友乾营

报表的SQL植入风险

规避风险：让你的报表变的安全起来

SQL植入的概念

恶意的SQL

归根结底：执行了不该允许执行的SQL命令，达到非法的目的

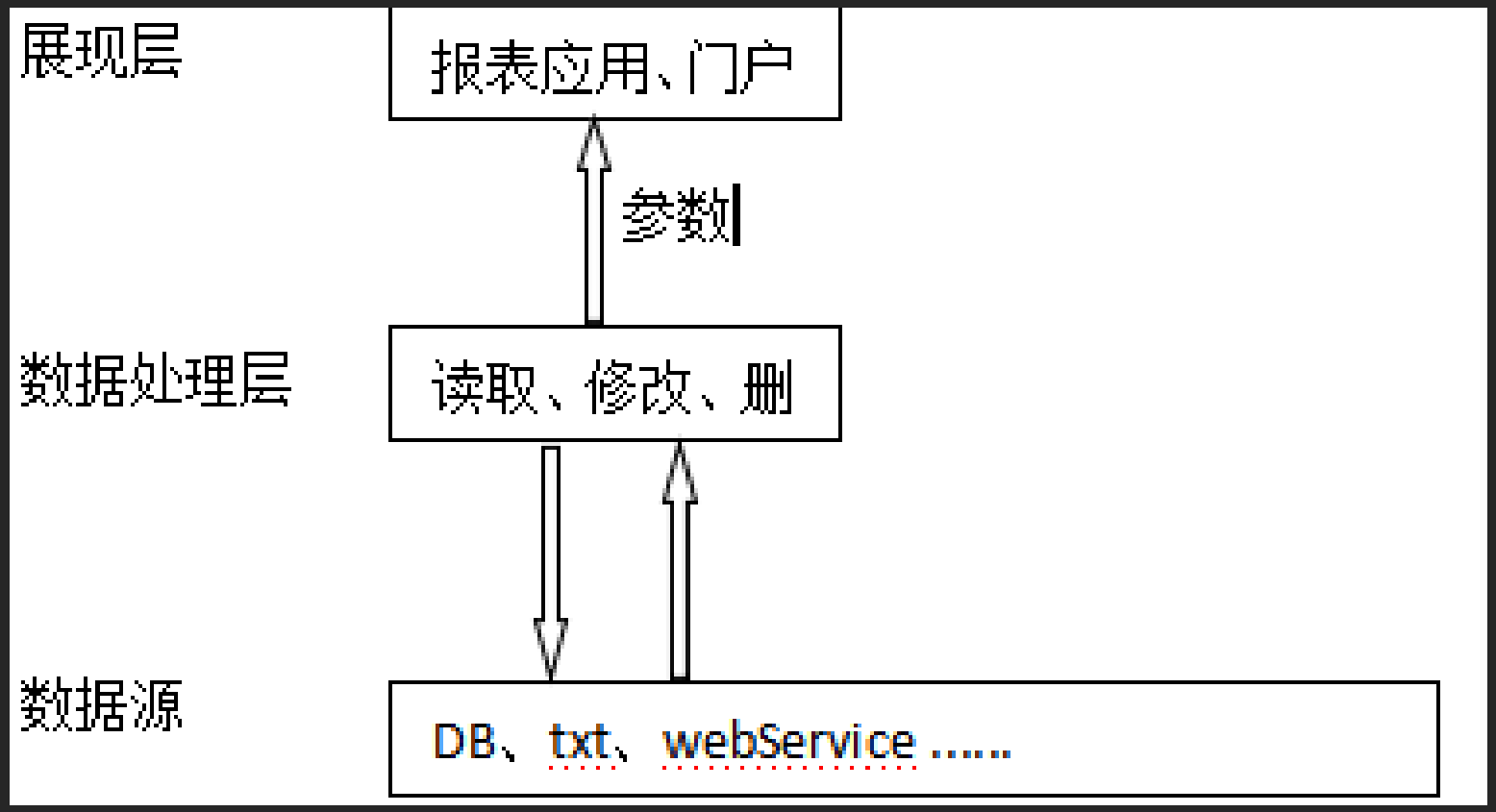
常见案例

骗过登录验证

非法获取账号信息

篡改、删除数据

为什么存在SQL植入



植入原理

如何攻击

特殊的输入参数

未处理特殊字符“--”、“#”

