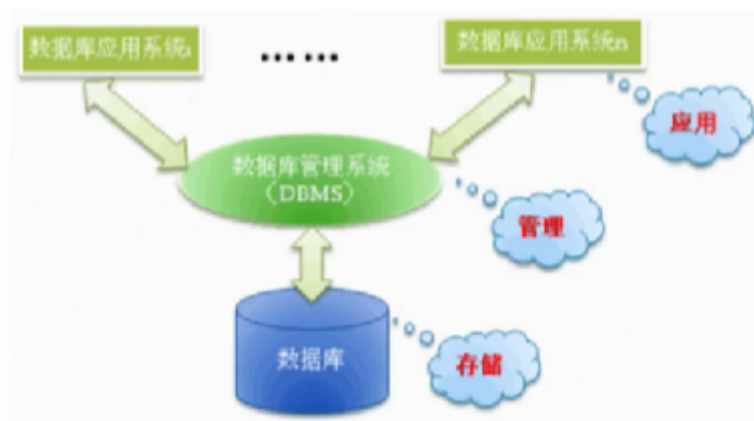
6.mysql数据库导入导出

四、数据库漏扫工具scuba介绍

一、数据库管理系统

(一) .数据库管理系统介绍

DBMS是由数据库及其管理软件组成的系统



2.常用的数据库管理厂商

Oracle数据库: (<https://www.oracle.com/>): Oracle数据库是被认为比较成功的一款**关系型数据库**，由世界第二大软件供应商**Oracle公司**于1983年推出。Oracle数据库具有运行稳定、功能齐全、性能优异等特点，在数据库产品中技术也比较先进。在多年的数据库市场竞争中，一直占据着比较有利的态势，尽管如此，Oracle并没有满足于现有的优势，在不断完善自身技术同时，也在开辟着新市场领域。Oracle数据库是一种大型数据库系统，一般用于商业，政府部门，它功能强大，在网络方面也用的非常多。

IBM DB2数据库: (<https://www.ibm.com/cn-zh>): DB2数据库是IBM出口的一系列关系型数据库管理系统，分别在不同的操作系统平台上服务。虽然DB2产品是基于UNIX的系统和个人计算机操作系统，在基于UNIX系统和微软在windows系统下的Access方面，DB2追寻了ORACLE的数据库产品。

SQL Server数据库: (<https://www.microsoft.com/zh-cn/sql-server/sql-server-2019>): SQL Server数据库是一款功能全面的数据库，可用于中大型企业单位，它由世界第一软件供应商Microsoft公司推出，与其他数据库相比，在操作性和交互性上有着很大的优势。SQL，**结构化查询语言**。SQL语言的主要功能就是同各种数据库建立联系，进行沟通。按照ANSI的规定，SQL被作为关系型数据库管理系统的标准语言。SQL语句可以用来执行各种各样的操作，例如更新数据库中的数据，从数据库中提取数据等。

PostgreSQL数据库: (<https://www.postgresql.org/>): PostgreSQL数据库是一款功能强大的**开源对象关系数据库管理系统 (ORDBMS)**，用于安全地存储数据;支持最佳做法，并允许在处理请求时检索它们。PostgreSQL由PostgreSQL**全球开发集团**(全球志愿者团队)开发。它不受任何公司或其他私人实体控制。它是开源的，其源代码是免费提供的。PostgreSQL是跨平台的，可以在许多操作系统上运行，如Linux，FreeBSD，OS X，Solaris和Microsoft Windows等。

MySQL数据库: (<https://www.mysql.com/>): MySQL数据库是一款开源的小型关系型数据库管理系统，开发者为**瑞典MySQLAB公司**，在2009年被Oracle公司收购，但是MySQL仍然是开源的，与其他数据库相比它有着体积小、速度快、使用灵活等特点，MySQL被广泛地应用在Internet上的中小型网站中。许多中小型网站为了降低网站总体拥有成本而选择了MySQL作为网站数据库。

Sybase数据库: (<http://www.sybase.com.cn/>): Sybase是美国Sybase公司研制的一种关系型数据库系统，是一种典型的UNIX或WindowsNT平台上客户机/服务器环境下的大型数据库系统。Sybase提供了一套应用程序编程接口，可以与非Sybase数据源及服务器集成，允许在多个数据库之间复制数据，适于创建多层应用。系统具有完备的触发器、存储过程、规则以及完整性定义，支持优化查询，具有较好的数据安全性。

南大通用GBase 8a数据库: (<http://www.gbase.cn/news/387.html>): 南大通用分析型数据库GBase 8a是支撑大数据快速分析的新型数据库，作为列存储的分析型数据库，南大通用Gbase还是有其独到之处的，以新型的存储结构、数据压缩、数据映照和优化算法等技术大幅度提高对海量数据进行统计分析的运算速度。GBase 8a能够实现大数据的全数据（结构化数据、半结构化数据和非结构化数据）存储管理和高效分析，为大数据应用提供完整的数据库解决方案。GBase 8a以新型的存储结构、数据压缩、数据映照和优化算法等技术大幅度提高对海量数据进行统计分析的运算速度。

redis数据库: (<https://redis.io/>): redis是一个key-value存储系统。和Memcached类似，它支持存储的value类型相对更多，包括string(字符串)、list(链表)、set(集合)、zset(sorted set --有序集合)和hash（哈希类型）。这些数据类型都支持push/pop、add/remove及取交集并集和差集及更丰富的操作，而且这些操作都是原子性的。在此基础上，redis支持各种不同方式的排序。与memcached一样，为了保证效率，数据都是缓存在内存中。区别的是redis会周期性的把更新的数据写入磁盘或者把修改操作写入追加的记录文件，并且在此基础上实现了master-slave(主从)同步。

