网络空间安全导论 · Ch13

计01　容逸朗　2020010869

Q1.

请解释 XSS 攻击的原理，简述一种防御方法并简单分析原因。

- **攻击原理：**恶意攻击者往 Web 页面里插入恶意可执行网页脚本代码，然后用户浏览该页时嵌入其中 Web 里面的脚本代码会被执行，这样攻击者便可以盗取用户信息或完成其他侵犯用户安全隐私的目的。
- **防御方法：**使用转义字符，对于引号、尖括号、斜杠进行转义，通常采用白名单过滤的办法。这是因为攻击者会利用一些特殊的符号来让代码崩溃，但是通过转义后，某些符号仍能正常显示（如 `&lt` 可以显示为 `<`），但是不会被视为是程序的一部分，这样可以防御部分的 XSS 攻击。

Q2.

请解释 SQL 注入攻击的基本原理和防御的基本原理。

- **攻击原理：**网络应用程序对用户输入数据的合法性没有判断或过滤不严，导致攻击者可以在 web 应用程序中事先定义好的查询语句的结尾上添加额外的 SQL 语句，从而盗取数据库中特定的数据信息。
- **防御原理：**将数据与代码分离。例如后端要检查数据是否符合预期，对特殊字符做转义处理，还应该避免直接拼接 SQL 语句，同时需要严格控制 Web 应用对数据库的操作权限。