ch13 应用安全

沙之洲 2020012408

1 请解释XSS攻击的原理，简述一种防御方法并简单分析原因

XSS Cross-Site Scripting 跨站脚本攻击。攻击之二通过往 Web 页面里插入恶意可执行的网页脚本代码，当其他用户浏览被攻击的 Web 页面的时候，嵌入其中的恶意代码就会被执行，从而达到攻击者窃取，侵犯其他用户隐私的目的。一般分为两种攻击类型

- 反射型 XSS 攻击，也称非持久型 XSS 攻击：攻击者通过发送 URL 连接或者我Web 页面给受害者，诱骗受害者点击加载运行恶意脚本代码
- 存储型 XSS，也成为持久型 XSS 攻击：攻击者利用往回走哪漏洞，将可执行代码永久存储在服务器中，任何一个访问被攻击网站的用户都有可能会执行恶意代码。

可以通过 转义字符防御 的方式对 XSS 攻击进行防御。该方法是对用户的输入输出进行转义处理，避免它们组合成控制指令，被攻击者利用。

2 请解释SQL注入攻击的基本原理和防御的基本原理

SQL 注入的攻击原理是因为 Web 应用对用户输入数据的合法性没有判断或者进行过滤的时候不严格，攻击者利用这一漏洞在实现定义好的查询语句后添加额外的 SQL 语句，欺骗数据库进行非授权的查询，进而得到非公开的数据信息。

防御的基本原理是将数据和代码分离，具体有四种方法：

1. 后端进行严格的输入代码检查。具体来说，使用正则表达式进行一些匹配处理。
2. 对于特殊字符进行转义处理。
3. 参数化查询接口，不让用户直接向 SQL 语句中输入变量。
4. 限制网络应用对数据库的操作权限，给用户提供能满足其需求的最低权限。