java代码审计深度解析

第四课 mybatis-like-in注入防护

SQL注入-Mybatis

#{}　　预处理

```
<select id="selectByPrimaryKey" resultMap="BaseResultMap" parameterType="java.lang.Integer'
    select
    <include refid="Base_Column_List" />
    from tb_admin
    where id = #{id,jdbcType=INTEGER}
</select>
```

PreparedStatement预处理

SQL注入-Mybatis—like防注入

Mysql:

```
select * from t_user where name like concat('%', #{name}, '%')
```

Oracle:

```
select * from t_user where name like '%' || #{name} || '%'
```

Sql Server:

```
select * from t_user where name like '%' + #{name} + '%'
```

SQL注入-Mybatis—in防注入

```
<if test="paramBrands != null" >
and brand.brand_id in
<foreach collection="paramBrands" item="perBrand" open="(" close=")" separator=",">
#{perBrand.brandId}
</foreach>
</if>
```

SQL注入-Mybatis—like防注入

Mysql:

```
select * from t_user where name like concat('%', #{name}, '%')
```

Oracle:

```
select * from t_user where name like '%' || #{name} || '%'
```

Sql Server:

```
select * from t_user where name like '%' + #{name} + '%'
```

谢谢观赏