链滴

《阿里巴巴 Java 开发手册》四、安全规约

作者：junjiecheng
原文链接：https://ld246.com/article/1534226969112
来源网站：链滴

1.【强制】隶属于用户个人的页面或者功能必须进行权限控制校验。

说明：防止没有做水平权限校验就可随意访问、修改、删除别人的数据，比如查看他人的私信内容、改他人的订单。

2.【强制】用户敏感数据禁止直接展示，必须对展示数据进行脱敏。

说明：查看个人手机号码会显示成:158****9119，隐藏中间 4位，防止隐私泄露。

3.【强制】用户输入的 SQL参数严格使用参数绑定或者 METADAT字段值限定，防止 SQL注入，

禁止字符串拼接 SQL访问数据库。

4.【强制】用户请求传入的任何参数必须做有效性验证。

说明：忽略参数校验可能导致：

 page size过大导致内存溢出

 恶意 order by导致数据库慢查询

 任意重定向

 SQL注入

 反序列化注入

 正则输入源串拒绝服务 ReDoS

说明：Java 代码用正则来验证客户端的输入，有些正则写法验证普通用户输入没有问题，但是如果攻人员使用的是特殊构造的字符串来验证，有可能导致死循环的结果。

5.【强制】禁止向 HTML页面输出未经安全过滤或未正确转义的用数据。

6.【强制】表单、AJAX提交必须执行 CSRF安全过滤。

说明：CSRF(Cross-site request forgery)跨站请求伪造是一类常见编程漏洞。对于存在CSRF漏洞的用/网站，攻击者可以事先构造好 URL，只要受害者用户一访问，后台便在用户不知情情况下对数据中用户参数进行相应修改。

7.【强制】在使用平台资源，譬如短信、邮件、电话、下单、支付，须实现正确的防重放限制，

如数量限制、疲劳度控制、验证码校验，避免被滥刷、资损。

说明：如注册时发送验证码到手机，如果没有限制次数和频率，那么可以利用此功能骚扰到其它用户并造成短信平台资源浪费。

8.【推荐】发贴、评论、发送即时消息等用户生成内容的场景必须实防刷、文本内容违禁词过滤等风控策略。