



java代码审计 深度解析

第一课 mybatis-sql注入漏洞分析

免责声明
DISCLAIMER

本课程仅限于学习交流，请严格遵守国家法律法规！如利用技术从事违法活动，后果自负！



PART 01

Mybatis、iBatis链接方
式—sql注入



SQL注入-Mybatis

`#{}`

直接拼接

```
<select id="selectByPrimaryKey" resultMap="BaseResultMap" parameterType="java.lang.String" >
  select
  <include refid="Base_Column_List" />
  from tb_admin
  where username = #{username}
</select>
```

Statement不能防止sql注入



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



The image features a central figure of a person wearing a black hoodie, with their right hand pressed against their forehead in a gesture of stress or contemplation. The background is a vibrant blue digital landscape. It includes a glowing globe on the right side, a network of interconnected nodes and lines, and several padlock icons scattered throughout, suggesting themes of cybersecurity or digital privacy. The overall aesthetic is futuristic and high-tech.

谢谢观赏