数据库配置不合理

植入原理： 案例1，特殊输入参数

union

- 猜表名： union all select * from t_user

or

条件恒真

植入原理： 案例1，特殊输入参数

or： 骗过登录

strSQL = "SELECT * FROM users WHERE userID = '" + userID + "' and pw = '"+ passWord +"';"

userID： 1 OR 1=1;

passWord： '1' OR 1=1;

strSQL = "SELECT * FROM users WHERE userID=1 OR 1=1 and pw =' 1' OR 1=1;"

植入原理： 案例2，特殊符号

友乾营

--

一般数据库注释均采用“--”

#

- mysql注释

植入原理： 案例2，特殊符号

骗过登录

strSQL = “select * from users where userID=”+userID+“and password=”+psw；

userID： “ " or 1=1 -- ”；

select ... from users where userID=" or 1=1 -- and pass...

userID： “" or 1=1 #”；

select ... from users where userID=" or 1=1 # and pass ...

植入原理： 案例3，数据库配置不合理

友乾营

篡改

拼update

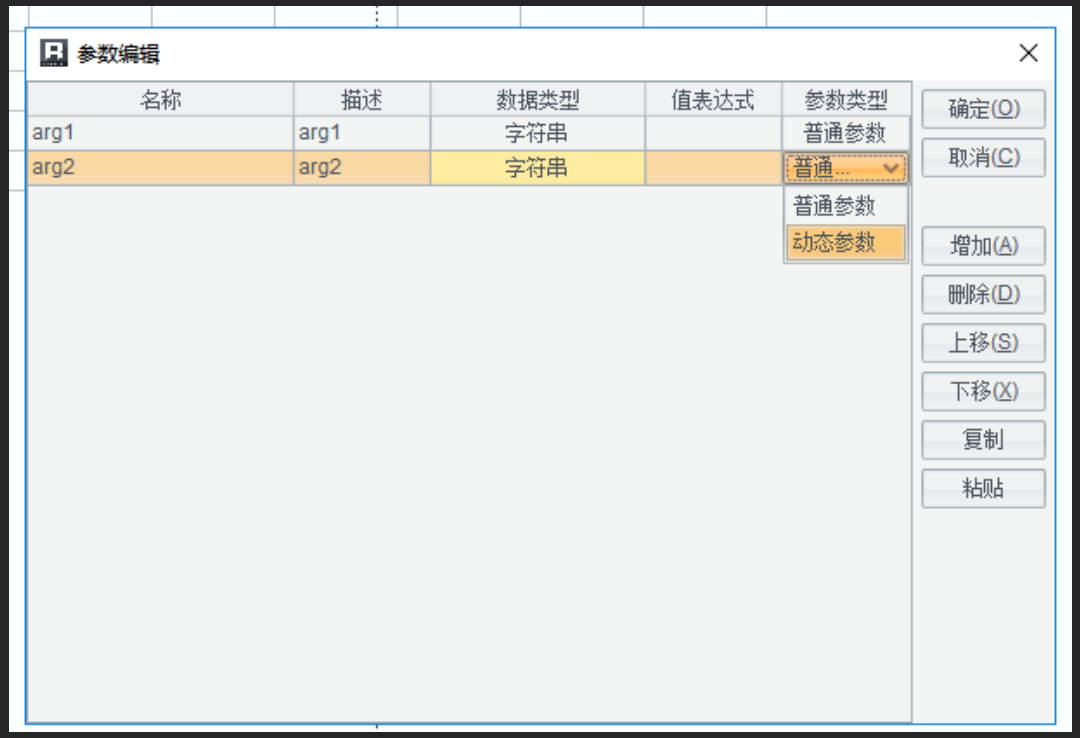
; update Users set pwd='1'

删除

- 拼delete、drop
- ; delete from users
- ;drop from users

报表和SQL植入有啥关系

报表参数



报表和SQL植入有啥关系：普通用法

普通用法：select * from t where date>=? and date<=?

一般写死的相对安全

报表和SQL植入有啥关系：通用查询

SQL1：select * from t where ${mac1}

mac1：date>=value1 and date<=value2

亦或： area in (1,2,3)

SQL2：select ${zd} from T where ...

