《软件安全设计》
实验报告

姓　　名	
班　　级	
开 设 学 期	
实 验 题 目	
实 验 日 期	
评 定 成 绩	

东北大学软件学院

一、题目背景

某高校需开发一套学生成绩管理系统（提示：核心功能包括学生基础信息管理（学生网上注册完成）、教师基础信息管理（由系统导入）、课程基础信息管理（由系统导入）、成绩管理、系统管理、审计管理等，其他功能可以自行设计），该系统通过 Web 方式提供相关成绩服务。

请完成如下任务要求：

1. 对该系统进行软件安全需求分析(15 分)

a) 给出一个误用用例图，包含 5 个以上误用用例。(7 分)

b) 画出 2 个滥用用例图，每个用例图包含 3 个以上滥用用例。(8 分)

2. 给出系统的数据流，并进行威胁建模。（20 分）

a) 数据流图。(10 分)

b) 画出 2 棵威胁树，并给出对应的威胁表。(10 分)

作业要求：

（1）利用 VISO 或其他绘图工具完成，不能手绘，手绘成绩为零分；

（2）作业按照 Word 或 PDF 版本提交，图片可以嵌入到 Word 或 PDF 文档中，作业命名格式：学号-姓名-班级；

（3）作业提交时间：4 月 30 日晚 17：00 之前提交个各班学委，各班学委收集齐后，将压缩文档发送到 124335062@qq.com 邮箱，逾期取消该项作业成绩。

二、系统用例图

为了对该系统进行软件安全需求分析，首先需要绘制该系统的用例图。

用例（Use Case）是软件工程中对系统如何反应外界请求的描述，是一种通过用户的使用场景来获取需求的技术。

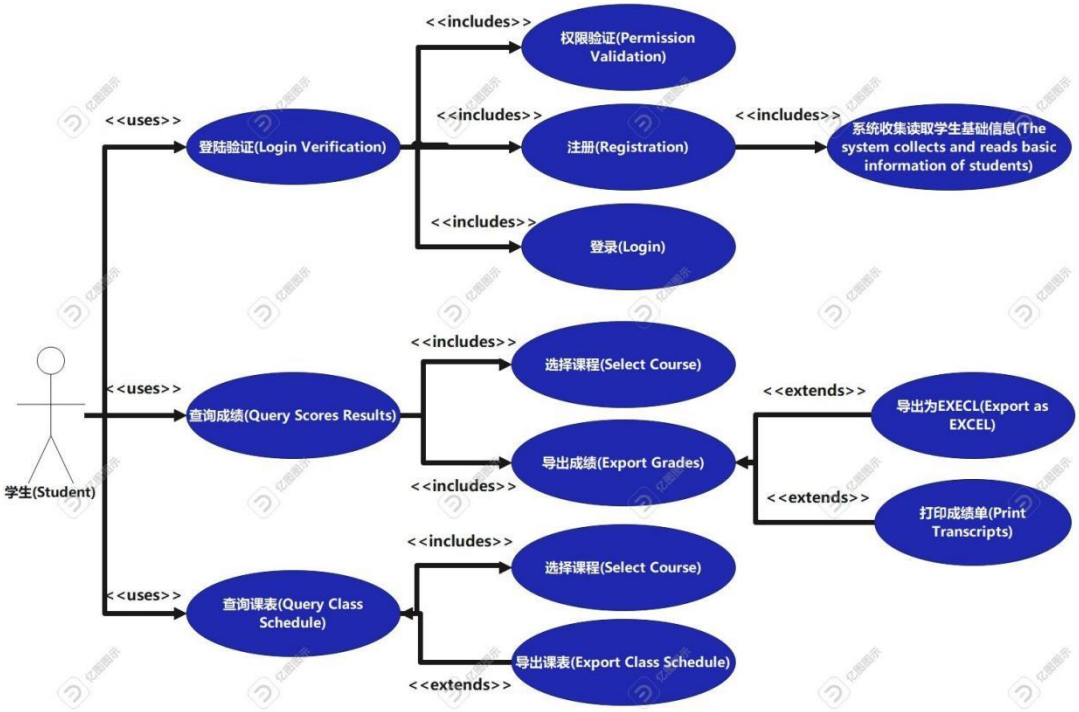
用例包括确定动作者（访问主体）、预期的系统行为（使用用例）、执行序列，以及动作者和使用用例之间的关系。动作者可能是一个个体、一个角色或非自然人，例如一个人、管理员或后台批处理过程都可能是一个动作者。

用例可以帮助软件开发人员规范地描述软件或系统的预期行为，即，通过用例描述用户的预期行为，而预期行为则描述了完成业务功能所需要的行为和事件的顺序。

用例是软件产品使用者（参与者）和软件产品本身之间的交互。

参与者（Actor）：与软件产品发生关联的人，包括软件的使用者，某项业务的发起者和用例中起到关键作用的人。

在本题目中，相关的用例图的参与者有学生(Student)，教师(Teacher)和管理员(Administrator)(更加清晰的版本见附件)：

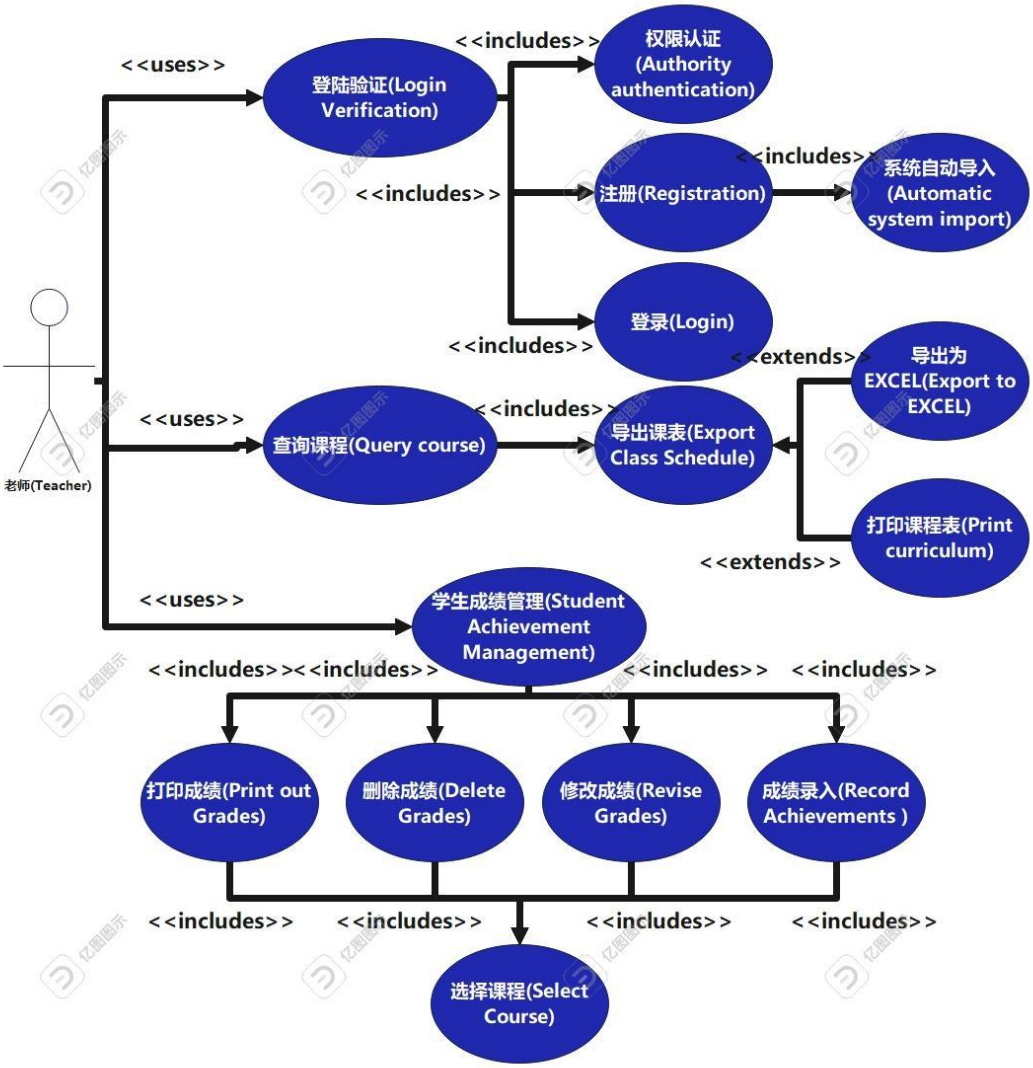


参与者 1：学生(Student)。学生包含 3 个主要用例：登陆验证、查询成绩和查询课表。

登陆验证包含 3 个子用例：权限验证、注册和登录。其中权限验证作用是判断用户权限，如果用户权限为学生，则按照学生权限开放相关功能；注册需要学生手动输入信息，系统收集。

