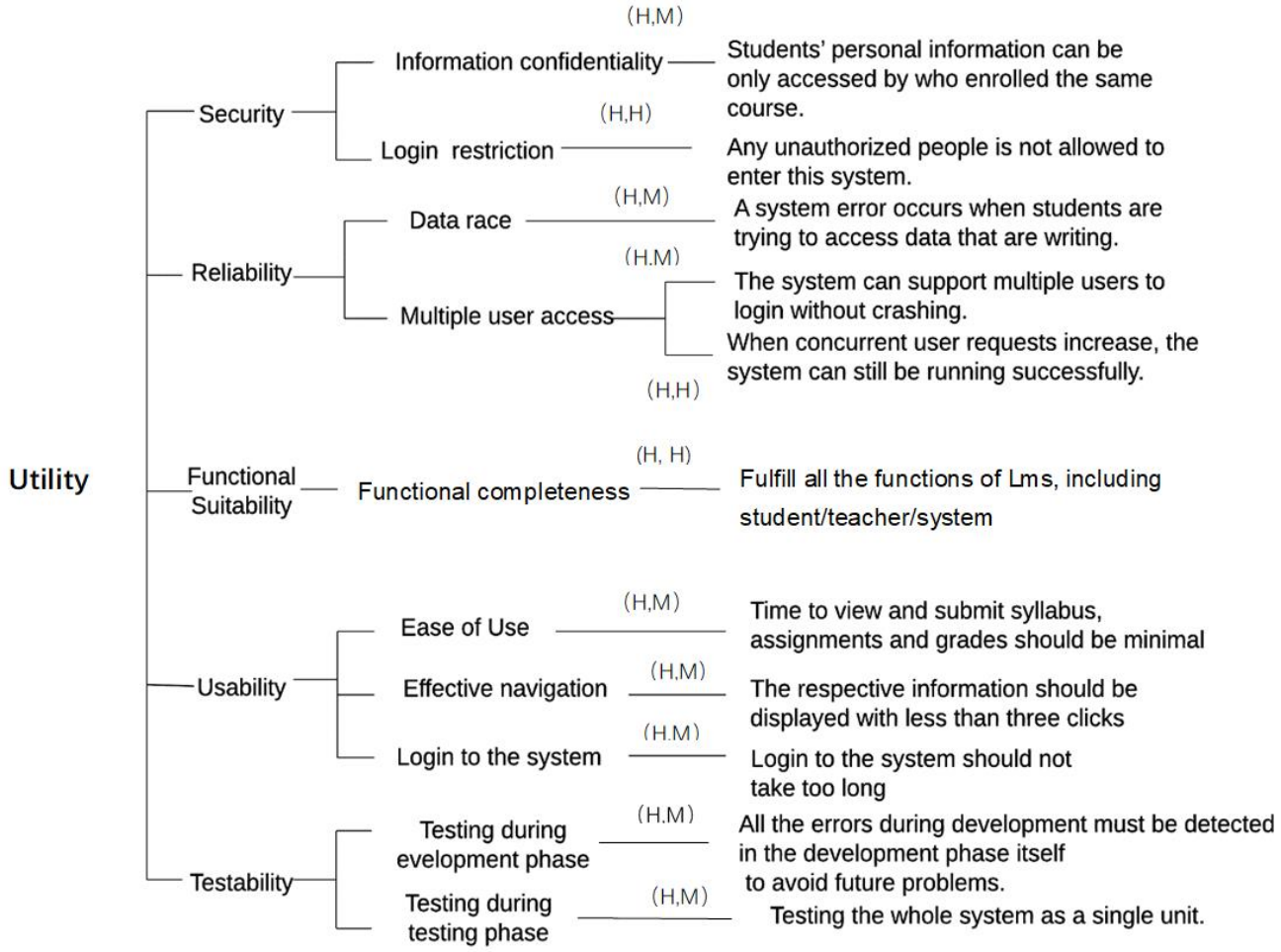
Requirements Analysis
Team2-Chalkbox

---

1. Software quality utility tree



2. Utility scenarios

Quality attribute	**Security**
Scenario name	Login restriction
Source	Unauthorized people
Stimulus	Try to log in without out correct account
Artifact	The system
Environment	At runtime
Response	Displays the notice of denying invalid login activity.
Response measure	Identifies invalid account and password in three seconds.

