**一、常见web安全性问题：**

**SQL注入：**

SQL注入攻击指的是通过构建特殊的输入作为参数传入Web应用程序，而这些输入大都是SQL语法里的一些组合，通过执行SQL语句进而执行攻击者所要的操作，其主要原因是程序没有细致地过滤用户输入的数据，致使非法数据侵入系统。

根据相关技术原理，SQL注入可以分为平台层注入和代码层注入。前者由不安全的数据库配置或数据库平台的漏洞所致；后者主要是由于程序员对输入未进行细致地过滤，从而执行了非法的数据查询。

**防止SQL注入的方法：**

　　1. 不要信任用户的输入。对用户的输入进行校验，可以通过正则表达式，或限制长度；对单引号和双"-"进行转换过滤等。

　　2. 不要使用动态拼装sql，可以使用参数化的sql或者直接使用存储过程进行数据查询存取。（不要拼sql，使用参数化）

　　3. 不要使用管理员权限的数据库连接，为每个应用使用单独的权限有限的数据库连接。（给程序分配合理的数据库操作权限）

　　4. 不要把机密信息直接存放，加密或者hash掉密码和敏感的信息。（敏感信息加密）

　　5. 应用的异常信息应该给出尽可能少的提示，最好使用自定义的错误信息对原始错误信息进行包装。

**跨站脚本攻击（XSS）：**

跨站脚本攻击(Cross Site Scripting)，为不和层叠样式表(Cascading Style Sheets, CSS)的缩写混淆，故将跨站脚本攻击缩写为XSS。恶意攻击者往Web页面里插入恶意Script代码，当用户浏览该页之时，嵌入其中Web里面的Script代码会被执行，从而达到恶意攻击用户的特殊目的，比如获取用户的Cookie，导航到恶意网站，携带木马等。