3.数据库排名

(<https://db-engines.com/en/ranking>)最新的全球10大数据库排名

397 systems in ranking, October 2022								
Rank			DBMS	Database Model	Score			
Oct 2022	Sep 2022	Oct 2021			Oct 2022	Sep 2022	Oct 2021	
1.	1.	1.	Oracle +	Relational, Multi-model i	1236.37	-1.88	-33.98	
2.	2.	2.	MySQL +	Relational, Multi-model i	1205.38	-7.09	-14.39	
3.	3.	3.	Microsoft SQL Server +	Relational, Multi-model i	924.68	-1.62	-45.93	
4.	4.	4.	PostgreSQL +	Relational, Multi-model i	622.72	+2.26	+35.75	
5.	5.	5.	MongoDB +	Document, Multi-model i	486.23	-3.40	-7.32	
6.	6.	6.	Redis +	Key-value, Multi-model i	183.38	+1.91	+12.03	
7.	7.	↑ 8.	Elasticsearch	Search engine, Multi-model i	151.07	-0.37	-7.19	
8.	8.	↓ 7.	IBM Db2	Relational, Multi-model i	149.66	-1.73	-16.30	
9.	9.	↑ 11.	Microsoft Access	Relational	138.17	-1.87	+21.79	
10.	10.	↓ 9.	SQLite +	Relational	137.80	-1.02	+8.43	

所以，目前数据库管理系统由关系型数据库管理系统和非关系性数据库管理系统

关系型数据库和非关系型数据库在使用场景上差别比较大，所以并不存在孰强孰弱，只有结合自身的业务特点才能发挥出这两类数据库的优势

(二) 关系型数据库管理系统

Oracle SQL-Server MySQL DB2 Maria DB Access Sqlite

1.数据存储结构：二维表结构

2.查询能力：支持复杂查询能力

3.数据一致性：强一致性ACID使得对于安全性能有很高的数据访问要求得以实现

4. 高价值型

信息	站票1	剖析	状态							
stuid	stuname	sex	age	birth	mr	home	tel	email	beizhu1	
1	张三	m	25	1996-01-01 00:00	0	北京	18762533546	abc@def.com	(Null)	
6	李四	m	25	1996-01-01 00:00	0	北京	18762533546	(Null)	(Null)	
7	张三	f	25	1996-02-01 00:00	0	北京	18769533546	ddd@def.com	(Null)	
8	王二3	m	25	1996-01-01 00:00	0	北京市朝阳区	18764533546	sfsdf@def.com	(Null)	
9	张三5	m	24	1997-01-01 00:00	0	北京	18762533546	abc@def.com	(Null)	
10	六六1	f	27	1994-02-01 00:00	0	上海	18769533546	ddd@def.com	(Null)	

(三) 非关系型数据库

MongoDB redis HBASE

1.数据存储结构：一种数据结构化存储方法的集合，可以是文档或者键值对等。

2.查询能力：复杂查询欠缺

3.扩展性好

4.无事务处理的概念

5.高扩展性

6.低成本性

```
{
  "resultcode": "200",
  "reason": "succeeded",
  "result": [
    {
      "wid": "00",
      "weather": "晴"
    },
    {
      "wid": "01",
      "weather": "多云"
    }
  ],
  "error_code": 0
}
```

（四）关系型数据库VS非关系型数据库

	关系型数据库	非关系型
强大的查询能力	√	×
强一致性	√	×
二级线索	√	×
灵活模式	×	√
扩展性	×	√
性能	×	√

1.不是否定关系型数据库，而是做关系型数据库的补充

2.想做老大，先学会做老二

Mysql数据库简介

1.看排名：(<https://db-engines.com/en/ranking>)

Rank			DBMS	Database Model	Score		
Oct 2022	Sep 2022	Oct 2021			Oct 2022	Sep 2022	Oct 2021
1.	1.	1.	Oracle +	Relational, Multi-model ⓘ	1236.37	-1.88	-33.98
2.	2.	2.	MySQL +	Relational, Multi-model ⓘ	1205.38	-7.09	-14.39
3.	3.	3.	Microsoft SQL Server +	Relational, Multi-model ⓘ	924.68	-1.62	-45.93
4.	4.	4.	PostgreSQL +	Relational, Multi-model ⓘ	622.72	+2.26	+35.75
5.	5.	5.	MongoDB +	Document, Multi-model ⓘ	486.23	-3.40	-7.32
6.	6.	6.	Redis +	Key-value, Multi-model ⓘ	183.38	+1.91	+12.03
7.	7.	↑8.	Elasticsearch	Search engine, Multi-model ⓘ	151.07	-0.37	-7.19
8.	8.	↓7.	IBM Db2	Relational, Multi-model ⓘ	149.66	-1.73	-16.30
9.	9.	↑11.	Microsoft Access	Relational	138.17	-1.87	+21.79
10.	10.	↓9.	SQLite +	Relational	137.80	-1.02	+8.43

2.企业使用



3.版本选择

mysql的版本选择

- 1.稳定版 发行6-12个月以内的
- 2.小版本 偶数版本，奇数版本不选是测试开发版本

所以我们选择5.7.30 5.7要选择5.7.17版本以上 因为有MVV(高性能)

4.安装及远程连接

安装windows版本的mysql5.5

1.安装之前需要注意以下几

建议不要安装最新版本，一般找mysql5.0系列版本即可；

mysql官网有.zip和.msi两种安装形式；

zip是压缩包，直接解压缩以后使用的，需要自己配置各种东西；msi是安装包，系统直接帮我们安装搞定；

新手建议使用msi安装方式；

2.mysql下载地址(<https://dev.mysql.com/downloads/windows/installer/>)

General Availability (GA) Releases

MySQL Installer 5.7.28

Select Version:
5.7.28

Select Operating System:
Microsoft Windows

Looking for the latest GA version?