查询成绩包含 2 个子用例：选择课程和导出成绩。导出成绩有两个扩展子用例，分别是导出成绩为 excel 文件和打印成绩单。

查询课表包含 1 个子用例选择课程，和 1 个扩展子用例导出课表。

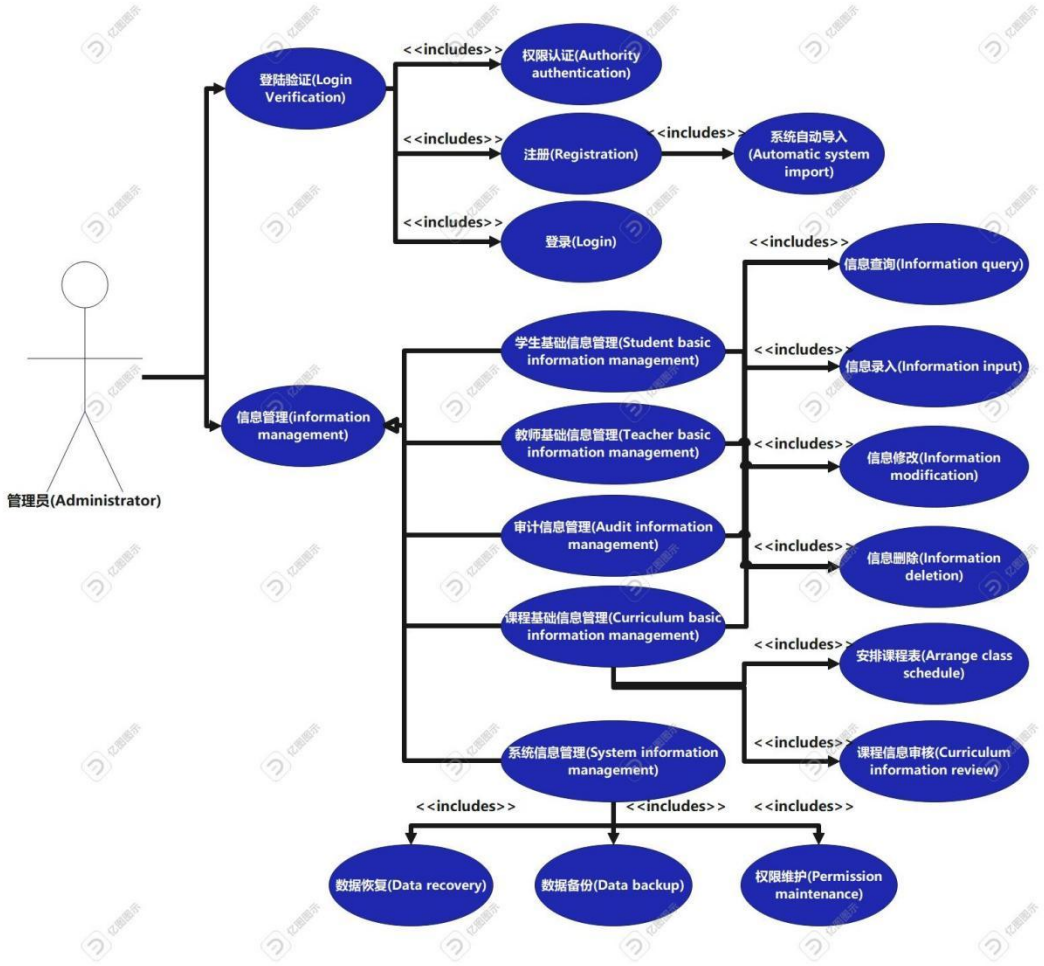


参与者 2：教师(Teacher)。教师包含 3 个主要用例：登陆验证、查询课程和学生成绩管理。

登陆验证包含三个子用例：权限验证、注册和登录。其中权限验证作用是判断用户权限，如果用户权限为教师，则按照教师权限开放相关功能；注册不需要教师手动输入信息，系统自动导入。

查询课程包含 1 个子用例：导出课表。导出课表有 2 个扩展子用例，分别是导出课表为 excel 文件和打印课表。

学生成绩管理包含 4 个子用例：打印成绩、删除成绩、修改成绩和成绩录入。同时，这 4 个子用例又包含 1 个子用例：选择课程。



参与者 3：管理员(Administrator)。管理员包含 2 个主要用例：登陆验证和信息管理。

登陆验证包含三个子用例：权限验证、注册和登录。其中权限验证作用是判断用户权限，如果用户权限为管理员，则按照管理员权限开放相关功能；注册不需要管理员手动输入信息，系统自动导入。

信息管理是一个父类用例，其拥有 5 个子用例：学生基础信息管理、教师基础信息管理、审计信息管理、课程基础信息管理和系统信息管理。其中学生基础信息管理、教师基础信息管理、审计信息管理和课程基础信息管理均包含 4 个子用例：信息查询、信息录入、信息修改和信息删除。课程基础信息管理还拥有额外的 2 个子用例：安排课程表和课程信息审核。系统信息管理包含 3 个子用例：数据恢复、数据备份和权限维护。

三、系统滥用用例图

传统用例分析方法只能用于分析获取软件系统的功能性需求，无法获取软件的安全需求。

开发安全的软件，软件开发人员要更多考虑意外或反常的行为，这样才能更好地理解如何创建安全的软件。

滥用用例（Abuse Case）和误用用例（Misuse Case）对传统用例分析方法的扩展，弥补了传统用例分析方法在获取软件安全需求方面的缺陷。

其主要思想为：帮助软件开发人员将软件置于敌手环境（受攻击状态）中，从攻击者的角度考虑系统面临的威胁，对软件在运行过程中可能面临的非期望的、非标准的情况进行描述性陈述，分析系统存在的安全漏洞，建立威胁用例，针对威胁用例建立安全需求用例，进而达到减少攻击者可利用漏洞的目的。