报表和SQL植入有啥关系：通用查询

SQL1：select * from t where ${mac1}

mac1：1=0 union select ... from user

SQL1：select * from t where （${mac1}）

报表和SQL植入有啥关系：通用查询

SQL1：select * from t where （${mac1}）

mac1： 1=0) union select … from user where (1=1

rr

报表和SQL植入有啥关系：通用查询

SQL1：select * from t where （${mac1}）or ${mac1}

mac1： 1=0) union select … from user where (1=1

rr

报表工具提供防SQL植入的方法

xml配置选项

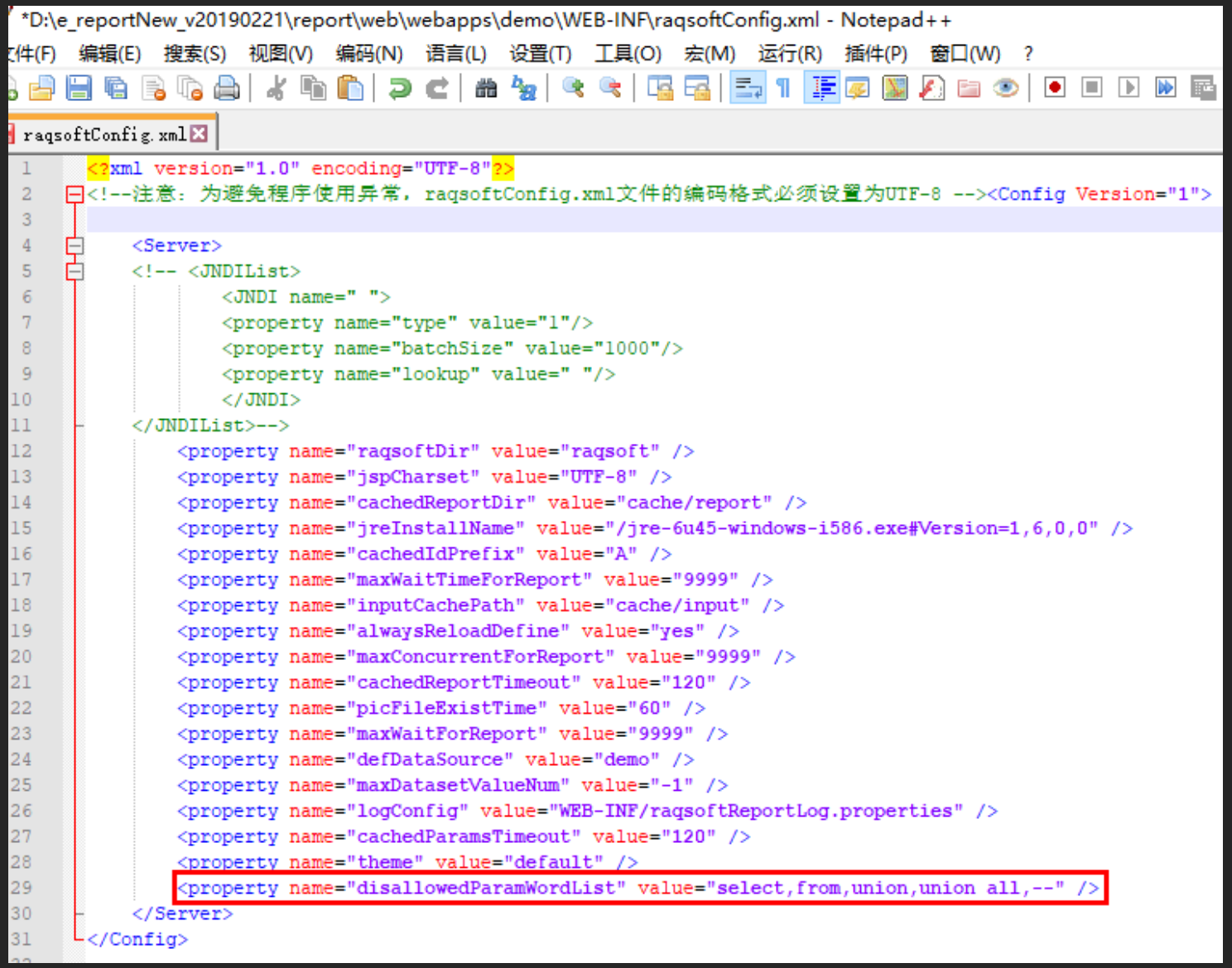
自定义

报表防植入： 报表工具xml配置

raqsoftConfig.xml

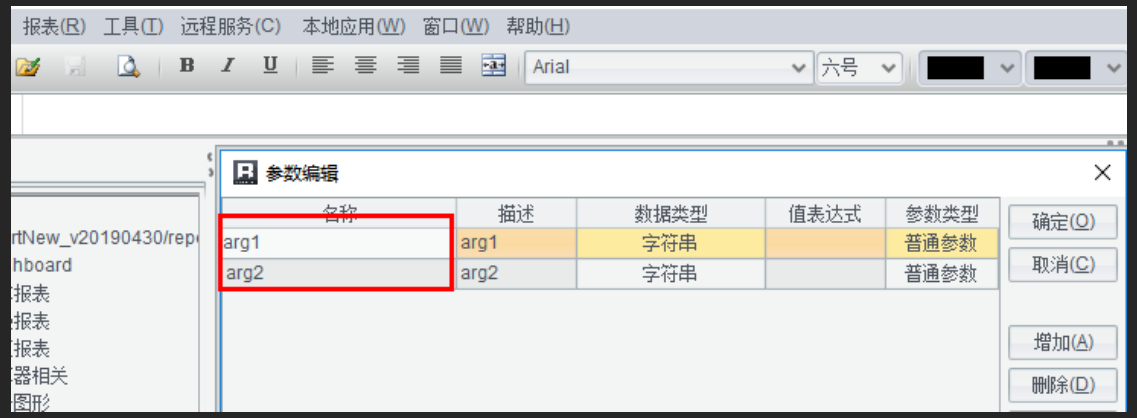
disallowedParamWordList
如:
<property name="disallowedParamWordList"
value="select,from,union,union all,or,--" />

报表防植入： 报表工具xml配置



报表防植入： 报表工具xml配置

Url： http://localhost:6868/demo/reportJsp/showReport.jsp?rpx=a.rpx&arg2=华北 union select * from users



错误提示：

报表防植入： 报表工具自定义参数检查类接口

1、对所有参数值检查
2、针对某些参数进行检查
3、自定义检查后返回的错误提示信息

```
public class ResistSQLInject implements IParamChecker {
    //校验不通过返回false，提供paramName以便用户只检查某种形式的参数
    public boolean check(String s, String s1) {
        //s为报表--参数内，定义的参数名；s1为报表接收到的对应s的参数值
        return false;
    }
    //检验不通过是可获取详细信息
    public String getCause() {
        return "错误信息";
    }
}
```

自定义类的具体实现方法

程序方式： 1、实现接口类（所有参数检查）


```
public class ResistSQLInject implements IParamChecker {
    private String cause = "";
    private List<String> wordList = new ArrayList<String>();
    public boolean check(String paramName, String inputValue) {
        if(inputValue == null || inputValue.length() == 0){//如果参数值为空，则无需检查
            return true;
        }
        if(wordList == null){ //如果检测关键字列表是空，则不作检查
            return true;
        }
        for(int i = 0; i < wordList.size(); i++){
