

Instructional Scenario

Banking Security

Breach Investigation



Course/Duty Area: Java Programming (Oracle)/Handling Exceptions; Exploring Database Input/Output

Scenario:

A local bank has recently detected unauthorized access to its customer records. As part of their cybersecurity and IT team, you are tasked with investigating the breach. You must develop a Java program that reads log files, detects anomalies, and handles potential exceptions caused by missing or corrupt files.

Big Question:

How can exception handling and file input/output be used to analyze security logs and identify potential breaches?

Focused Questions:

- How does Java handle exceptions, and why is it important in file-reading operations?
- What are the common security vulnerabilities in file-based systems?
- How can logging and error handling improve system security?

Student Project or Outcome:

Students will write a Java program that

- reads and analyzes log files from a simulated banking system
- implements exception handling to manage missing or corrupted log entries
- identifies suspicious activities, such as unauthorized access attempts.

Project-Based Assessment:

- Java code implementation (file reading and exception handling)
- A brief report on detected anomalies and how the program identifies them
- A demonstration of how the program handles errors and missing files

Teacher Resources:

- Sample log files with simulated breaches (see below)
- Java documentation on exception handling and file I/O
- Bank security case studies for discussion

Sample Log File (security_logs.txt)

```
[2025-02-20 10:15:32] LOGIN SUCCESS - User: JohnDoe
[2025-02-20 10:16:10] LOGIN FAILED - User: Unknown
[2025-02-20 10:17:45] ACCESS DENIED - User: Hacker123, Attempted access: Admin Panel
[2025-02-20 10:20:10] LOGIN SUCCESS - User: AliceW
[2025-02-20 10:25:05] TRANSACTION FAILED - User: AliceW, Amount: $5000, Reason: Suspicious Activity
[2025-02-20 10:30:01] LOGIN SUCCESS - User: BobM
[2025-02-20 10:32:12] UNAUTHORIZED ACCESS ATTEMPT - IP: 192.168.1.100
[2025-02-20 10:40:20] LOGIN SUCCESS - User: CharlieX
```

Java Code: Log Analyzer

```
import java.io.*;
import java.util.regex.*;

public class LogAnalyzer {
    public static void main(String[] args) {
        String filePath = "security_logs.txt";

        try (BufferedReader reader = new BufferedReader(new FileReader(filePath))) {
            String line;
            while ((line = reader.readLine()) != null) {
                analyzeLogEntry(line);
            }
        } catch (FileNotFoundException e) {
            System.out.println("Error: Log file not found.");
        } catch (IOException e) {
            System.out.println("Error reading the log file.");
        }
    }

    public static void analyzeLogEntry(String log) {
        if (log.contains("LOGIN FAILED") || log.contains("UNAUTHORIZED ACCESS ATTEMPT") ||
            log.contains("ACCESS DENIED")) {
            System.out.println("[ALERT] Suspicious Activity Detected: " + log);
        } else if (log.contains("TRANSACTION FAILED")) {
            System.out.println("[WARNING] Transaction Issue: " + log);
        } else {
            System.out.println("[INFO] Normal Activity: " + log);
        }
    }
}
```

Expected Output:

```
[INFO] Normal Activity: [2025-02-20 10:15:32] LOGIN SUCCESS - User: JohnDoe
[ALERT] Suspicious Activity Detected: [2025-02-20 10:16:10] LOGIN FAILED - User: Unknown
[ALERT] Suspicious Activity Detected: [2025-02-20 10:17:45] ACCESS DENIED - User: Hacker123, Attempted
```

access: Admin Panel

[INFO] Normal Activity: [2025-02-20 10:20:10] LOGIN SUCCESS - User: AliceW

[WARNING] Transaction Issue: [2025-02-20 10:25:05] TRANSACTION FAILED - User: AliceW, Amount: \$5000,
Reason: Suspicious Activity

[INFO] Normal Activity: [2025-02-20 10:30:01] LOGIN SUCCESS - User: BobM

[ALERT] Suspicious Activity Detected: [2025-02-20 10:32:12] UNAUTHORIZED ACCESS ATTEMPT - IP:
192.168.1.100

[INFO] Normal Activity: [2025-02-20 10:40:20] LOGIN SUCCESS - User: CharlieX

Scenario submitted by David Vogel, King George High School, King George County Public Schools