Windows (x86, 32-bit), MSI Installer (mysql-installer-web-community-5.7.28.0.msi)	5.7.28	18.6M	Download
Windows (x86, 32-bit), MSI Installer (mysql-installer-community-5.7.28.0.msi)	5.7.28	493.0M	Download

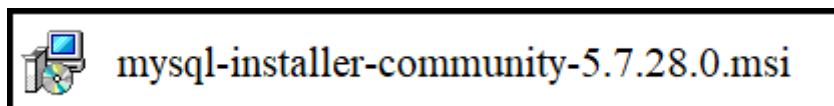
We suggest that you use the MD5 checksums and GnuPG signatures to verify the integrity of the packages you download.

web这种表示在线安装

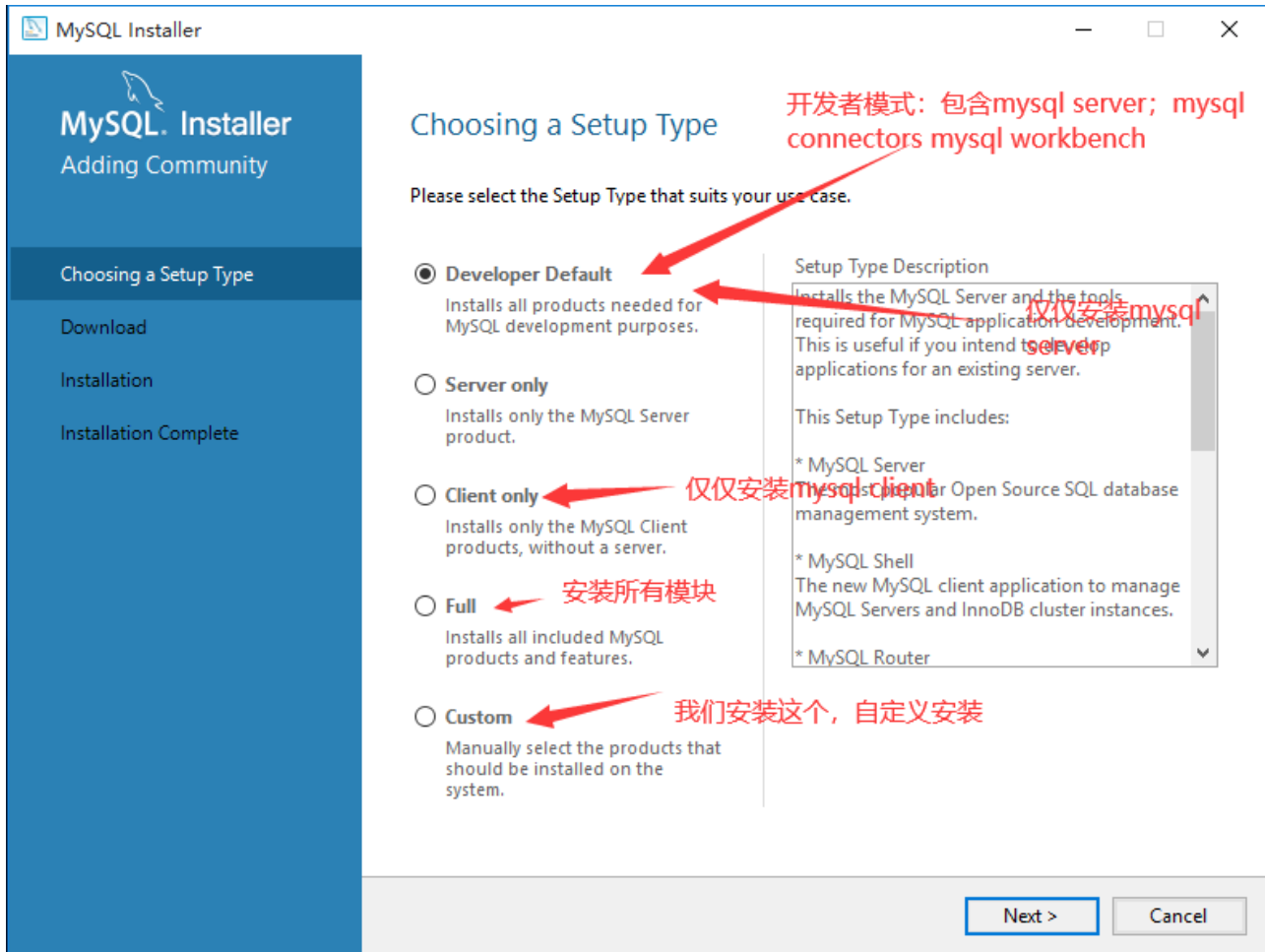
这种表示离线安装，我们选择这种。

3.安装步骤

双击这个程序



*出现如下这个界面后，勾选"I accept the license terms"， 点击"Next"。



出现如下界面后，我们进行如下的操作。

MySQL. Installer

Adding Community

Choosing a Setup Type

Select Products

Installation

Product Configuration

Installation Complete

Select Products

Please select the products you would like to install on this computer.



Filter:

All Software, Current Bundle, Any

Edit

Available Products:

- MySQL Servers
- Applications
- MySQL Connectors
 - Connector/ODBC
 - Connector/C++
 - Connector/J
 - Connector/J 8.0
 - Connector/J 8.0.31 - X86
 - Connector/NET
 - Connector/Python
- Documentation

Products To Be Installed:

- MySQL Server 5.7.40 - X64
- MySQL Workbench 8.0.31 - X64
- Connector/J 8.0.31 - X86

