
Domain: Gaming & Casino Systems
Role: Senior Quality Analyst
Project Name: *PlaySecure – Casino Player Profile Management System*

□ Project Overview

PlaySecure is a regulatory-compliant player profile management system used by multiple casinos to manage player identities, gaming preferences, playing history, and account activities. This system integrates with various subsystems like loyalty programs, financial transactions, and responsible gaming checks, providing a centralized and secure platform for player data. As a QA lead, I was responsible for validating core business flows, backend validations, and regression test coverage across the web interface and APIs.

🚩 Realistic Problem Faced

In regulated environments like casinos, a single data mismatch or access rights failure could lead to fines or fraud. The PlaySecure system needed extremely tight access control, real-time transaction sync, and accurate player data linking across systems. During testing, we observed inconsistent loyalty points allocation and flawed profile merge logic. These issues could have led to financial loss and compliance violations if pushed live.

✅ My QA Approach

- **Test Planning & Design:**
  - Created 150+ detailed test cases covering CRUD operations for player profiles, financial actions, and loyalty triggers.
  - Used exploratory testing to identify integration flaws across systems.
- **Test Execution & Tools Used:**
  - Used **TFS** (Team Foundation Server) to write and execute test cases.
  - Conducted **API testing** using Postman for backend player lookup and merging logic.
  - Performed **SQL queries** for DB-level verification of player details and transaction consistency.
- **Cross-system Validation:**
  - Validated profile linkage between PlaySecure and external loyalty programs.
  - Used dummy player data to simulate real-world behavior.

📌 Critical Scenarios Covered

- Verifying account merge functionality when the same player registers under two IDs.
- Testing deletion of a player account and ensuring associated financial data is preserved in archives.
- Validating loyalty points allocation post successful gameplay using mock transaction triggers.
- Checking access control: casino staff vs admin roles when viewing or editing player data.
- Simulating multiple transactions in a short time span to test rate limiting and fraud detection.
- Ensuring proper validation during manual account updates (e.g., birthdate, ID proof).

❗ Notable Defects Caught

- **Loyalty Points Duplication:**
  A race condition was found where players were rewarded twice for the same gameplay event due to backend retries.
- **Merge Profile Flaw:**
  On merging duplicate player profiles, the new merged ID was sometimes linked to outdated email/contact info, violating compliance norms.
- **Unauthorized Access:**
  Staff with basic roles were able to export full player data CSVs, breaching GDPR and local gaming regulations.
- **Incorrect Transaction Sync:**
  Some gameplay transactions were not syncing back to the financial system due to broken webhook callbacks.
- **Data Integrity on Deletion:**
  Player deletion was permanently removing related financial transactions, instead of archiving — leading to loss of audit trail.

📈 Business Impact

- Prevented regulatory breach which could have caused **fines up to $10,000** by catching access control issues pre-production.
- Avoided financial discrepancies by identifying **loyalty point duplication** saving approx **$4,000 in bonus payouts**.
- Enabled smoother audits by pushing for improved **data retention logic** in player deletion.
- Overall, my efforts ensured the product went live with **zero high-priority bugs** in UAT.
