Java安全知识

# 一、会话标识未更新

**1、会话标识未更新**

|  |  |
| --- | --- |
| 严重性: | 中 |
| 类型: | 应用程序级别测试 |
| WASC 威胁分类: | 会话定置 |
| CVE 标识: | 不适用 |
| CWE 标识: | 613 |
| 安全风险: | 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务 |

修订建议

[一般](http://blog.csdn.net/javaee_ssh/article/details/23255303)

始终生成新的会话，供用户成功认证时登录。 防止用户操纵会话标识。 请勿接受用户浏览器登录时所提供的会话标识

每次请求登陆的action或servlet时清空cookie 生成新的session

**[java code]**

try {

    log.debug("sessionId1 = " + request.getSession().getId());

    request.getSession().invalidate();

    log.debug("sessionId2 = " + request.getSession(true).getId());

    if (request.getCookies() != null) {

         Cookie cookie = request.getCookies()[0];// 获取cookie

         cookie.setMaxAge(0);// 让cookie过期

    }

} catch (Exception e) {

      e.printStackTrace();

}

session = request.getSession(true);