这一步，我们可以将左边窗口中，需要安装的一些东西，移动到右边窗口及逆行安装

☐ Enable the Select Features page to customize product features

Published: 2022年10月11日

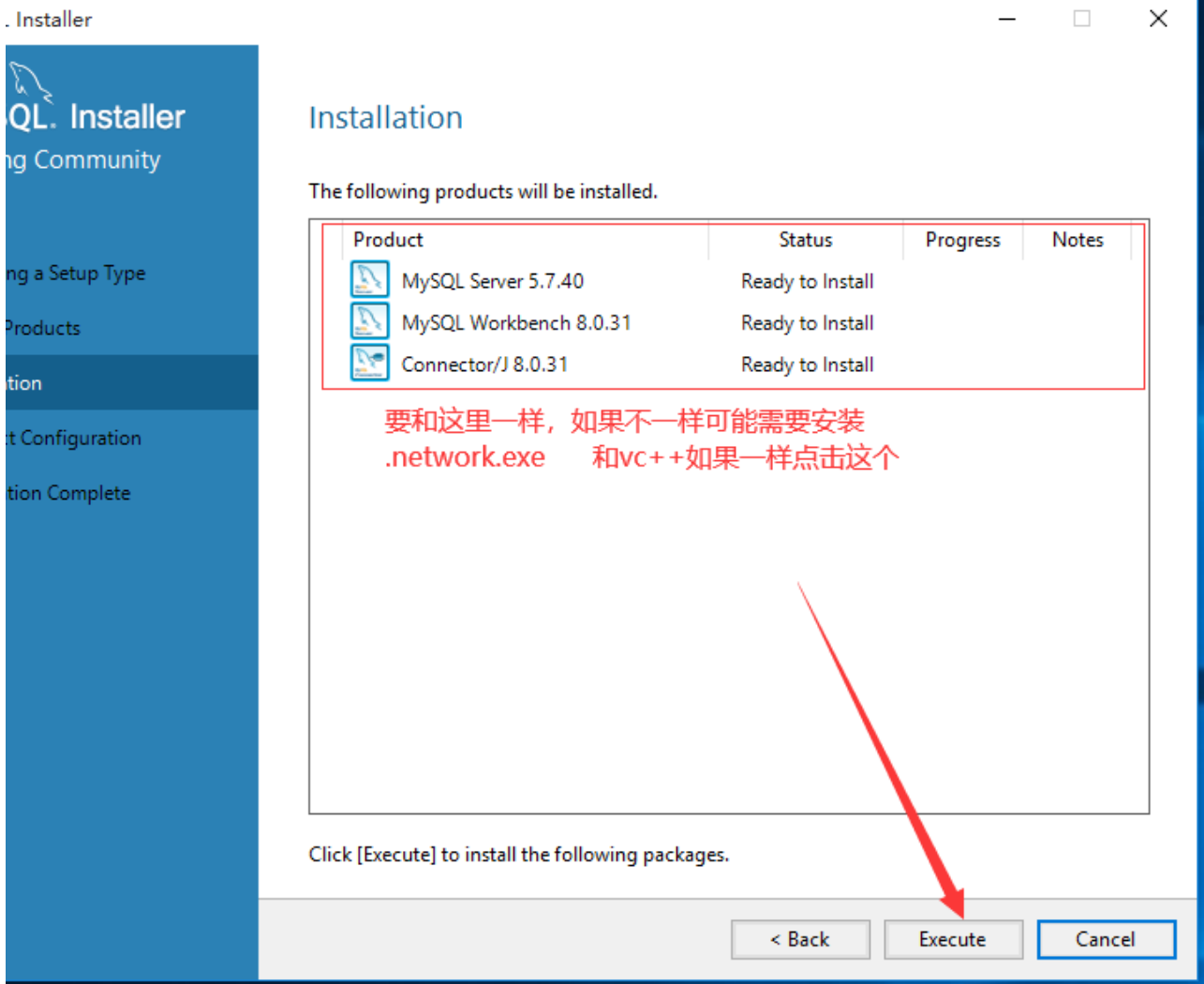
Release Notes: <https://dev.mysql.com/doc/relnotes/connector-j/8.0/en/news-8-0-31.html>

< Back

Next >

Cancel

出现如下界面后，证明可以了，点击"Execute"。



当出现如下界面后，点击"Next"。

Installation

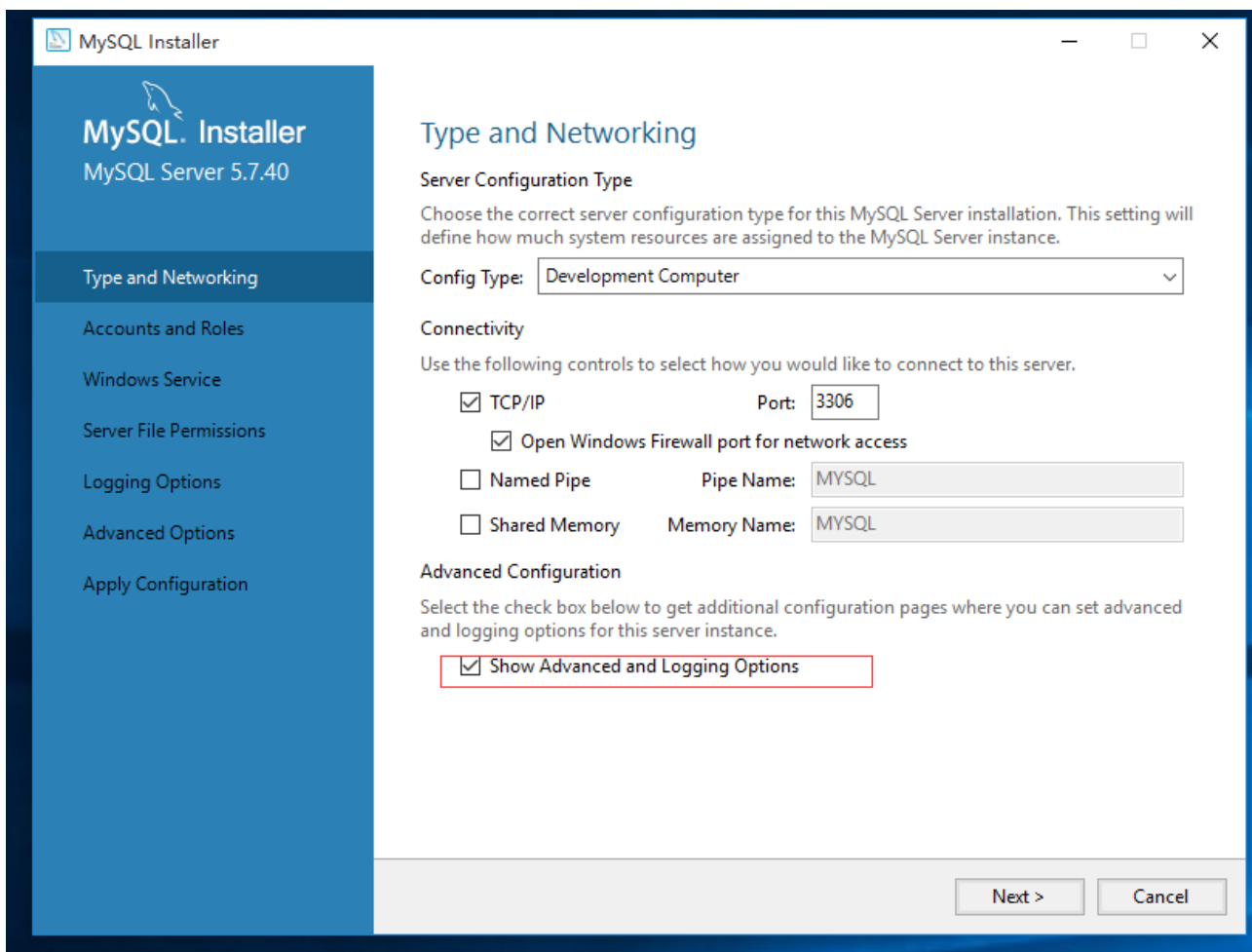
The following products will be installed.

