**应** **用** **系** **统** **威** **胁** **建** **模** **指** **南**

**目** **录**

[1 威胁建模流程 ...................................................3](#_bookmark1)

[2 应用程序分解 ...................................................3](#_bookmark2)

[3 识别威胁.......................................................4](#_bookmark3)

[4 安全检查.......................................................4](#_bookmark4)

1 威胁建模流程

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | 威胁建模流程 |  |  | | --- | | 1. 识别资产 |  |  | | --- | | 2. 创建体系结构概述 |  |  | | --- | | 3. 分解应用程序 |  |  | | --- | | 4. 识别威胁 |  |  | | --- | | 5. 记录威胁 |  |  | | --- | | 6. 分级威胁 | |

图 1 威胁建模流程

2 应用程序分解

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 应用程序分解  安全配置文件  信任边界  输入检查  会话管理  数据流  验证  加密  入口点  授权  参数操作  特权代码  配置管理  异常管理  敏感数据  审计   |  |  |  |  | | --- | --- | --- | --- | |  | | | | |  | |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | | |  |  | |

图 2 应用程序分解

3 识别威胁

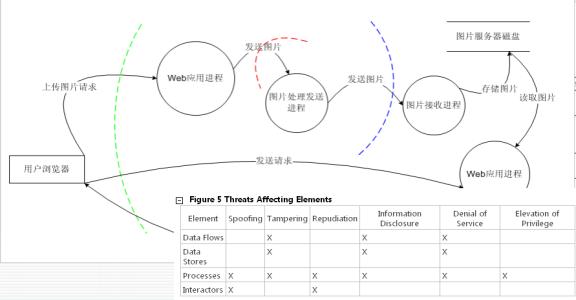


图 3 识别威胁

4 安全检查

|  |  |
| --- | --- |
| **检查类别** **检查内容** | |
| **输入** | 是否使用了数据库？是否将用户的输入直接作为参数来操作数据库？用户可以 执行什么类型的操作？ |
| 是否将用户的输入作为执行系统命令的参数？执行了什么系统命令 ？ |
| 是否将用户的输入作为代码来执行？执行了什么操作 ？ |
| 是否允许用户上传文件？可以上传什么类型的文件？上传到什么地方 ？ |
| 是否会使用用户的输入作为文件操作的参数？执行了什么操作 ？ |
| 是否会使用用户输入的 URL 作为跳转地址 ？ |
| 是否会使用第三方数据作为数据输入 ？用处是什么？ |
| 是否还有其它类型的数据来源 ？ |

|  |  |
| --- | --- |
| **输出** | 是否会使用用户的输入作为页面输出的数据源？输出到哪个 HTML 元素中 ？ |
| 是否允许用户输入特定的 HTML 代码 ？ |
| 是否对用户提供的 URL 进行了安全检查 ？ |
| **验证** | 需要用户登录验证吗 ？ |
| 使用什么样的验证方式？依赖集中认证系统吗 ？ |
| 是否采用登录验证码 ？是否有登录失败安全处理机制？ |
| 是否要求使用严格的账户策略 ？ |
| **远程管理** | 是否支持远程管理 ？ |
| 是否支持对管理地址进行限制 ？ |
| 采用了什么样的认证方式 ？ |
| 是否会与用户数据进行交换？ |
| **授权** | 对关键资源、 URL 是否实施了权限检查 ？ |
| 关键操作是否通过 POST 请求？是否添加了 |
| **敏感数据** | 应用程序处理何种敏感数据 ？ |
| 是否加密或变换了认证信息 （密码）？ |
| 使用了何种加密类型以及如何保护加密密钥的安全 ？ |
| **会话管理** | 会话是如何维持的 ？ |
| 会话 ID 如何生成？是否用户端可以控制 ？ |
| 会话 ID 是否通过 URL 传递 ？ |
| 会话 ID 是否在登录后重新生成 ？ |
| 会话管理中是否对用户的 IP、 浏览器等其它特征作为用户标识 ？ |
| 会话用时间限制吗 ？ |

|  |  |
| --- | --- |
|  | 应用程序如何与会话存储进行验证 ？ |
| **异常处理** | 应用程序如何处理出现的错误 ？ |
| 是否允许异常信息发送至客户端 ？ |
| 错误消息是否经过安全编码后发给客户端 ？ |
| **日志审计** | 是否对用户的关键操作进行了记录 ？ |
| 如何保护日志文件的安全 ？ |