通过分析软件可能面临的常见攻击，可以有效地捕获误用和滥用用例。

1. 滥用用例

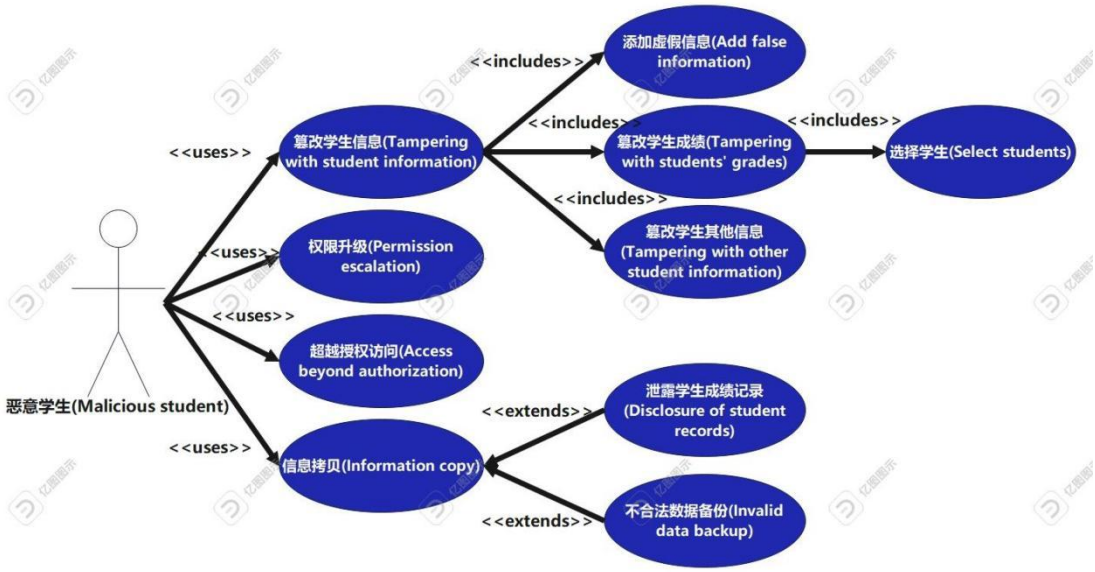
滥用用例是对系统与一个或多个参与者之间的具有破坏性的交互行为的描述，即，交互行为的结果对系统、某个参与者或系统利益相关者是有害的。不能仅根据参与者与系统之间的交互来定义滥用行为，而是必须根据交互过程所造成的实际损害来对滥用进行定义。

滥用用例是在用例基础上，通过对负面场景（即不是系统预期的行为，而是一个不希望在正常使用用例情境中发生的动作）进行建模，来捕获攻击者与系统之间的交互所产生的威胁，进而确定安全威胁和安全需求内容。

滥用安全例构建过程：

- Step 1. 描述参与者和用例。
- Step 2. 引入主要的滥用者和滥用用例。
- Step 3. 研究滥用用例和用例之间潜在的 include（包含）关系。
- Step 4. 引入新的用例来发现或阻止滥用用例。
- Step 5. 形成更加详细的需求记录。

根据已经完成的学生成绩管理系统用例图，通过分析，我们可以绘制出学生成绩管理系统滥用用例图，参与者分别是恶意学生(Malicious student)和恶意黑客组织(Malicious hacker groups),如下图：



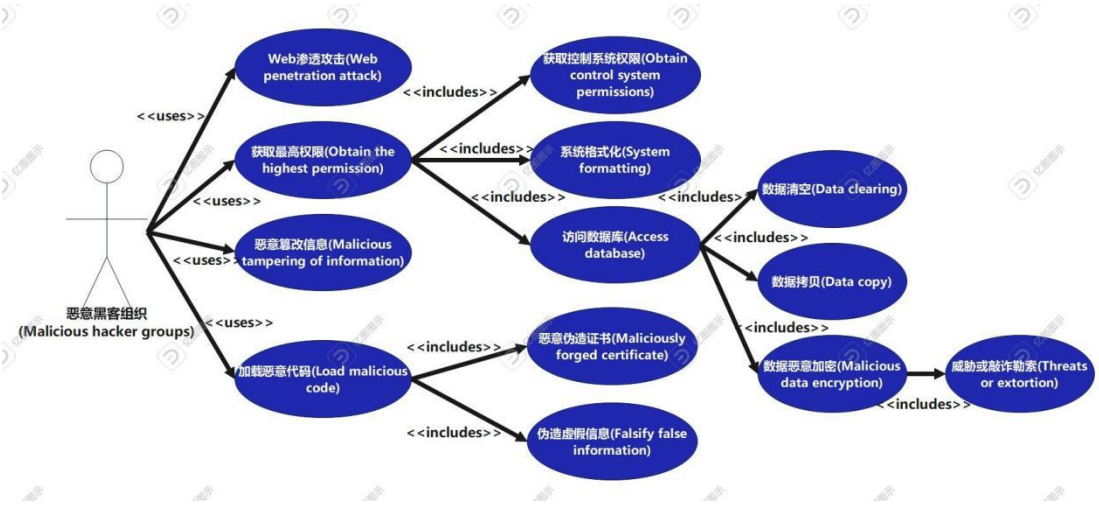
参与者 1：恶意学生(Malicious student)。恶意学生包含 4 个主要用例：篡改学生信息、权限升级、超越授权访问和信息拷贝。

篡改学生信息拥有 3 个子用例：添加虚假信息、篡改学生成绩和篡改学生其他信息。篡改学生信息指攻击者通过对学生信息进行修改，来影响学生的成绩、课程选修情况等信息。这种攻击可能会影响学生的学术成就和未来的就业前景。

权限升级指攻击者获取未授权的高级别访问权限，例如管理员或超级用户权限，从而能够执行敏感操作或窃取敏感数据。这种攻击可能会导致学生成绩、课程、学生信息等数据泄露或被篡改。

超越授权访问指攻击者利用漏洞绕过访问控制机制，从而可以访问其未被授权的资源或功能。这种攻击可能会导致攻击者能够访问或修改学生信息、成绩或敏感数据。

信息拷贝拥有 2 个扩展子用例：泄露学生成绩记录和不合法数据备份。信息拷贝指攻击者通过获取访问权限或利用其他漏洞，将学生信息、成绩或其他敏感数据复制到攻击者的系统中。这种攻击可能会导致学生的隐私受到侵犯，也可能会导致学生的成绩或其他敏感数据泄露。



参与者 2：恶意黑客组织(Malicious hacker groups)。恶意学生包含 4 个主要用例：Web 渗透攻击、获取最高权限、恶意篡改信息和加载恶意代码。

Web 渗透攻击是指攻击者通过利用 Web 应用程序中的漏洞，越过应用程序的边界进入系统内部，从而获取对系统的控制权或敏感信息的攻击行为。攻击者可以利用多种技术进行 Web 渗透攻击，如 SQL 注入、跨站脚本攻击、文件上传漏洞等。

获取最高权限包含 3 个子用例：获取控制系统权限、系统格式化和访问数据库。其中访问数据库拥有 3 个子用例：数据清空、数据拷贝和恶意数据加密。恶意数据加密又包含 1 个子用例：威胁或敲诈勒索。获取最高权限是指攻击者成功获得系统管理员或超级用户的权限，从而能够完全控制整个系统。攻击者可以利用各种漏洞或攻击技术来获取最高权限，如滥用系统漏洞、利用社会工程学手段

获取管理员账户密码等。可以利用最高权限格式化系统、访问数据库等敏感信息等，进一步获取敏感信息并威胁或敲诈勒索，造成巨大威胁。

恶意篡改信息是指攻击者通过修改或删除系统中的数据，篡改或破坏系统的正常运行。攻击者可以利用各种漏洞或攻击技术进行恶意篡改信息，如 SQL 注入、跨站脚本攻击等。

加载恶意代码拥有 2 个子用例：恶意伪造证书和伪造虚假信息。恶意伪造证书是指攻击者使用虚假证书来欺骗用户，使其认为正在与合法网站进行通信，从而达到窃取敏感信息或者篡改信息的目的;伪造虚假信息则是指攻击者伪造或篡改数据，欺骗用户或系统，达到获取非法利益、破坏系统或者误导用户等目的。加载恶意代码是指攻击者通过向系统注入恶意代码，从而在系统内部执行任意的恶意操作。攻击者可以通过利用各种漏洞或攻击技术来加载恶意代码，如通过 XSS 攻击、文件上传漏洞等。一旦恶意代码成功加载到系统中，攻击者就可以执行各种恶意操作，如窃取用户信息、篡改系统数据等。

