

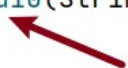
Statement vs PreStatement & SQL Injection

Experiment 1:

Add a new function 'findMoviesByTitleLimited10' in interface file

Step1: add function in interface

```
public interface DataManipulation {  
  
    public int addOneMovie(String str);  
    public String allContinentNames();  
    public String continentsWithCountryCount();  
    public String FullInformationOfMoviesRuntime(int min, int max);  
    public String findMovieById(int id);  
    public String findMoviesByTitleLimited10(String title);  
  
}
```



Step2: add realization functions in DatabaseManipulation/FileManipulation class.



```
@Override  
public String findMoviesByTitleLimited10(String title) {  
    return null;  
}
```



```
@Override  
public String findMoviesByTitleLimited10(String title) {  
  
    return null;  
}
```

Experiment 2:

Test statement versus prestatement in realization function of DatabaseManipulation class

Step1:Create a SQL to achieve

```
select m.title, c.country_name country, m.runtime,m.year_released
from movies m join countries c on m.country = c.country_code
where m.title like '%||'ah'||%'limit 10;
```

Step2:Complete the fuction

```
@Override
public String findMoviesByLimited10(String title) {
    getConnection();    // start connection
    String sql = "select m.title, c.country_name country,
m.runtime,m.year_released\n"+
        "from movies m join countries c on m.country = c.country_code\n"+
        "where m.title like '%||"+title+"||%'limit 10;";// string
    combination
    try {
        Statement statment = con.createStatement();
        resultSet = statment.executeQuery(sql);

        StringBuilder strb=new StringBuilder(); //combine multi-strings
        while (resultSet.next()){
            strb.append(String.format("%-20s\t",
resultSet.getString("country")));
            strb.append(resultSet.getInt("year_released")).append("\t");
            strb.append(resultSet.getInt("runtime")).append("\t");
            strb.append(resultSet.getString("title")).append("\n");
        }
        return strb.toString();
    } catch (SQLException throwables) {
        throwables.printStackTrace();
    }
    finally {
        closeConnection();    // close connection
    }
    return null;
}
```

Step3:Add output in client file , run client, and get the result.

```
System.out.println(dm.findMoviesByLimited10("'aba'"));
```

Step4:Test SQL Injection (Cheerful, aha!). A table will be deleted in database, you should rebuild again.

```
System.out.println(dm.findMoviesByLimited10("'aba';drop table movies;--"));
```

Step5:Change Prestatement instead of statement

```

@Override
public String findMoviesByLimited10(String title) {
    getConnection();    // start connection
    String sql = "select m.title, c.country_name country,
m.runtime,m.year_released\n"+
        "from movies m join countries c on m.country =
c.country_code\n"+
        "where m.title like '%'||?||'%'limit 10;";// string combination
    try {
        PreparedStatement preparedStatement = con.prepareStatement(sql);//
change here!
        preparedStatement.setString(1, title);// change here!
        resultSet = preparedStatement.executeQuery();// and here!

        StringBuilder strb=new StringBuilder(); //combine multi-strings
        while (resultSet.next()){
            strb.append(String.format("%-20s\t",
resultSet.getString("country")));
            strb.append(resultSet.getInt("year_released")).append("\t");
            strb.append(resultSet.getInt("runtime")).append("\t");
            strb.append(resultSet.getString("title")).append("\n");
        }
        return strb.toString();
    } catch (SQLException throwables) {
        throwables.printStackTrace();
    }
    finally {
        closeConnection(); // close connection
    }
    return null;
}

```

Step6:Test step 4 in client file again, and watch the result.

```
system.out.println(dm.findMoviesByLimited10("'aba';drop table movies;--"));
```

Step7:Test following language in client file, and watch the result.

```
System.out.println(dm.findMoviesByLimited10("aba"));
```