第十六章：安全性工程

列出至少 3～5 种电子商务系统中的安全风险：

1、数据泄露和隐私问题：电子商务系统处理大量敏感用户数据，包括个人身份信息、支付信息等。如果系统存在漏洞或不当配置，黑客可能能够访问这些数据，导致用户信息泄露和隐私问题。为了减少这种风险，电子商务系统应采取合适的访问控制和身份验证措施，加密存储和传输敏感数据，并且进行定期的安全漏洞扫描和渗透测试。

2、跨站脚本攻击（XSS）：XSS 攻击是指攻击者通过在网页中注入恶意代码来获取用户敏感信息或窃取用户会话信息。电子商务系统如果没有足够的输入验证和输出编码，可能容易受到 XSS 攻击。为了防止 XSS 攻击，系统应对用户的输入进行有效的过滤和转义，确保不会被解释为可执行的代码。同时，使用安全的浏览器策略，如 CSP（Content Security Policy）也能提供额外的保护。

3、注入攻击：注入攻击是指黑客通过将恶意代码注入到应用程序中的输入字段，从而破坏数据库或执行未经授权的操作。例如，SQL 注入攻击可以导致数据库信息泄露或篡改。为了防止注入攻击，应使用参数化查询或预编译语句来处理数据库查询，避免将用户输入直接拼接到查询语句中。同时，对于其他类型的注入攻击，如命令注入和 LDAP 注入等，也需要进行相应的输入验证和过滤。

4、跨站请求伪造（CSRF）：CSRF 攻击是一种利用用户在已登录的状态下发起的未经授权的请求的攻击。黑客通过诱使用户点击恶意链接或访问恶意网站，从而执行未经授权的操作，如更改密码、购买商品等。为了防止 CSRF 攻击，可以使用 CSRF 令牌来验证每个请求的合法性，并在页面中设置适当的 SameSite 和 HTTP Referer 策略，以限制跨站请求。

5、不安全的支付和交易处理：电子商务系统涉及在线支付和交易处理，因此必须具备安全的支付机制和保护用户支付信息的能力。如果支付过程存在漏洞，黑客可能窃取用户的支付信息或欺诈用户。为了确保支付安全，电子商务系统应该采用加密的传输协议（如 HTTPS），使用安全的支付网关和第三方支付服务提供商，并遵循 PCI DSS（Payment Card Industry Data Security Standard）等支付行业标准。