Product		Status	Progress	Notes
✓	MySQL Server 5.7.40	Complete		
✓	MySQL Workbench 8.0.31	Complete		
✓	Connector/J 8.0.31	Complete		

[Show Details >](#)

< Back Next > Cancel

当出现如下界面后，使用界面默认内容即可，点击"Next"。



当出现如下界面后，设置好密码后，点击"Next"。

Accounts and Roles

Root Account Password

Enter the password for the root account. Please remember to store this password in a secure place.

MySQL Root Password:

Repeat Password:

Password strength: **Weak**

输入密码

MySQL User Accounts

Create MySQL user accounts for your users and applications. Assign a role to the user that consists of a set of privileges.

MySQL User Name	Host	User Role
-----------------	------	-----------

Add User

Edit User

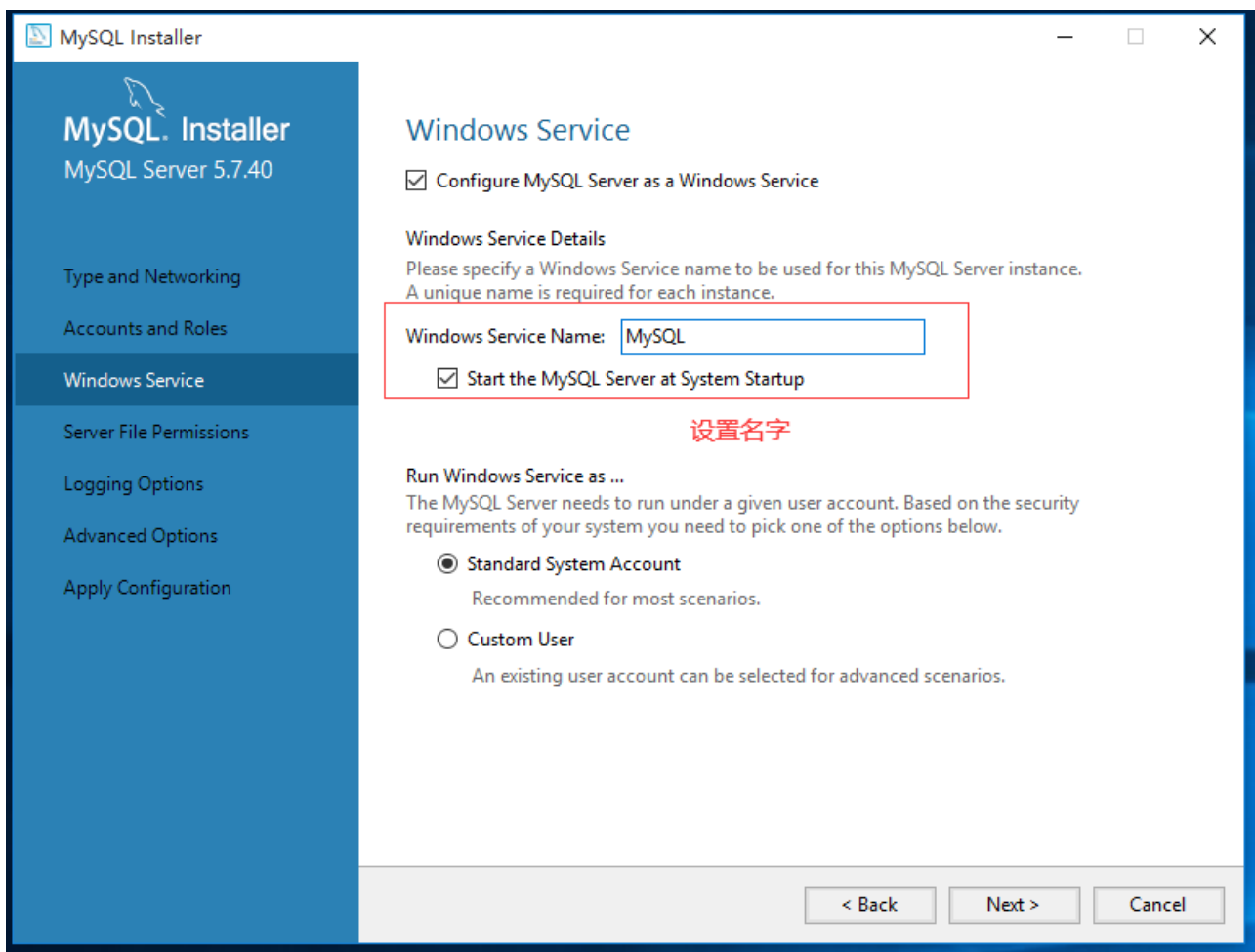
Delete

< Back

Next >

Cancel

当出现如下界面后，进行如下设置后，点击"Next"。



当出现如下界面后，直接点击"Finish"。

Apply Configuration

The configuration operation has completed.