四、系统误用用例图

对于误用用例：误用用例用于描述系统或用户所不希望发生的行为。在误用用例中，描述了系统或其他实体可以与误用用户（Misuser）交互执行的一系列动作序列，如果这些动作序列被允许，并执行完成，则会对系统的相关用户造成损害。

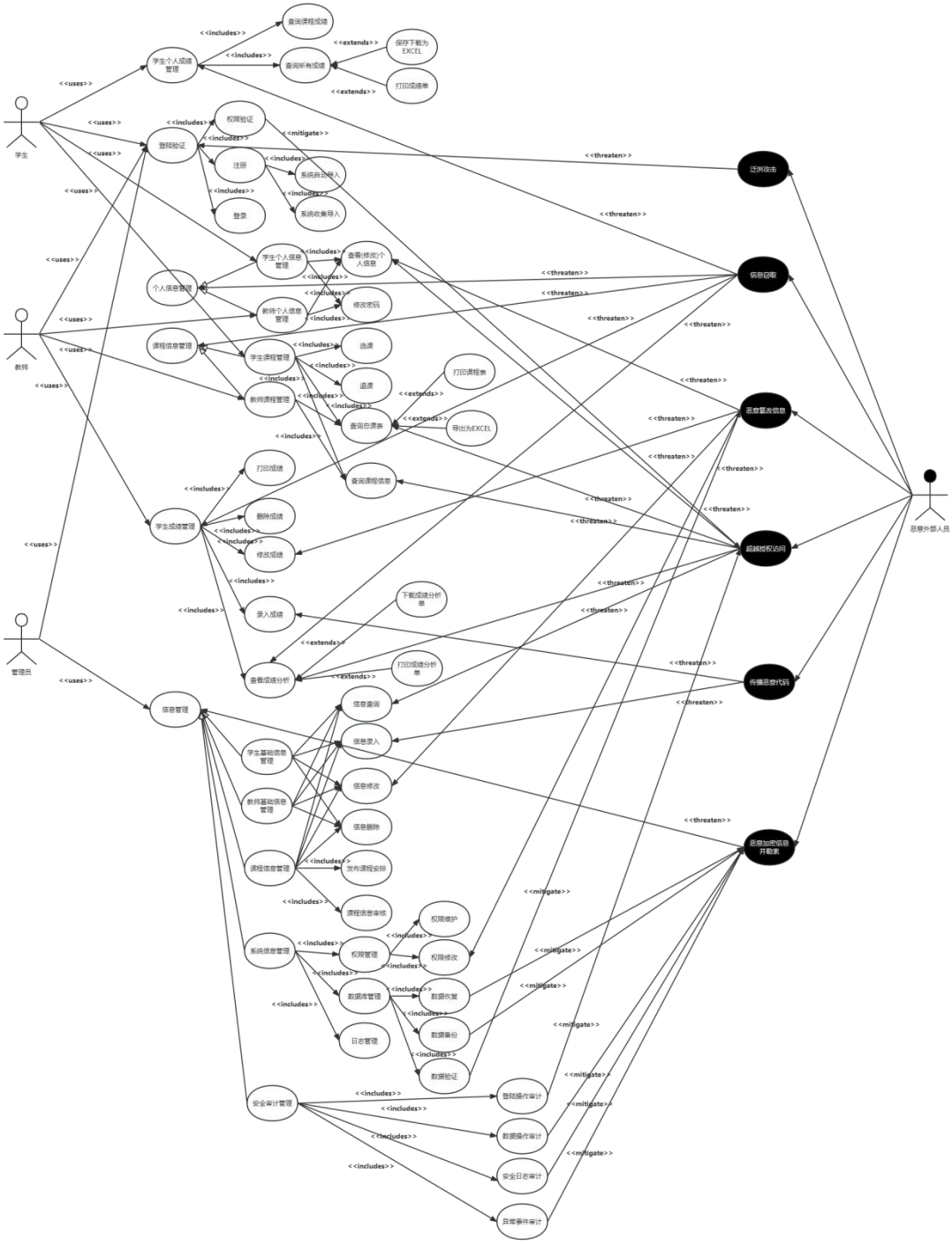
误用用户是指，有意或无意地引发误用用例的行为人。

除了标准的“include”和 “extends”关系之外，误用用例中引入了一些新的关系，误用用例和用例既可以是“威胁”关系也可以是 “消减”关系。用例可以减轻误用情况，这意味着用例减少了误用用例成功的机会。误用案例也可以威胁用例，即用例被误用用例利用或阻碍。

误用用例的构建过程：

- Step 1. 关注正常用户和他们引起的用例，例如，不考虑任何安全问题的用户需求的服务。利用 UML 方法建议的正常方式描述角色（用户）和用例。
- Step 2. 引入主要的误用用户和误用案例，例如可能发生的威胁。
- Step 3. 分析误用用例和用例的潜在关系。这一步非常重要，因为系统的许多威胁很大程度上可以通过使用系统的正常功能来实现。
- Step 4. 引入新的用例来“消减”误用用例。
- Step 5. 继续编写更详细的需求文档。

通过对学生成绩管理系统更加完善的分析，这里绘制出来了完善的学生成绩管理系统误用用例图，如下图所示(误用用例图要素太多，可能不太能看清楚，因此更加清晰的版本见附件)：



由于误用用例图要素太多，整体来看比较复杂，这里对误用用例图进行详细的解读。

1. 普通用例

误用用例图拥有以下**普通用例**：

学生个人成绩管理。学生个人成绩管理包含 2 个子用例：查询课程成绩和查询所有成绩。查询所有成绩包含 2 个扩展子用例：保存下载为 excel 和打印成绩单。

登陆验证。登陆验证包含三个子用例：权限验证、注册和登录。其中权限验

证作用是判断用户权限，如果用户权限为管理员，则按照管理员权限开放相关功能；注册不需要管理员和教师手动输入信息，系统自动导入。如果用户权限为学生，则按照学生权限开放相关功能；注册需要学生手动输入信息，系统收集。

个人信息管理是一个父类用例。学生个人信息管理和教师个人信息管理分别是它的子类用例。子类用例包含 2 个子用例：查看（修改）个人信息和修改密码。

课程信息管理是一个父类用例。学生课程信息管理和教师课程信息管理分别是它的子类用例。教师课程信息管理包含 2 个子用例：查询课程信息和查询总课表。学生课程信息管理包含 4 个子用例：选课、退课、查询课程信息和查询总课表。查询总课表包含 2 个扩展用例：打印课程表和导出为 excel。

学生成绩管理(教师)。学生成绩管理有 5 个子用例：打印成绩、删除成绩、修改成绩、录入成绩和查看成绩分析。查看成绩分析有 2 个扩展用例：下载成绩单分析和打印成绩分析单。

信息管理是一个父类用例。它的子类用例有：学生基础信息管理(管理员)、教师基础信息管理(管理员)、课程基础信息管理(管理员)、系统信息管理和安全审计管理。学生基础信息管理(管理员)、教师基础信息管理(管理员)和课程基础信息管理(管理员)均包含 4 个子用例：信息查询、信息录入、信息修改和信息删除。课程基础信息管理(管理员)还包含额外的 2 个子用例：发布课程安排和课程信息审核。系统信息管理包含 3 个子用例：权限管理、数据库管理和日志管理。权限管理包含 2 个子用例：权限维护和权限修改。数据库管理包含 3 个子用例：数据恢复、数据备份和数据验证。安全审计管理包含 4 个子用例：登陆操作审计、数据操作审计、安全日志操作审计和异常事件操作审计。

