用例规约：<学生登陆>

# 用例名称

学生登录

## 简要说明

此用例描述了学生通过输入用户名和密码登录在线考试平台的过程。登录后，学生可以访问个人主页，查看可用考试、成绩查询以及其他功能。

# 事件流

## 基本流

 学生访问在线考试平台的登录页面。

 系统显示登录界面，要求输入用户名和密码。

 学生输入有效的用户名和密码。

 系统验证输入的用户名和密码。

* 如果用户名和密码匹配，系统加载学生的个性化主页并成功登录。
* 如果用户名和密码不匹配，系统显示错误消息，要求重新输入。

 学生成功登录后，系统显示学生的个人信息、考试安排、成绩查询等功能。

## 备选流

### <密码错误>

**简要说明：**

此备选流描述了学生在登录过程中输入错误密码时的处理流程。系统会提示错误并要求重新输入密码，若多次失败，系统会锁定账户并提示进行密码重置。

**事件流：**

1. **学生输入错误密码**：
   * 学生在登录页面输入用户名和密码，但密码输入错误。
2. **系统验证失败**：
   * 系统检测到密码与用户名不匹配，提示“密码错误，请重新输入”。
3. **学生重新输入密码**：
   * 学生尝试重新输入密码并点击“登录”按钮。
   * 如果密码正确，登录过程继续，进入主页面。
4. **连续三次密码错误**：
   * 如果学生连续输入错误密码三次，系统会暂时锁定账户。
   * 锁定账户后，系统提示：“由于多次密码输入错误，账户已被锁定，请通过邮件或手机重置密码”。
5. **密码重置**：
   * 学生点击“忘记密码”链接，系统要求提供注册时的邮箱或手机号码进行身份验证。
   * 学生完成验证后，系统允许其重置密码。
6. **账户解锁**：
   * 在重置密码后，学生使用新密码登录系统，恢复访问权限。

**结束条件：**

* 如果学生成功输入密码，系统继续执行主事件流，学生进入个人主页。
* 如果学生无法在限定时间内输入正确密码或完成密码重置，登录流程终止，并提示学生稍后再试。

**特殊要求：**

* 为确保账户安全，系统应限制用户在短时间内尝试输入密码的次数，避免暴力破解。
* 密码输入应使用加密传输（如SSL/TLS协议），防止密码泄露。

#### <备选分支流>

**简要说明：**

此分支流描述了在学生尝试通过重置密码恢复账户访问时，输入的验证信息不匹配系统记录的情况。系统会提示验证失败，要求学生重新输入或采取其他措施。

**事件流：**

1. **学生点击“忘记密码”链接**：
   * 学生在密码错误界面点击“忘记密码”链接，系统将引导学生到密码恢复界面。
2. **学生输入注册信息**：
   * 学生输入与账户相关联的邮箱地址或手机号码。
3. **系统验证输入信息**：
   * 系统检查输入的邮箱地址或手机号码是否与账户记录匹配。
4. **验证失败**：
   * 如果系统未能匹配到正确的注册信息，系统将提示：“验证失败，请重新输入您的邮箱或手机号码”。
5. **学生重新输入验证信息**：
   * 学生可以选择重新输入邮箱或手机号码，点击“提交”进行再次验证。
6. **多次验证失败**：
   * 如果学生连续多次输入错误的邮箱或手机号码，系统会提示“多次验证失败，请稍后再试”，并在指定时间内禁止重新尝试。
7. **密码重置失败终止**：
   * 如果学生仍无法通过验证，系统将提示：“账户恢复失败，请联系管理员”。

**结束条件：**

* 如果学生输入正确的邮箱或手机号码，系统会发送重置密码的链接或验证码，恢复主事件流。
* 如果学生验证失败，系统结束此分支流，登录流程被中止。

**特殊要求：**

* 密码恢复过程必须符合数据隐私政策，确保学生信息安全。
* 在输入错误多次后，应加入延迟机制，避免系统受到暴力破解攻击。
* 验证过程中应确保所有信息的传输通过安全通道进行（例如SSL加密）。

### <账户锁定>

**简要说明：**

此备选流描述了当学生连续多次输入错误的用户名或密码，导致账户被锁定时的处理流程。学生将需要通过密码重置流程来恢复账户访问。

**事件流：**

1. **学生输入错误的用户名或密码**：
   * 学生在登录页面输入用户名和密码，但密码错误。
2. **系统验证失败**：
   * 系统检测到密码与用户名不匹配，提示“密码错误，请重新输入”。
3. **学生连续错误输入三次密码**：
   * 如果学生连续三次输入错误密码，系统会暂时锁定账户。
   * 系统提示：“由于多次密码输入错误，账户已被锁定，请通过邮件或手机号恢复密码”。
4. **学生选择密码重置**：
   * 学生点击“忘记密码”链接，系统引导学生进入密码恢复流程。
5. **系统要求学生提供注册信息**：
   * 学生输入注册时绑定的邮箱地址或手机号码。
6. **系统验证注册信息**：
   * 系统检查输入的邮箱或手机号码是否正确匹配系统中存储的注册信息。
7. **密码重置成功**：
   * 如果验证通过，系统会发送重置密码的链接或验证码至学生的邮箱或手机。
8. **学生重置密码并重新登录**：
   * 学生通过重置链接设置新密码，并通过新密码重新登录系统。
9. **密码重置失败**：
   * 如果验证失败，系统会提示“账户恢复失败，请稍后再试”。
   * 如果学生在规定的时间内无法完成密码重置，则需要联系管理员恢复账户。