Configuration Steps Log

- ✓ Writing configuration file
- ✓ Updating Windows Firewall rules
- ✓ Adjusting Windows service
- ✓ Initializing database (may take a long time)
- ✓ Updating permissions for the data folder and related server files
- ✓ Starting the server
- ✓ Applying security settings
- ✓ Updating the Start menu link

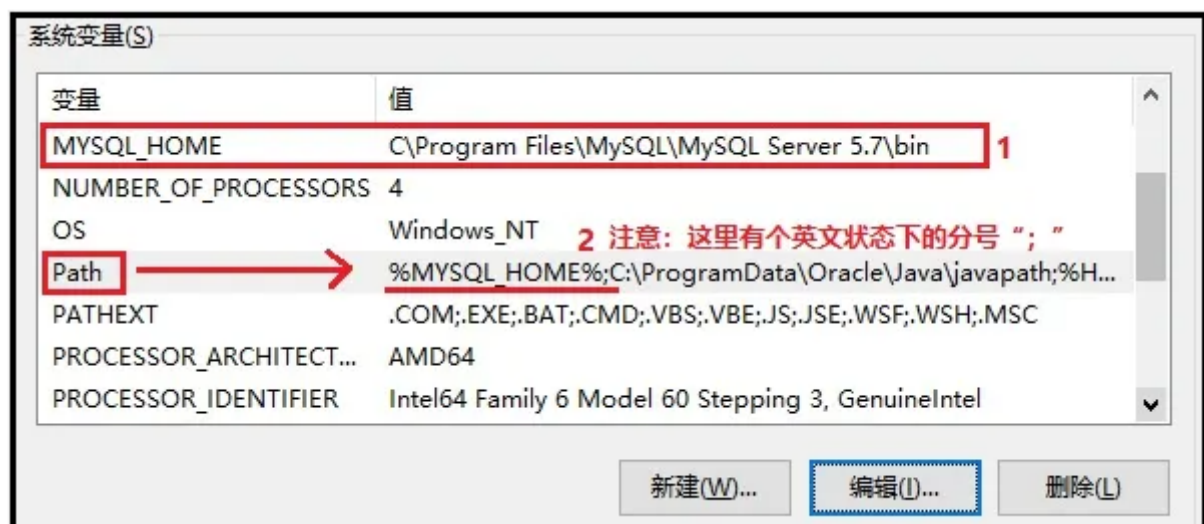
The configuration for MySQL Server 5.7.40 was successful.
Click Finish to continue.

Finish

配置变量

配置环境变量：打开我的电脑->属性->高级->环境变量，在系统变量里选择 PATH。

只需要添加如下两处内容即可：




```
C:\Users\hy>mysql -uroot -p
Enter password: *****
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
Server version: 5.7.40-log MySQL Community Server (GPL)

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
mysql>
mysql>
mysql>
```

这样我们就成功了

远程连接

SQLyog-13.1.7-0.x64Community	2021/8/3 13:50	应用程序	6,063 KB
安装这个软件，直接下一步就可以			

连接到我的SQL主机

新建 Clone... 保存 重命名 删除

保/存的连接 ☐ 新连接

MySQL HTTP SSH SSL 高级功能

MySQL Host Address localhost

用户名 root

密码 ☒ 保存密码

端口 3306

数据/库

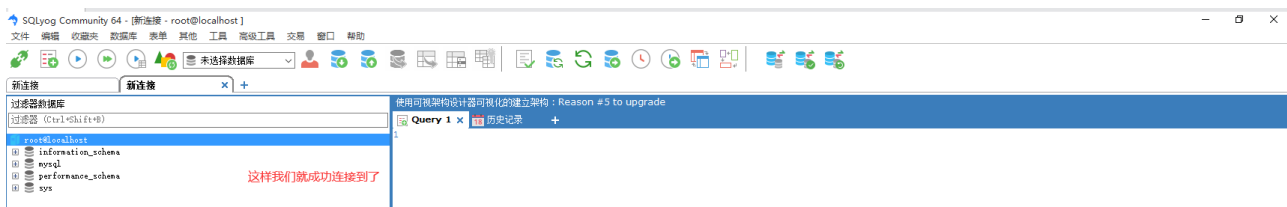
(Use ';' to separate multiple databases. Leave blank to display all)

☒ Use Compressed Protocol

会话空闲超时 ☒ 默认 ☐ 28800 (秒) Keep-Alive Interval (秒)

[Need Help?](#)

连接 取消(L) 测试连接



二、MySQL数据库简介

1.mysql的基本操作

--创建学生数据库

```
CREATE DATABASE IF NOT EXISTS student;
```

--创建学生信息表

三、安全值守数据库常用语句

1.用户权限设置

--MySQL中用户是如何定义的

用户名@主机域

例如：10.0.0.0.51、10.0.0.0.%、%、10.0.0.0/255.255.255.0、Db01、Localhost、127.0.0.1

--用户创建

```
create user xinjing@ '%' identified by '123';
```

--用户删除

```
drop user username;
```

username: 是要删除的用户名

如: drop user root@'%'

