

Name the type of the oversight for each of the following scenarios, Explain the effect of the oversight, and identify how it can be prevented.

#### Scenario 1: File Upload Vulnerability

You are in charge of reviewing the code of a file-sharing website where users can upload files. You discover that the application does check the file extension before allowing the upload, but it doesn't validate the file content. This oversight allows users to upload malicious files with executable code.

**Incomplete Mediation. This oversight allows users to upload malicious files with executable code. It can be prevented by checking the file content before uploading it.**

#### Scenario 2: Online Banking Application

You were asked to examine a multi-threaded banking application that handles financial transactions. You observed that multiple transactions can access and modify a shared bank account simultaneously without proper synchronization mechanisms. This could lead to incorrect balance calculations and potential data fraud.

**Race Condition. This could lead to incorrect balance calculations and potential data fraud. It can be prevented by allowing one transaction at a time to access and modify.**

#### Scenario 3: ATM Transaction

A student discovers that they can withdraw more money from the campus ATM than their account balance allows. By quickly cancelling the transaction just before it is processed, they can receive the cash without any deductions from their account balance.

**Time-of-Check to Time-of-Use. This oversight allows to withdraw more money from the campus ATM than the account balance has. It can be prevented by ensuring that the transaction is completed and the account balance is updated before dispensing cash to the user.**

#### Scenario 4: Network Server Application

You got many complaints about the network server application being unresponsive. When you investigated the situation, you found out the server application crashed unexpectedly after receiving an unprecedented large volume of data.

**Buffer Overflow. This oversight can crash the network server application unexpectedly after receiving an unprecedented large volume of data. It can be prevented by checking the limit first of the network server application.**