**结束条件：**

* 如果密码重置成功，学生能够重新登录系统并访问相关功能。
* 如果密码重置失败，学生无法登录系统，且需通过其他途径恢复账户。

**特殊要求：**

* 密码重置过程必须符合数据隐私政策，确保学生信息的安全性。
* 重置密码过程中使用加密传输协议（如SSL）确保数据的安全。
* 在账户锁定期间，系统应该防止进一步的密码输入尝试，以保护系统不受暴力破解攻击。

# 特殊需求

## <数据加密和安全传输>

为了确保学生、教师和教务人员在平台上使用过程中，个人信息和敏感数据（如用户名、密码、成绩等）不被泄露，系统必须实施数据加密和安全传输措施。此需求包括密码存储的加密方式、数据在传输过程中的加密协议以及对系统访问的严格控制。

**详细需求**

1. **密码存储加密**：
   * 所有用户（学生、教师、教务人员）的密码必须使用哈希算法进行加密存储。推荐使用如 bcrypt、PBKDF2 或 Argon2 等强加密算法。
   * 密码不得以明文存储在数据库中。若发生系统数据泄露，密码应无法被恢复或破解。
2. **数据传输加密**：
   * 系统在传输用户数据时，必须采用SSL/TLS协议（安全套接字层/传输层安全协议）进行加密。这样确保用户的敏感数据（如用户名、密码、成绩等）在传输过程中不被窃取或篡改。
   * 所有与平台相关的接口和数据交换（如登录请求、成绩查询、注册等）都应使用HTTPS协议，而非HTTP协议。
3. **用户数据加密存储**：
   * 除了密码之外，所有用户的敏感信息（如个人身份信息、考试成绩、学号等）必须在数据库中加密存储。采用对称加密（如AES-256）对这些数据进行加密，确保即使数据泄露也无法被直接读取。
   * 解密密钥应妥善存储在加密的硬件安全模块（HSM）中，或采用其他安全的密钥管理方案。
4. **会话安全**：
   * 登录后，系统应通过安全的会话管理机制（如HTTPOnly和Secure标记的Cookies）来保护用户的登录状态。
   * 用户会话应设置超时机制，在用户空闲超过一定时间（如15分钟）时，自动注销并清除会话信息。
5. **多因素认证**：
   * 对于所有用户（特别是教师和教务人员），在登录时应支持启用多因素认证（MFA），如通过短信或电子邮件发送验证码，增强账户的安全性。

**特殊要求**

1. **加密算法标准**：
   * 所有加密算法和密钥长度应符合行业标准，如NIST（美国国家标准与技术研究院）或其他相关安全标准的要求。
2. **安全审计和日志记录**：
   * 系统应定期进行安全审计，检查加密策略的执行情况和加密算法的有效性。
   * 所有安全相关的操作（如密码重置、登录失败、多次登录尝试等）应生成日志并保存，以供审计和问题排查。
3. **合规性**：
   * 系统需要符合相关的数据保护法规，如GDPR（通用数据保护条例）、中国《个人信息保护法》等，确保用户数据在存储和传输过程中得到充分的保护。

# 前置条件

## <学生已注册并拥有有效的账户和密码>

* **学生注册：**在执行学生登录用例之前，学生必须完成平台的注册流程，包括提供有效的个人信息（如姓名、学号、邮箱、密码等），并成功提交注册请求。
* **有效账户信息：**学生的账户信息应已经存储在系统中，包括学生的用户名和密码。密码必须经过加密处理以确保安全性。
* **确认邮箱或手机号**：学生在注册过程中提供的邮箱或手机号必须经过验证，用于后续的密码重置和身份确认。
* **账户激活**：如果系统要求激活账户（例如通过邮箱或短信发送验证链接），学生必须完成账户激活，以便后续使用该账户登录系统。

# 后置条件

## <学生成功登录并进入个人主页>

* **成功登录**：在学生成功输入正确的用户名和密码并通过系统验证后，学生成功登录系统。
* **个人主页加载**：学生的个人主页应加载，并显示其相关的个性化信息，包括：可用的考试信息、安排以及进入考试的入口。
* 个人成绩查询功能，学生能够查看自己的历次考试成绩。提供练习区和复习材料，帮助学生准备即将到来的考试。
* **系统会话开始**：系统为该学生创建一个有效的会话，记录学生的登录状态，并且在会话期间保持学生的登录状态，直到会话超时或学生主动退出。
* **权限验证**：登录成功后，系统确认学生的权限，仅允许学生访问其所能访问的功能，如查看成绩、参加考试等，确保系统数据安全。

# 扩展点

## <密码恢复扩展点>

**扩展点位置**：

* 此扩展点位于**学生登录用例**的“密码错误”或“用户名不存在”事件流中，当学生多次输入错误密码或输入不存在的用户名时，系统将提供“密码恢复”功能。
* 在事件流中，如果学生未能成功登录（例如输入错误密码三次），系统会提示学生选择“忘记密码”链接，并引导学生进入密码恢复流程。此时，用例流程会转向密码重置，用以恢复账户访问权限。

**扩展点描述**：

* 当学生点击“忘记密码”链接时，系统不再执行标准的登录流程，而是将学生引导至密码恢复流程。
* 在密码恢复过程中，学生需提供与账户关联的邮箱或手机号进行身份验证。如果学生能够成功验证，系统会通过邮件或短信发送重置密码的链接或验证码。
* 如果身份验证失败，系统会提示“验证失败，请重新输入您的邮箱或手机号码”，并要求学生重新输入验证信息。

**扩展点触发条件**：

* 如果学生连续三次输入错误密码，或者学生输入的用户名不存在，系统将提示错误，并为学生提供通过密码恢复功能解决问题的选项。

**扩展点结束条件**：

* 如果学生成功通过密码恢复流程，能够重置密码并重新登录，扩展点结束，返回标准的登录成功状态。
* 如果学生无法通过验证重置密码，系统提示“账户恢复失败，请稍后再试”，并终止当前用例流程。