drop user '@'127.0.0.1' 用户名为空的删除

--用户查询

```
use mysql
```

```
select user,host from user;
```

--权限级别介绍

全局————可以管理整个MySQL

库————可以管理指定的数据库

表————可以管理指定数据库的指定表

字段————可以管理指定数据库的指定表的指定字段

权限存储在mysql库中的user、db、tables_priv、columns_priv、procs_priv

这几个系统表中，待MySQL实例启动后就加载到内存中

--查看用户权限赋予情况

```
show grants for xinjing@'%' 查看用户权限
```

--用户授权

`grant all privileges on stu.* to xinjing'@%' identified by '123' with option;`

给新进的xinjing@%这个用户用密码123可以有stu数据库的所有权限，并可以给其他用户授权

`revoke all privileges on stu.* from 'xinjing'@'%';` 取消xinjing@%用户的所有

权限

2.元数据查询

`Select version();` 服务器版本信息

`Select database();` 当前数据库名

`Select user();` 当前用户名

`Select status;` 服务器状态

`Select variables;` 服务器配置变量

`Show global variables like '%datadir%';` 看数据文件存放位置

`Show global variables like '%datadir%'`

`Select @@datadir;` 查询数据库的路径

`Select @@basedir` 查询mysql的安装路径

3.union查询详解

union查询就是把2条或者多条sql语句的查询结果，合并成一个结果集。

sql1: N行, sql2: M行, `sql1 union sql2`---->N+M行

要求结果集中的列数一致就可以（如果都是2列或者N行）

union取出的最终列名，以第一条sql为准

union查询默认会去重，如果不想去重就用union all

例:`use student;` 使用student数据库

create table temp1(uid int primary key auto_increment, uname varchar(20)
not null) 新建temp1表

insert into temp1(uname) values('zs'),('ls'),('ll'); 插入数据

create table temp2(eid int primary key auto_increment, age int not null) 新建temp2表

insert into temp2(age) values(11),(19),(20); 插入数据

select * from temp1 union select * from temp2 用union联合查询temp1和temp2表

4.分组查询

GROUP_CONCAT() 信息组合在一起查询 分组展示

select sid, GROUP_CONCAT(cid), GROUP_CONCAT(cj order by cj desc
SEPARATOR ' ') from score GROUP BY sid

5.字符串函数

LOWER(COLUMN|STR) 将字符串全部转换为小写字母

UPPER(COLUMN|STR) 将字符串全部转换为大写字母

CONCAT(COLUMN|STR1,COLUMN|STR2,..) 将多个字符串首尾相连后返回

CONCAT_WS(SERAPATOR,STR1,STR2...) 将多个字符串指定连接符serarator的首尾相连后返

SUBSTR(STR,POS[,LEN]) 从字符串中的指定位置pos开始取一个字符串返回

LENGTH(STR) 返回字符的存储长度

CHAR_LENGTH(STR) 返回字符串的字符个数

6.mysql数据库导入导出

----表数据（记录）导入导出

-----导出为txt文件

```
select * from demo1 into outfile '/trem/utemp1data.txt';
```

```
use student;
```

```
show VARIABLES like "secure_file_priv";
```

----导入txt文件

```
load data local infile '/root/utemp1data.txt' into table temp;
```

----Mysqldump导出

----dump出表utemp1

```
----mysqldump -uroot -p student utemp1>uyemp1.sql
```

----dump出库student

```
----mysqldump -uroot -p student>student.sql
```

----dump所有的数据库及数据库表

```
-----mysqldump -u root -p --all-databases>mysqldatabases.sql
```

----mysql数据库导入"<"

----新建一个数据库

```
create database dumpdemo1
```

----回到mysql接口

```
----mysql -u root -p654321 dumpdemo1<student.sql
```

---- 进入mysql验证

```
use dumpdemo1
```

```
show tables;
```

----mysql的数据库导入"source"

```
mysql -u root -p
```

```
create database sourcedumpdemo;
```

```
source /var/lib/mysql-files/student.sql
```

四、数据库漏扫工具scuba介绍

Scuba是一款数据库扫描软件

扫描数据库漏洞，寻找不安全的因素，提升数据库安全等级，及时解决漏洞问题

支持Oracle，SQLServer，SAP Sybase，IBM DB2和MYSQL等数据库

本地需要安装有JDK和MYSQL-CONNECTOR-JAVA-5.1.44-BIN.JAR即可

```
java-vesion
```

一、前言

Scuba(数据库扫描工具)官方版是一款高效的数据库扫描工具。Scuba(数据库扫描工具)最新版可扫描世界领先的企业数据库，以查找安全漏洞和配置缺陷(包括修补级别)。Scuba(数据库扫描工具)官方版可以对个人数据库扫描，也可以对企业数据库扫描，让管理人员及时发现漏洞，及时维护数据库。

Scuba 针对 Oracle Database、Microsoft SQL Server、SAP Sybase、IBM DB2、Informix 和 MySQL 提供了接近 1200 次评估测试。

二、下载

链接: <https://pan.baidu.com/s/1L4tvnYu9q5D3IjzBf6NFNg>

提取码: lqvh

三、安装与使用

第一步：解压“scuba数据库漏洞扫描”的压缩包

此电脑 > 文档 (D:) > BaiduNetdiskDownload > scuba数据库漏洞扫描

名称	修改日期	类型	大小
mysql-connector-java-5.1.44	2017/8/29 4:13	文件夹	
Scuba-Windows	2021/6/1 9:37	文件夹	
java64w_69959.rar	2017/11/2 15:17	WinRAR 压缩文件	86,888 KB
mysql-connector-java-5.1.44.zip	2017/11/2 11:52	WinRAR ZIP 压缩...	3,732 KB
Scuba-Linux-x64.tar.gz	2017/11/2 10:03	WinRAR 压缩文件	94,016 KB
Scuba-Windows.zip	2017/11/2 10:01	WinRAR ZIP 压缩...	85,638 KB

把这两个解压出来



第二步：安装jdk(已有忽略)，将mysql-connector-java-5.1.44文件夹下的mysql-connector-java-5.1.44-bin.jar，复制到\Scuba-Windows\ODBC\Production\MYSQL目录下