2. **误用用例**

误用用例图拥有以下**误用用例**：

泛洪攻击，信息窃取，恶意篡改信息，超越授权访问，传播恶意代码和恶意加密信息并勒索。

泛洪攻击：也称为 DoS 攻击（拒绝服务攻击），旨在通过向目标服务器发送大量流量来使其崩溃或无法正常工作。攻击者可能会使用单个计算机或多个计算机来发起攻击，这取决于攻击的规模和复杂性。

信息窃取：这种攻击旨在获取敏感信息。攻击者可以通过多种方式进行信息窃取，如钓鱼邮件、恶意软件和社会工程学攻击等。

恶意篡改信息：这种攻击旨在修改目标系统中的数据，以便满足攻击者的特定目的。攻击者可以通过多种方式进行恶意篡改信息，如 SQL 注入攻击和跨站脚本攻击等。

超越授权访问：这种攻击旨在通过绕过目标系统的身份验证和授权控制来访问未经授权的信息。攻击者可以使用多种技术进行超越授权访问，如会话劫持、缓冲区溢出和 Web 应用程序漏洞利用等。

传播恶意代码：这种攻击旨在通过向目标计算机或网络中引入恶意软件来控制受害者的系统或获取机密信息。攻击者可以使用多种途径进行传播恶意代码，如电子邮件、恶意广告和网络钓鱼攻击等。

恶意加密信息并勒索：这种攻击旨在使用加密算法将受害者的数据锁定起来，并勒索受害者支付赎金来恢复数据。这种攻击也称为勒索软件攻击。攻击者可以使用多种方式进行这种攻击，如通过电子邮件附件、恶意下载和网络钓鱼攻击等。

3. 用例关系

普通参与者 1：学生。学生包含 4 个主要用例：学生个人成绩管理、登陆验证、学生课程管理和学生个人信息管理。

普通参与者 2：教师。教师包含 4 个主要用例：学生成绩管理(教师)、登陆验证、教师课程管理和教师个人信息管理。

普通参与者 3：管理员。管理员包含 2 个主要用例：登陆验证和个人信息管理。

恶意参与者 1：恶意外部人员。恶意外部人员包含 6 个主要用例：泛洪攻击，信息窃取，恶意篡改信息，超越授权访问，传播恶意代码和恶意加密信息并勒索。

(1) 威胁关系(A==>B，表示 A 用例威胁 B 用例)：

- 泛洪攻击==>登陆验证
- 信息窃取==>学生个人信息管理
- 信息窃取==>个人信息管理
- 信息窃取==>课程信息管理
- 信息窃取==>学生成绩管理
- 信息窃取==>信息管理
- 恶意篡改信息==>查看(修改)个人信息
- 恶意篡改信息==>修改成绩
- 恶意篡改信息==>信息修改
- 恶意篡改信息==>权限修改
- 传播恶意代码==>录入成绩
- 传播恶意代码==>信息录入
- 恶意加密信息并勒索==>信息管理

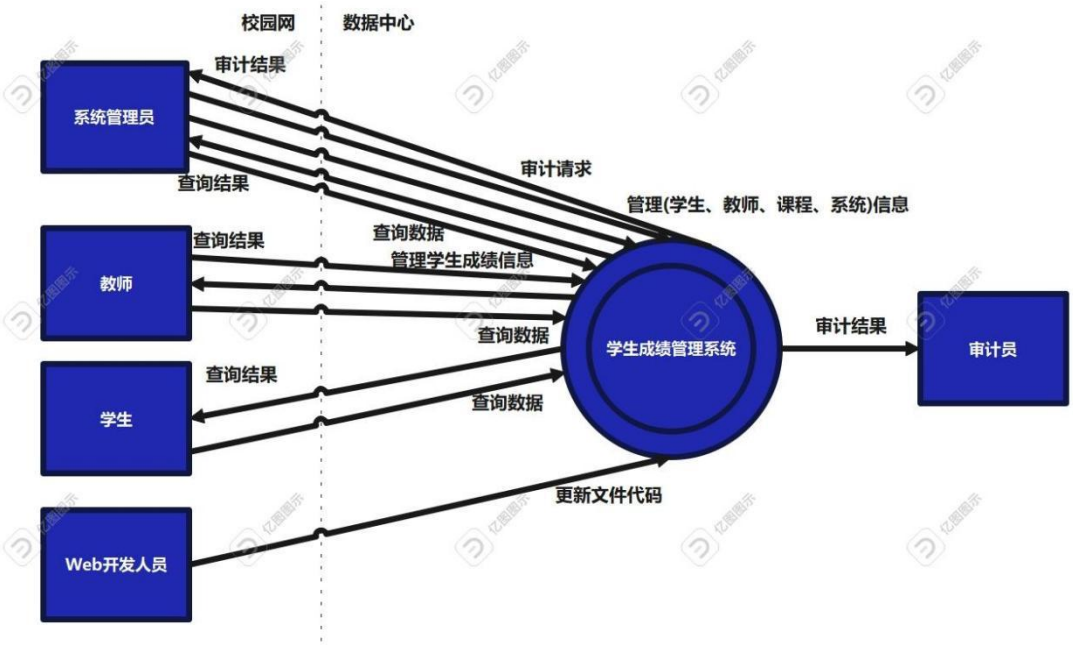
(2) 消减关系(A==>B，表示 A 用例消减 B 用例)：

- 权限验证==>超越授权访问
- 登陆操作审计==>超越授权访问
- 数据恢复==>恶意加密信息并勒索
- 数据备份==>恶意加密信息并勒索
- 数据操作审计==>恶意加密信息并勒索