            inputValue = inputValue.toLowerCase();//这里做，是为了不区分大小写
            if(inputValue.indexOf(wordList.get(i).toLowerCase()) >= 0){
                StringBuffer sb = new StringBuffer();
                sb.append("校验未通过，").append(paramName).append("参数中含有以下词汇：").append(wordList.get(i))
                        .append("\n位置：").append(inputValue.indexOf(wordList.get(i).toLowerCase()));
                this.cause = sb.toString();
                return false;
            }
        }
        return true;
    }

    public String getCause() {
        String tmp = this.cause;
        this.cause = "";
        return tmp;
    }
}
```

程序方式： 1、实现接口类（特定参数检查）


```
private String cause = "";
private List<String> wordList = new ArrayList<String>();
/*
 * @paramName 验证的参数名
 * @inputValue 验证的参数值
 */
public boolean check(String paramName, String inputValue) {
    //wordList.add("select");
    if(wordList == null){ //如果检测关键字列表是空，则不作检查
        return true;
    }
    if(paramName=="userID"){
        if(inputValue == null || inputValue.length() == 0){//如果参数值为空，则无需检查
            return true;
        }
        for(int i = 0; i < wordList.size(); i++){
            inputValue = inputValue.toLowerCase();//这里做，是为了不区分大小写
            if(inputValue.indexOf(wordList.get(i).toLowerCase()) >= 0){
                StringBuffer sb = new StringBuffer();
                sb.append("校验未通过，").append(paramName).append("参数中含有以下词汇：").append(wordList.get(i))
                        .append("\n位置：").append(inputValue.indexOf(wordList.get(i).toLowerCase()));
                this.cause = sb.toString();
                return false;
            }
        }
    }
    return true;
}
```