D:\BaiduNetdiskDownload\scuba数据库漏洞扫描\Scuba-Windows\ODBC\Production\MYSQL

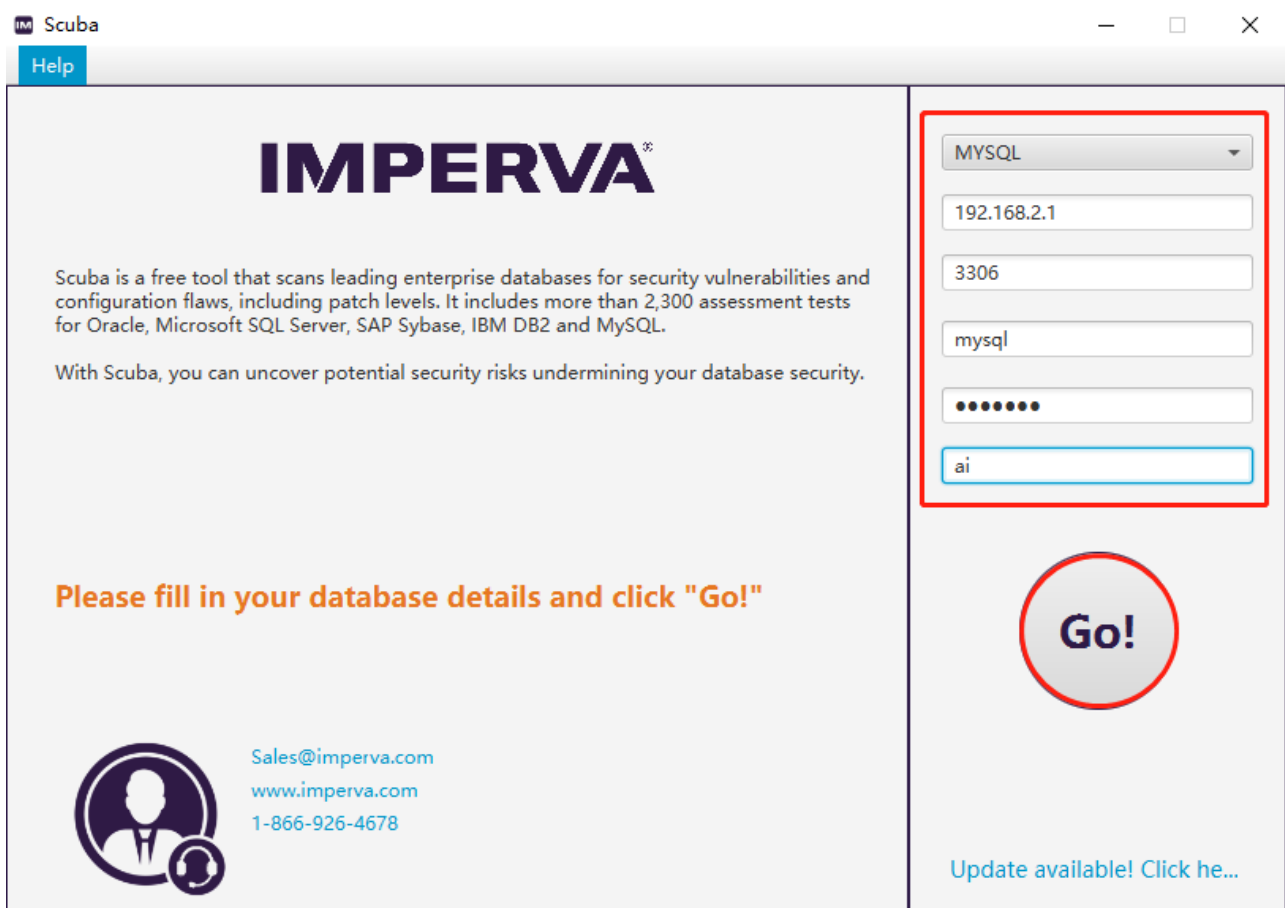
名称	修改日期	类型	大小
 mysql-connector-java-5.1.44-bin.jar	2017/8/29 4:13	Executable Jar File	977 KB

第三步：启动程序，双击Scuba.exe

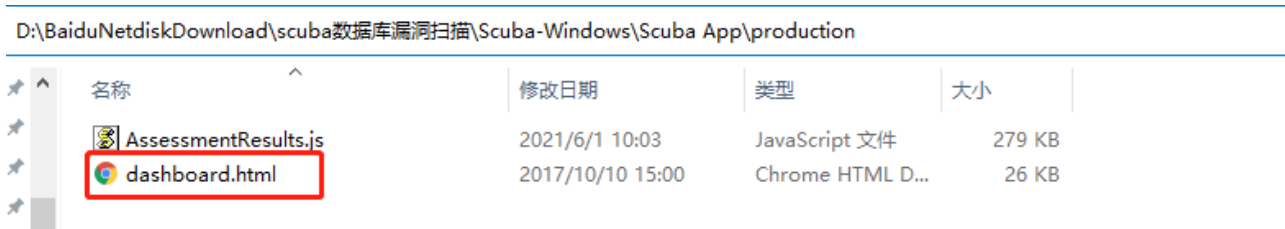
\BaiduNetdiskDownload\scuba数据库漏洞扫描\Scuba-Windows

名称	修改日期	类型	大小
Assessments	2017/10/10 15:00	文件夹	
conf	2021/6/1 9:41	文件夹	
css	2017/10/10 15:00	文件夹	
Documentation	2017/10/10 15:00	文件夹	
jre	2017/10/10 15:00	文件夹	
lib	2017/10/10 15:00	文件夹	
logs	2021/6/1 9:37	文件夹	
ODBC	2017/10/10 15:00	文件夹	
Scuba App	2017/10/10 15:00	文件夹	
ntlmauth.dll	2017/1/2 15:29	应用程序扩展	48 KB
 Scuba.exe	2017/10/10 14:59	应用程序	154 KB
 Scuba.jar	2017/10/10 15:00	Executable Jar File	318 KB

第四步：扫描，选择扫描的数据库类型，配置IP、端口、用户名、密码、数据库名，点击Go!



第五步：扫描完成后生成报告



第六步：查看报告

