用户认证

密码复杂性

会话管理

访问控制

输入数据验证

输出编码

安全传输/网络层安全

文件上传

错误处理

记录和审计

加密

Cookie管理

未经验证的重定向和转发备忘单

SQL注入

跨站脚本

跨站请求伪造

防止恶意网站框架（ClickJacking）

不安全的直接对象引用