Quality attribute	**Reliability**
Scenario name	Multiple user access
Source	Users
Stimulus	Multiple users try to access the same piece of datum at the same time
Artifact	website
Environment	Run time

Response	The system should respond the correct information to every user correctly.
Response measure	The response time and the correctness of the return information.

Quality attribute	**Function Suitability**
Scenario name	Functional completeness
Source	Developers
Stimulus	It reaches the deadline of the development process and the system is published to the users.
Artifact	website
Environment	Run time
Response	System provides all of services or most of the services as it is supposed to.
Response measure	The implemented rate of the functions.

Quality attribute	**Usability**
Scenario	Ease of usability
Source	User(student/Instructor)

Stimulus	users want to use the system
Artifact	The System
Environment	At Runtime
Response	Access syllabus, assignments and grades, submit assignments/grades.
Response Measure	Time to view and submit syllabus, assignments and grades should be minimal(less than 3 seconds).

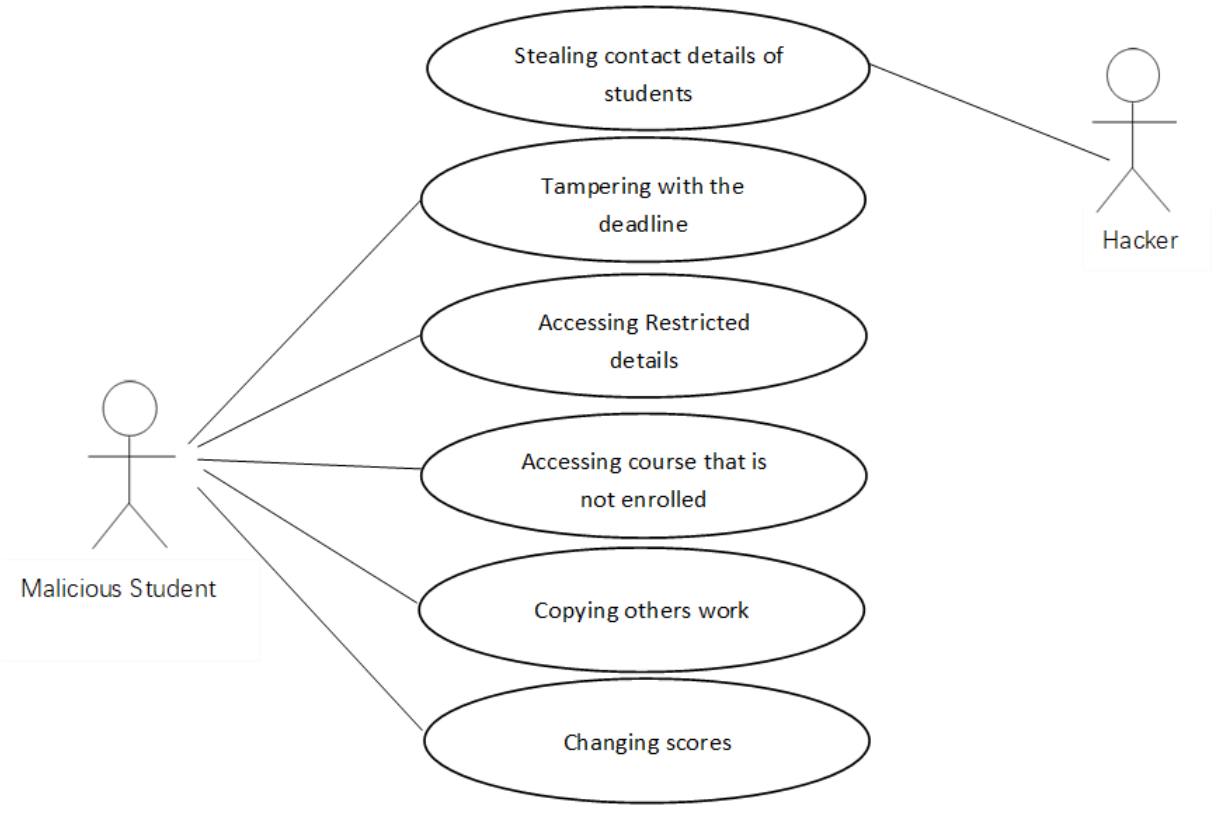
Quality attribute	**Usability**
Scenario name	Effective navigation
Source	A user
Stimulus	Navigates the site in search of a page he/she needs
Artifact	Website
Environment	At runtime
Response	Displays the right page when the respective tab/link is clicked.
Response measure	The respective information should be displayed with less than three clicks

