# XX 系统源代码安全审计报告

XX 部门

20XX 年 X 月

# 目 录

# 1. 源代码审计概述

## 1.1. 审计对象

*描述本文档适用范围、场景等相关的背景情况,便于读者充分了解审计对象信息.*

## 1.2. 审计目的

*描述开展源代码审计工作的目的、依据、要求以及预期效果。*

## 1.3. 审计流程

*描述源代码代码审计工作的流程,包括但不限于测试环境的搭建、测试方法或模式（例如工具测试、人工检查）、审计报告及整改方案的撰写，并明确各项工作的相关职责方。*

## 1.4. 审计组织

*描述开展代码审计工作组织情况，包括但不限于安全保密以及审计工作准备情况。*

# 2. 源代码审计范围

*描述被审计系统情况，包括但不限于源代码行数、源代码文件大小、设计语言及组件、开发软件环境、系统架构、编译器、系统类库、系统服务器及数据库等信息.*

# 3. 源代码审计详情

## 3.1. 安全风险定义

*源代码安全审计是运用工具和人工分析对源代码进行检查,检查系统软件存在的安全缺陷.根据安全缺陷可能存在的安全风险对检查中发现的各个缺陷给出了相对应的风险评价，并对风险评价中涉及到的各个等级给予一定说明和界定,如风险级别高、中、低并依次描述各级别对应威胁，示例如下:*

| ***序号*** | ***风险级别*** | ***威胁描述*** |
|---|---|---|
| *1* | *高* | *对目标系统的安全存在较大的威胁，应该立即得到修正,防止对系统带来影响，造成重大损失.如：xxxxx* |

| | | |
|---|---|---|
| *2* | *中* | *对目标系统或系统的客户端的安全有威胁， 应该及时得到修正，防止对系统带来影响，造成不必要的损失。如：xxxx* |
| *3* | *低* | *对系统造成的损失很小或很难直接被利用，但仍应该得到开发人员重视,并对其加以修改，杜绝其带来的潜在风险。如：* |

## 3.2. 安全缺陷统计

*描述本次源代码安全审计的代码行数、文件数量、已发现的安全问题总数；分类简述存在的安全问题及数量并与安全风险级别进行对应；已图表形式对发现的安全缺陷进行统计，如下所示：*

| | | | |
|---|---|---|---|
| ***可执行代码行数(行）*** | *xxxxx* | | |
| ***检查文件数量（个）*** | *xxxxx* | | |
| ***已发现安全问题（个）*** | *xxxx* | | |
| ***安全问题描述（个）*** | *隐私泄露* | *XXXX 个* | *高/中/低* |
| | *跨站脚本漏洞* | *XXXX 个* | *高/中/低* |
| | *SQL 注入* | *XXXX 个* | *高/中/低* |
| | *xxxxx* | *xxxxx 个* | |

## 3.3. 安全缺陷示例

*逐条描述本次源代码审计工作发现的相关漏洞信息及相关风险,并以图例形式清晰表明问题代码信息及位置。*

### 3.3.1. 隐私泄露

*逐条描述发现的隐私泄露缺陷个数、缺陷分析、缺陷代码实例及修复建议.*

### 3.3.2. 跨站脚本漏洞

*逐条描述发现的跨站脚本漏洞缺陷个数、缺陷分析、缺陷代码实例及修复建议。*

### 3.3.3. SQL 注入缺陷

*逐条描述发现的 SQL 注入缺陷个数、缺陷分析、缺陷代码实例及修复建议。*

### 3.3.4. XXX 缺陷

*逐条描述发现的其它缺陷个数、缺陷分析、缺陷代码实例及修复建议。*

## 4. 总结

*综合本次代码审计发现的缺陷与安全风险定义，对比分析 XX 系统中高、中、地风险情况.*