- 安全日志审计==>恶意加密信息并勒索
- 异常事件审计==>恶意加密信息并勒索
- 数据验证==>恶意篡改信息

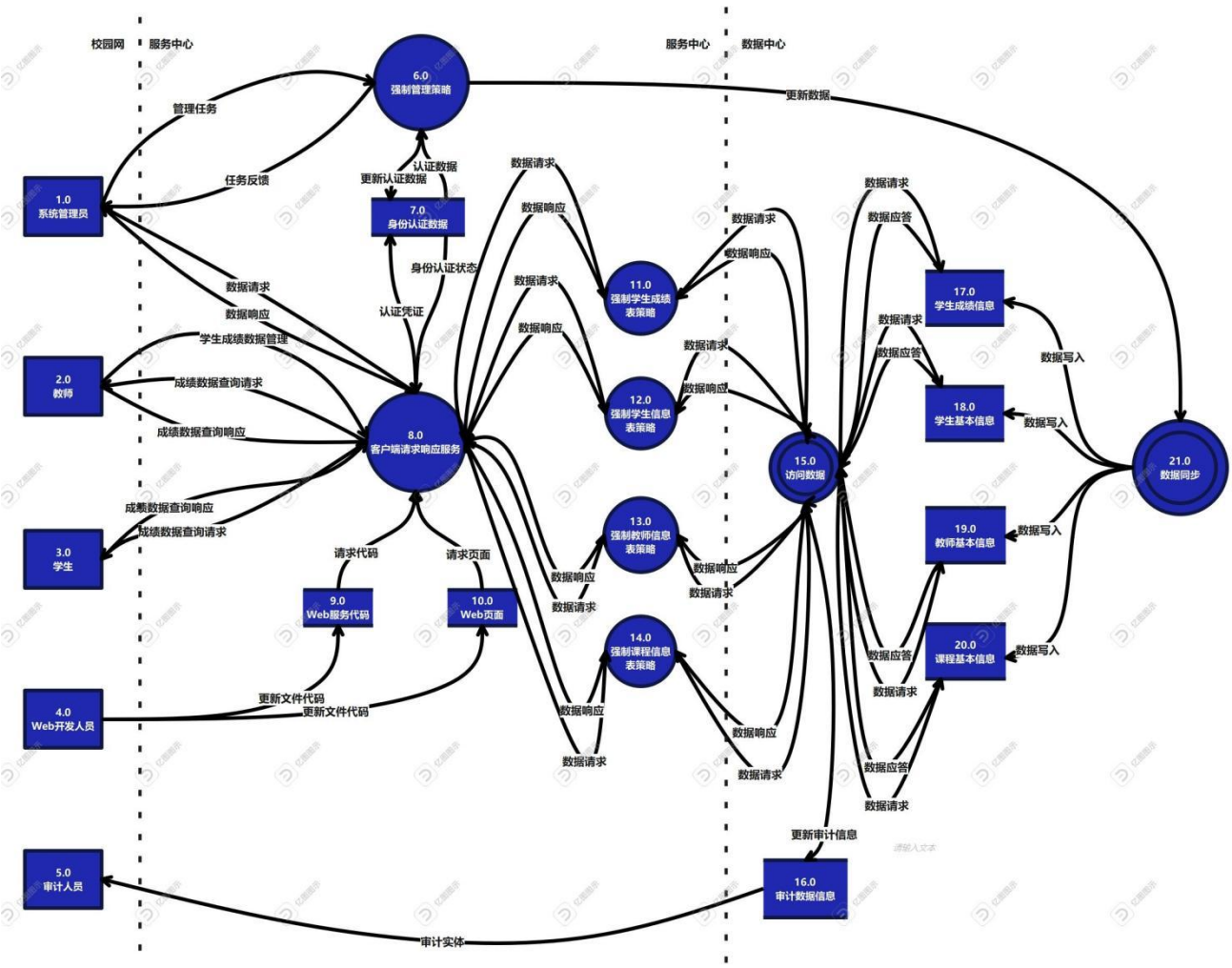
五、系统数据流图

学生成绩管理系统的顶层数据流图(更加清晰的版本见附件)：



顶层数据流图数据源点有：系统管理员、教师、学生和 Web 开发人员。数据终点有：系统管理员、教师、学生和审计员。多处理过程为学生成绩管理系统。箭头表示数据流的流向。例如，Web 开发人员将更新文件代码数据流流向学生成绩管理系统，审计员接受来自学生成绩管理系统的审计结果数据流。

学生成绩管理系统的 1 级数据流图(更加清晰的版本见附件)：



1 级数据流图显然更加复杂。数据源点有：系统管理员、教师、学生和 Web 开发人员。数据终点有：系统管理员、教师、学生和审计员。主要单次处理过程为客户端请求响应服务。该模块主要负责与数据库中的身份认证数据、Web 服务代码和 Web 页面进行数据交互。同时，该模块与多个强制表策略进行服务交互。强制表策略与其对应的数据库进行数据交互。此外，系统管理员和强制管理策略交互，强制管理策略的数据流向多次处理过程数据同步。数据同步的数据写入对应的所有数据表格。