Quality attribute	**Usability**
Scenario name	Login to the system
Source	User(Student/Instructor)
Stimulus	User tries login to the system
Artifact	Website
Environment	Normal operation
Response	The user is able to login to the system and access the course details without waiting too long.
Response measure	Login to the system should not take too long(less than 3 seconds) when the right credentials are entered. When the wrong credentials are entered the system should display the appropriate error message within 3 seconds.

Quality attribute	**Testability**
Scenario	Testing in various phases of development.
Source	Developer, Tester, User.
Stimulus	Developer or the Tester want to test the system or a part of it
Artifact	The entire system or just a part of it, code.

Environment	During development, testing phase.
Response	Comparing the expected outcomes with the actual output.
Response measure	Number of bugs/errors must be reduced after consecutive tests.

3. Abuse Case Diagram



4. Abuse case descriptions

Abuse case name: Stealing contact details of students
Actors: hacker
Trigger: A hacker tries to break into the system for stealing students' information.
Basic flow

- Hacker tries to log in for stealing contact details of students
- System denies its wrong account name and password. The log-in activity is unsuccessful.

Alternative flow

- Hackers enters the system in illegal way, trying to steal contact details of students.
- System responds that this information is locked when anyone who is not enrolled this course.

Exception flow – Hacker enters the system successfully. Students' personal information are exposed to hacker. Hacker makes a copy of contact details without any restriction.

Abuse case name: Changing scores
Actors: Malicious Student
Trigger: A malicious Student tries to change the score given by instructor.
Basic flow

- A malicious student tries to change the score given by the instructor.
- System denies his attempt because the score is locked and write access is available only to the instructor.

Alternative flow

- A malicious student hacks the system for changing the given score.
- System responds to this illegal operation and stop his attack.

Exception flow – A malicious student enters the system and he can change the score which already decided by the instructor. The system doesn't deny this activity.

Abuse case name: Tampering with the deadline
Actors: Malicious Student
Trigger: A malicious student tries to tamper the deadline for avoiding penalty.
Basic flow

- A student tries to submit the assignment after the deadline**.**
- The software denies the submission or accepts as overdue submission.

Alternative flow

- A malicious student tries to hack the system and upload the file without deadline detection.
- System responds to the operation and the student fails.

Exception flow —The malicious student applies some technology to upload the assignment on the server directly. The system doesn't mark the file as overdue, the tampering succeeds.

Abuse case name: Accessing Restricted details of enrolled courses

Actors: Malicious Student
Trigger: A malicious student tries to access restricted details(assignments/test papers) of enrolled courses.
Basic flow

- Student logs into his/her account.
- Student tries to access restricted details (such as unpublished assignment and test papers).
- System denies the request and informs that the assignments/test papers are not accessible right now.

Alternative flow

- Student tries sql injection or uses other abnormal way to get the restricted details.
- System detects the abnormal actions and denies the requests.
- System lock this student's account and keeps the records.

Exception flow—Student successfully accesses the restricted details and gets the secret data.

Abuse case name: Accessing courses not enrolled
Actors: Malicious Student
Trigger: Malicious Student tries to access courses he/she is not enrolled to
Basic flow:

- Malicious student tries to access/steal course materials he/she is not enrolled to.
- System provides access only to enrolled courses and does not give any information about other courses the student is not enrolled to.

Alternative flow:

- The students try to modify course materials he/she is not enrolled to.
- System does not allow students to modify the materials.

Exception flow —The malicious student hacks the system and access the other courses illegally. Student/Hacker successfully copies/steals the course materials.

Abuse case name: Copying others work
Actors: Malicious Student
Trigger: Malicious Student tries to copy the work of other students
Basic flow:

- Malicious student tries to copy the work of other students.
- System does not allow the student to view the answers given by other students.

Alternative flow:

- The students try to login into other student's account.
- System does not allow students to login without the proper credentials.

Exception flow—The malicious student views the answers given by other students and successfully copies their work.