# Assignment 2

## Question 1

5 abuse case and additional use case to mitigate it

1. Guess Password:

The attacker can use related software to guess the password of the student user’s blackboard account, so as to log in to the account to obtain the required information. In order to mitigate such attacks, blackboard should remind users to use stronger passwords when registering. The password should contain letters, numbers and characters.

1. View/Modify Assignments

The attacker may attack the website to view the assignments submitted by the students or modify the content of the assignments. Students can still view and modify the homework after submitting it, but the system needs to verify the identity of the user before viewing the content of the homework, and send a confirmation email after the student submits the homework.

1. Release Announcement

The attacker may post some false notices on the blackboard to mislead the students. The website should require the publisher to enter a password when publishing. Each teacher should set his own password to prevent attackers from issuing misleading notices.

1. Delete Items

The attacker may attack the website to delete some key content, such as upcoming assignments or exam content. Blackboard should notify the teacher when the content of the course changes, so as to make timely adjustments.

1. Modify Grades

Attackers may modify their own scores or lower the scores of others by attacking websites. The system should send a verification code to the modifier when the teacher or teaching assistant modifies the grade. The verification code can be sent by a mobile phone verification code or an email verification code. This can prevent the attacker from obtaining the verification code.

## Question 2

图示

描述已自动生成

## Question 3

1. Project owner

|  |  |  |  |
| --- | --- | --- | --- |
| Spoofing | Authentication |  |  |
| Tampering | Integrity |  |  |
| Repudiation | Non-repudiation | I didn’t post that thread | Security audit and logging  Digital signature |
| Information disclosure | Confidentiality |  |  |
| Denial of service | Availability |  |  |
| Elevation of privilege | Authorization |  |  |

1. General user

|  |  |  |  |
| --- | --- | --- | --- |
| Spoofing | Authentication | Pretend to project owner | Strong password or third-party authentication |
| Tampering | Integrity | Modify project data | Access control  Authentication Code |
| Repudiation | Non-repudiation |  |  |
| Information disclosure | Confidentiality |  |  |
| Denial of service | Availability |  |  |
| Elevation of privilege | Authorization |  |  |

1. Project data

|  |  |  |  |
| --- | --- | --- | --- |
| Spoofing | Authentication |  |  |
| Tampering | Integrity |  |  |
| Repudiation | Non-repudiation |  |  |
| Information disclosure | Confidentiality | Users can see other people’s project data | Encryption |
| Denial of service | Availability |  |  |
| Elevation of privilege | Authorization |  |  |

1. Web client

|  |  |  |  |
| --- | --- | --- | --- |
| Spoofing | Authentication |  |  |
| Tampering | Integrity |  |  |
| Repudiation | Non-repudiation |  |  |
| Information disclosure | Confidentiality |  |  |
| Denial of service | Availability | The project owner cannot access his own project data | Firewall |
| Elevation of privilege | Authorization |  |  |

1. Web server

|  |  |  |  |
| --- | --- | --- | --- |
| Spoofing | Authentication |  |  |
| Tampering | Integrity |  |  |
| Repudiation | Non-repudiation |  |  |
| Information disclosure | Confidentiality |  |  |
| Denial of service | Availability |  |  |
| Elevation of privilege | Authorization | General users can perform private operations of the project owner | Role control  Authorization |

1. Database

|  |  |  |  |
| --- | --- | --- | --- |
| Spoofing | Authentication | Pretend to be administrator | Strong password or third-party authentication |
| Tampering | Integrity | Modify database data | Access control  Authentication Code |
| Repudiation | Non-repudiation |  |  |
| Information disclosure | Confidentiality |  |  |
| Denial of service | Availability |  |  |
| Elevation of privilege | Authorization |  |  |