程序方式： 1、实现接口类（自定义错误信息）


```
public boolean check(String paramName, String inputValue) {
    //wordList.add("select");
    if(wordList == null){ //如果检测关键字列表是空，则不作检查
        return true;
    }
    if(inputValue == null || inputValue.length() == 0){//如果参数值为空，则无需检查
        return true;
    }
    for(int i = 0; i < wordList.size(); i++){
        inputValue = inputValue.toLowerCase();//这里做，是为了不区分大小写
        if(inputValue.indexOf(wordList.get(i).toLowerCase()) >= 0){
            StringBuffer sb = new StringBuffer();
            sb.append("参数：").append(paramName).append("检查未通过，").append("含有以下敏感词汇：
").append(wordList.get(i))
                    .append("。\n谨记：\n").append("道路千万条\n规范第一条\n数据不规范\n亲人两行泪");
            this.cause = sb.toString();
            return false;
        }
    }
    return true;
}
```

程序方式： 2、Xml内配置自定义类路径

友乾营

xml（raqsoftConfig.xml）：

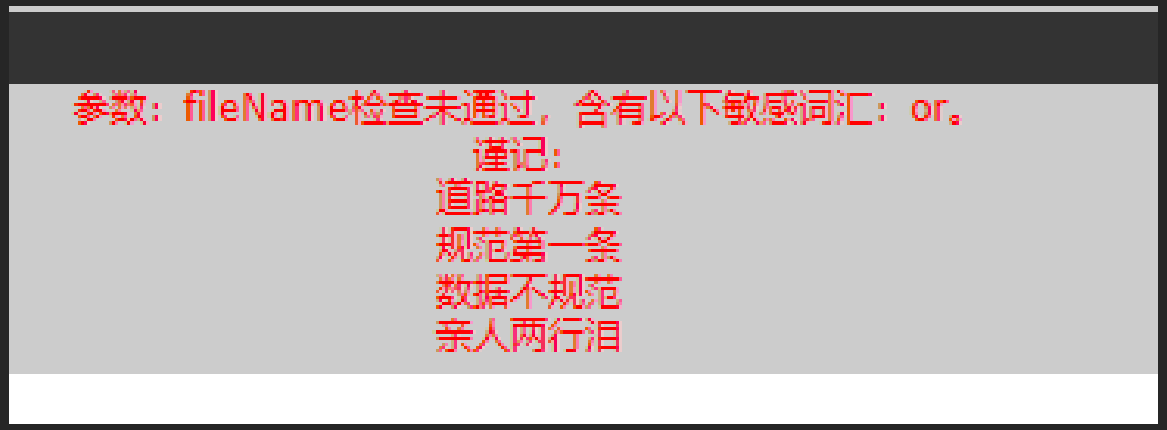
paramCheckClass设置参数值校验的类路径
<property name="paramCheckClass" value="com.raqsoft.hyl.ResistSQLInject " />

```
    <property name="raqsoftDir" value="raqsoft" />
    <property name="jspCharset" value="UTF-8" />
    <property name="cachedReportDir" value="cache/report" />
    <property name="jreInstallName" value="/jre-6u45-windows-i586.exe#Version=1,6,0,0" />
    <property name="cachedIdPrefix" value="A" />
    <property name="maxWaitTimeForReport" value="9999" />
    <property name="inputCachePath" value="cache/input" />
    <property name="alwaysReloadDefine" value="yes" />
    <property name="maxConcurrentForReport" value="9999" />
    <property name="cachedReportTimeout" value="120" />
    <property name="picFileExistTime" value="60" />
    <property name="maxWaitForReport" value="9999" />
    <property name="defDataSource" value="demo" />
    <property name="maxDatasetValueNum" value="-1" />
    <property name="logConfig" value="WEB-INF/raqsoftReportLog.properties" />
    <property name="cachedParamsTimeout" value="120" />
    <property name="theme" value="default" />
    <property name="disallowedParamWordList" value="select,from,union,union all,--" />
    <property name="paramCheckClass" value="com.raqsoft.hyl.ResistSQLInject " />
</Server>
```

报表防植入：报表工具自定义参数检查类接口

Url： http://localhost:6868/demo/reportJsp/showReport.jsp?rpx=a.rpx&arg2=华北 union select * from users

错误提示：



润乾线上直销系统

玩转好多乾（省钱攻略）

http://www.raqsoft.com.cn/wx/hdq-strategy-save.html

玩转好多乾（赚钱攻略）

http://www.raqsoft.com.cn/wx/hdq-strategy.html