六、系统威胁树及威胁表

1. 威胁树

威胁树（Threat Tree）起源于硬件故障识别领域常用的故障树（Fault Tree），采用树形结构描述系统面临的威胁。

威胁树的根节点表示系统所面临威胁的抽象描述，逐层细化威胁的细节信息，直到用叶节点表示具体攻击方式。

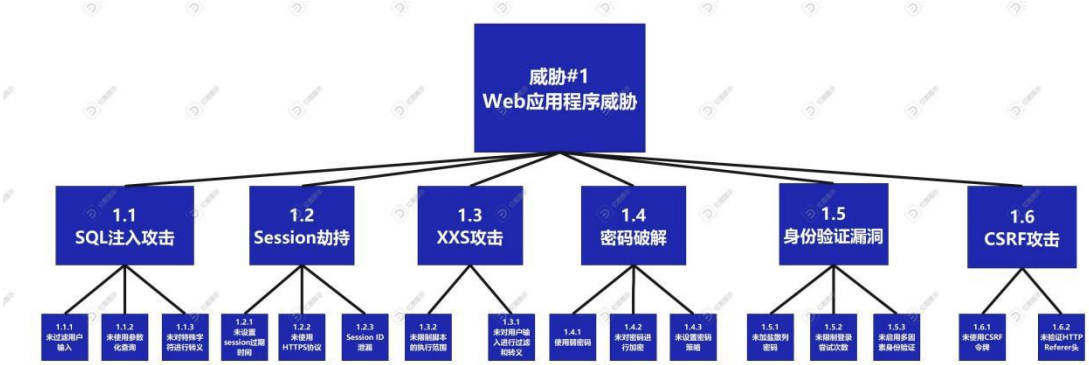
威胁树描述了攻击者破坏各组件所经历的决策过程。

威胁树主要思想：应用程序是由威胁目标构成的；每个目标都有漏洞；任何漏洞被攻击者成功利用后，都会使整个系统遭到破坏。

2. 学生成绩管理系统威胁树：

这里将学生管理系统威胁分类为 Web 应用程序威胁、内部威胁和外部威胁。总计 3 棵威胁树。

威胁树 1：



学生管理系统威胁树 1：

Web 应用程序威胁

1.1 SQL 注入攻击

1.1.1 未过滤用户输入

1.1.2 未使用参数化查询

1.1.3 未对特殊字符转义

1.2 Session 劫持

1.2.1 未设置 Session 过期时间

1.2.2 未使用 HTTPS 协议

1.2.3 Session ID 泄露

1.3 XSS 攻击

1.3.1 未对输入进行过滤和转义

1.3.2 未限制脚本的执行范围

1.4 密码破解

1.4.1 使用弱密码

1.4.2 未对密码进行加密

1.4.3 未设置密码策略

1.5 身份验证漏洞

1.5.1 未加盐散列密码

1.5.2 未限制尝试登陆次数

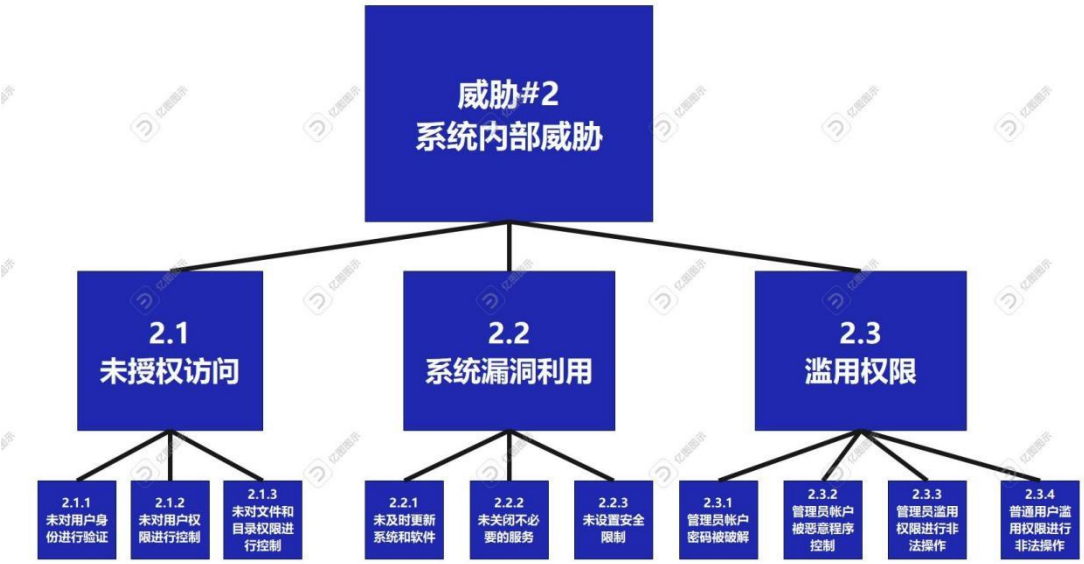
1.5.3 未启用多因素身份验证

1.6 CSRF 攻击

1.6.1 未使用 CSRF 令牌

1.6.2 未验证 HTTP Refer 头部

威胁树 2：



学生管理系统威胁树 2：

系统内部威胁

2.1 未授权访问

2.1.1 未对用户身份进行验证

2.1.2 未对用户权限进行控制

2.1.3 未对文件和目录权限进行控制

2.2 系统漏洞利用

2.2.1 未及时更新系统和软件

2.2.2 未关闭不必要服务

2.2.3 未设置安全限制

2.3 滥用权限

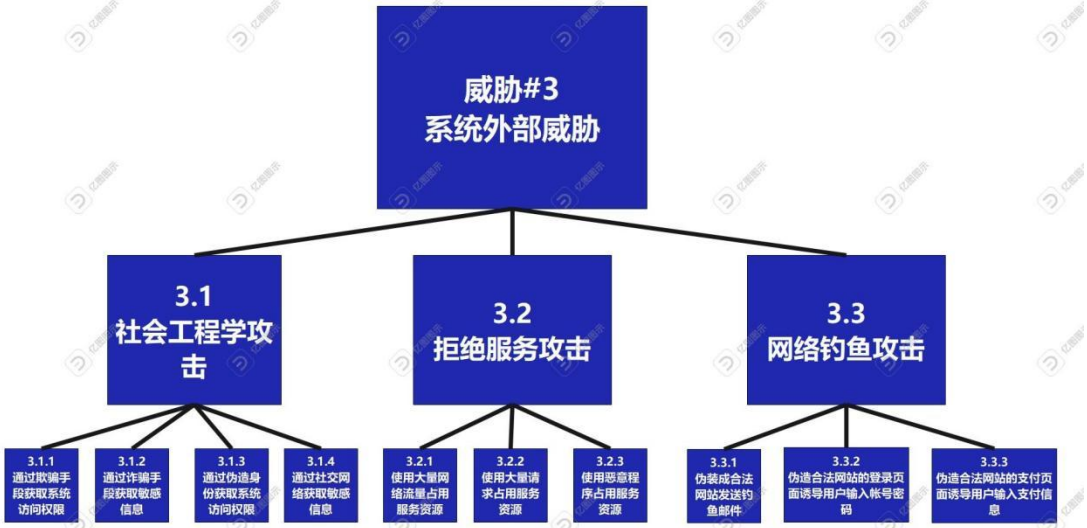
2.3.1 管理员账户被破解

2.3.2 管理员账户被恶意程序控制

2.3.3 管理员滥用权限进行非法操作

2.3.4 其他用户滥用权限进行非法操作

威胁树 3：



学生管理系统威胁树 3：

系统外部威胁

3.1 社会工程学攻击

3.1.1 通过欺骗手段获取系统访问权限

3.1.2 通过诈骗手段获取系统敏感信息

3.1.3 通过伪造身份获取系统访问权限

3.1.4 通过社交网络获取敏感信息

3.2 拒绝服务攻击

3.2.1 使用大量网络流量占用服务资源

3.2.2 使用大量请求占用服务资源

3.2.3 使用恶意程序占用服务资源

3.3 网络钓鱼攻击

3.3.1 伪装成合法网站发生钓鱼邮件

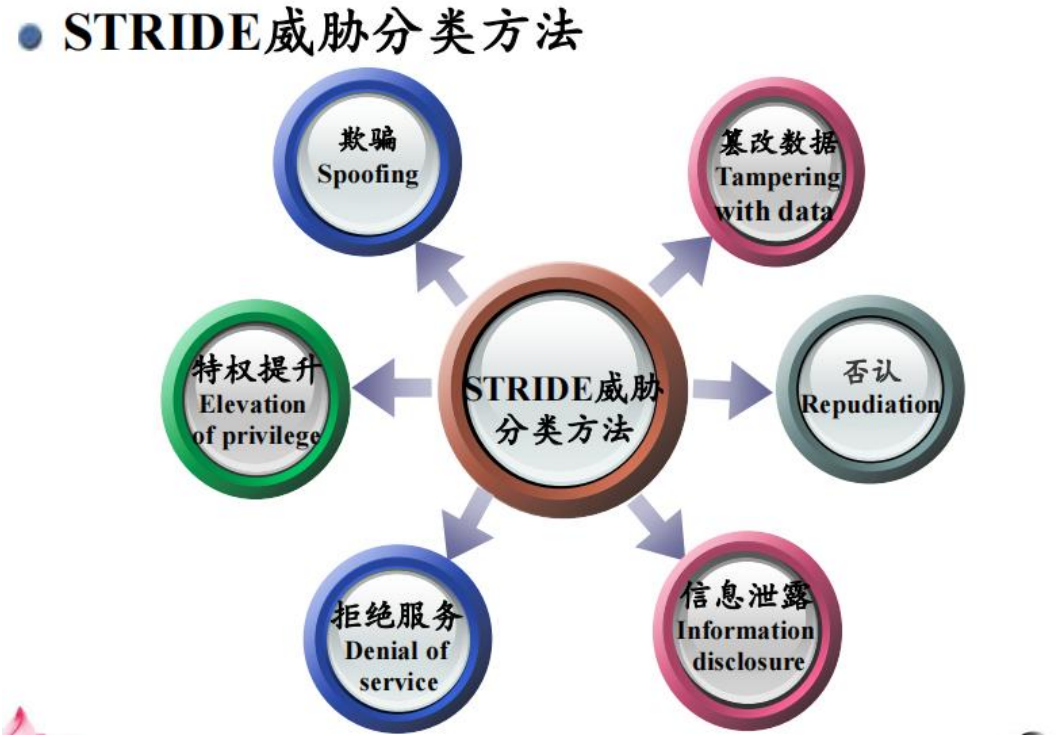
3.3.2 伪造合法网站的登录页面诱导用户输入敏感账号密码信息

3.3.3 伪造合法网站的支付页面诱导用户输入敏感支付信息

3. 威胁表

(1) 准备工作

1) STRIDE



2) DREAD 威胁评估方法（Microsoft）

- Damage potential(破坏性)：衡量威胁可能造成的实际破坏程度.
- Reproducibility(再现性)：衡量威胁变成实际攻击的难易程度
- Exploitability(可利用性)：衡量进行一次攻击需要多少努力和专业知识
- Affected users(影响用户)：攻击可能影响的用户数.
- Discoverability(可发现性)：衡量是否易于发现的程度（最难衡量的标准）

上述每个方面危害程度的取值范围是 1-10，数值越高造成的威胁越大 ，10 表示威胁造成的危害程度最大，1 表示威胁造成的危害程度最小。

3) DREAD 威胁评估方法取值示例

	低风险（1）	中风险（5）	高风险（10）
潜在破坏性（D）	普通的信息泄露	敏感信息泄露	攻击者可以破坏安全系统；获得完全信任授权；以管理员身份运行；可以上传任意内容
再现性（R）	即使存在安全漏洞，攻击也很难发生	在特定的情况和要求下，攻击可以发生	攻击在任何时刻都可以很容易地发生
可利用性（E）	攻击需要精深的专业知识或高级的专业工具	攻击需要普通的专业知识或一般专业工具	几乎不需要专业知识或仅需要常见的工具
受影响用户（A）	比例极低的用户	部分用户	全部用户
可发现性（D）	特征模糊，极难发现	存在于少部分的功能中，部分用户可以发现	特征明显，极易发现

4) 对威胁树主要威胁的评估

SQL 注入攻击：

潜在破坏性（Damage）：8/10

再现性（Reproducibility）：4/10

可利用性（Exploitability）：7/10

受影响用户（Affected users）：7/10

可发现性（Discoverability）：5/10

综合风险等级（Risk Rating）：6.2/10

Session 劫持：

潜在破坏性（Damage）：7/10

再现性（Reproducibility）：3/10

可利用性（Exploitability）：6/10

受影响用户（Affected users）：6/10

可发现性（Discoverability）：4/10

综合风险等级（Risk Rating）：5.2/10

XXS 攻击：

潜在破坏性（Damage）：6/10

再现性（Reproducibility）：3/10

可利用性（Exploitability）：6/10

受影响用户（Affected users）：6/10

可发现性（Discoverability）：4/10

综合风险等级（Risk Rating）：4.2/10

密码破解：

潜在破坏性（Damage）：7/10

再现性（Reproducibility）：3/10

可利用性（Exploitability）：5/10

受影响用户（Affected users）：5/10

可发现性（Discoverability）：5/10

综合风险等级（Risk Rating）：5.0/10

身份验证漏洞：

潜在破坏性（Damage）：7/10

再现性（Reproducibility）：4/10

可利用性（Exploitability）：6/10

受影响用户（Affected users）：6/10

可发现性（Discoverability）：4/10

综合风险等级（Risk Rating）：5.6/10

CSRF 攻击：

潜在破坏性（Damage）：6/10

再现性（Reproducibility）：3/10
可利用性（Exploitability）：6/10
受影响用户（Affected users）：6/10
可发现性（Discoverability）：4/10
综合风险等级（Risk Rating）：4.8/10

未授权访问：
破坏性（Damage）：4/10
可靠性（Reproducibility）：4/10
可利用性（Exploitability）：6/10
可影响的用户数（Affected Users）：8/10
时间敏感性（Discoverability）：4/10
综合风险等级（Risk Rating）：5.2/10

系统漏洞利用：
破坏性（Damage）：6/10
可靠性（Reproducibility）：6/10
可利用性（Exploitability）：7/10
可影响的用户数（Affected Users）：8/10
时间敏感性（Discoverability）：5/10
综合风险等级（Risk Rating）：6.4/10

滥用权限：
破坏性（Damage）：7/10
可靠性（Reproducibility）：4/10
可利用性（Exploitability）：6/10
可影响的用户数（Affected Users）：7/10
时间敏感性（Discoverability）：5/10
综合风险等级（Risk Rating）：5.8/10

社会工程学攻击：
破坏性（Damage）：4/10
可靠性（Reproducibility）：5/10
可利用性（Exploitability）：5/10
可影响的用户数（Affected Users）：9/10
时间敏感性（Discoverability）：9/10
综合风险等级（Risk Rating）：6.4/10

拒绝服务攻击：
破坏性（Damage）：8/10
可靠性（Reproducibility）：8/10
可利用性（Exploitability）：8/10

可影响的用户数（Affected Users）：8/10

时间敏感性（Discoverability）：5/10

综合风险等级（Risk Rating）：7.4/10

网络钓鱼攻击：

破坏性（Damage）：5/10

可靠性（Reproducibility）：7/10

可利用性（Exploitability）：6/10

可影响的用户数（Affected Users）：8/10

时间敏感性（Discoverability）：8/10

综合风险等级（Risk Rating）：6.8/10

(2) 威胁表

威胁	描述	影响	风险等级	威胁目标	威胁类型	缓和技术	威胁树
SQL 注入攻击	攻击者利用输入验证缺陷，通过向数据库发送恶意查询，获得未授权访问数据库的权限	可能导致数据泄露、数据完整性遭到破坏、系统被入侵	高	身份认证(8.0-7.0),服务请求(9.0-8.0,10.0-8.0)	Tampering	完整性验证：强完整性控制，访问控制列表，数字签名，MAC	威胁树1
Session 劫持	攻击者窃取用户的session ID，并使用这些信息冒充受害者的身份访问受限资源	可能导致敏感信息泄露、非授权访问、用户的数据和操作记录被破坏	高	身份认证(8.0-7.0),服务请求(9.0-8.0,10.0-8.0)	Spoofing	认证：Basic 认证，Digest 认证，Cookie 认证，Windows 认证，Kerberos 认证，SSL/TLS PKI，IPSec 数字签名，MAC，Hash 函数	威胁树1

威胁	描述	影响	风险等级	威胁目标	威胁类型	缓和技术	威胁树
XXS 攻击	攻击者利用 Web 应用程序的漏洞，向用户的浏览器注入恶意代码，例如 JavaScript 脚本	可能导致数据泄露、用户信息窃取、Web 应用程序的安全性受到影响	高	服务请求(9.0-8.0,10.0-8.0),学生成绩请求(2.0-8.0)	Tampering	完整性验证：强完整性控制，访问控制列表，数字签名，MAC	威胁树1
密码破解攻击	攻击者通过尝试多个可能的密码来访问系统	可能导致数据泄露、系统被入侵、数据完整性遭到破坏	中	身份认证(8.0-7.0)，登陆验证(7.0-6.0)	Tampering	完整性验证：强完整性控制，访问控制列表，数字签名，MAC	威胁树1
身份验证漏洞	应用程序在认证过程中存在漏洞，例如密码被明文存储或默认密码未更改	可能导致非授权访问、敏感信息泄露、数据完整性遭到破坏	中	身份认证(8.0-7.0)，登陆验证(7.0-6.0)	Spoofing	认证：Basic 认证，Digest 认证，Cookie 认证，Windows 认证，Kerberos 认证，SSL/TLS PKI，IPSec 数字签名，MAC，Hash 函数	威胁树1
CSRF 攻击	攻击者利用受害者已经登录的状态，向应用程序发送恶意请求，以冒充受害者的身份进行操作	可能导致敏感信息泄露、未授权操作、数据完整性遭到破坏	中	数据更新(6.0-21.0)等相关的	Tampering	完整性验证：强完整性控制，访问控制列表，数字签名，	威胁树1

威胁	描述	影响	风险等级	威胁目标	威胁类型	缓和技术	威胁树
				数据请求环节		MAC	
未授权访问	未被授权的用户可以访问系统中的某些资源	窃取、篡改、破坏敏感数据，系统稳定性受到威胁	高	身份认证(8.0-7.0)	Elevation of privilege	授权管理：访问控制列表组或角色成员，特权属主权限	威胁树2
系统漏洞利用	攻击者利用系统漏洞进行攻击	窃取、篡改、破坏敏感数据，系统稳定性受到威胁	高	可以是任何位置	Tampering	完整性验证：强完整性控制，访问控制列表，数字签名，MAC	威胁树2
滥用权限	被授权的用户或攻击者滥用权限	窃取、篡改、破坏敏感数据，系统稳定性受到威胁	高	数据更新(6.0-21.0)等相关的数据请求环节	Elevation of privilege	授权管理：访问控制列表组或角色成员，特权属主权限	威胁树2
社会工程学攻击	攻击者使用社会工程学手段获取信息或利用人性弱点进行攻击	窃取、篡改敏感数据，系统稳定性受到威胁	中	可以是任何位置	Spoofing	认证：Basic认证，Digest认证，Cookie认证，Windows认证，Kerberos认证，SSL/TLS PKI，IPSec数字签名，	威胁树3

威胁	描述	影响	风险等级	威胁目标	威胁类型	缓和技术	威胁树
						MAC ，Hash 函数	
拒绝服务攻击	攻击者通过大量恶意请求使系统瘫痪	无法使用系统，影响业务正常运转	高	可以是任何数据请求服务的位置	Denial of service	可用性技术：访问控制列表，过滤，配额，授权	威胁树 3
网络钓鱼攻击	攻击者伪造合法的网站或信息来欺骗用户泄露敏感信息	窃取用户的敏感信息，造成经济损失	中高	可以是任何位置	Spoofing	认证：Basic 认证，Digest 认证，Cookie 认证，Windows 认证，Kerberos 认证，SSL/TLS PKI，IPSec 数字签名，MAC ，Hash 函数	威胁树 3