Security Analyst and Red team lead

Objective: Identify, simulate, and mitigate potential security weaknesses to ensure the system is cheat-proof and reliable.

Red Team Test Plan:

1. Test Plan Overview.
    - Scope : QR-based check-in, device binding, IP subnet validation, attendance cutoff, manual overrides, flagging engine, and audit logging.
    - Goal: Ensure the system prevents fraud, unauthorized access, and misuse, while logging all suspicious activity.
2. Threat Scenarios and Test Cases:

#	Threat / Attack Scenario	Test Steps	Expected System Response	Status / Notes
1	Duplicate QR Scan	Attempt to scan the same QR multiple times using the same device or multiple devices	Only the first scan accepted; duplicates rejected and flagged	
2	Device Spoofing	Try to mark attendance using a device not registered to the student	System rejects the check-in and logs the attempt	
3	Unauthorized Network Access	Attempt check-in from Wi-Fi or IP outside the approved campus subnet	Attendance rejected; suspicious activity flagged	
4	Attendance After Cutoff	Submit attendance after the allowed time window	System auto-marks absent and logs late attempt	
5	Manual Override Abuse	Teacher/admin manually changes records without reason	System logs all changes with user, timestamp,	

Security Analyst and Red team lead

#	Threat / Attack Scenario	Test Steps	Expected System Response	Status / Notes
			and reason; missing reasons flagged	
6	QR Replay Attack	Capture QR and try to reuse it on a different device/session	Rejected if duplicate or invalid session; flagged	
7	Shared Account / Credential Abuse	Student tries to log in using another student's credentials	Login denied if multi-factor / device binding active; attempt logged	
8	Multiple Accounts on One Device	Attempt to check in multiple students using one device	System flags suspicious device usage and rejects duplicate check-ins	
9	Tampering with API or Backend Calls	Try to submit attendance via modified API requests	Server-side validation rejects invalid data; logged for review	
10	Logging / Audit Evasion Attempt	Attempt to bypass logging or hide actions	All actions recorded server-side; tampering prevented	

Security Analyst and Red team lead

3. Testing Methodology

1. **Simulated Attacks:** Each scenario is executed in a controlled environment to prevent real student data corruption.
2. **Observation:** Monitor system logs, dashboards, and flags for correct detection.
3. **Documentation:** Record test outcomes, including success, failure, or partial mitigation.
4. **Mitigation Validation:** Confirm that fixes or controls correctly prevent the simulated attack.
5. **Re-testing:** Re-run tests after any system changes to ensure persistent security.

4. Expected Outcomes

- All unauthorized or abnormal attendance attempts are **rejected and logged**.
- The system automatically **flags suspicious activity** on teacher dashboards.
- Manual overrides are **auditable and accountable**.
- Data integrity is maintained under all tested scenarios.
- The system demonstrates **resilience against common student-based fraud and attacks**.

5. Reporting & Recommendations

- Summarize findings in a **Red Team Report**: vulnerabilities, exploited weaknesses, and recommended mitigations.
- Provide clear **steps for developers** to implement fixes.
- Validate effectiveness of fixes through **retesting**.

Security Policies and their Purpose

These policies ensure that the attendance system is secure, cheat-proof, auditable, and reliable, while guiding the role of Security Analyst & Red Team Lead.

1. **Access Control Policy**
   Policy:

- Role-based access for Students, Teachers, and Admins.
- Principle of least privilege: users can only access features necessary for their role.
- Secure authentication mechanisms for all users.

How it Helps:

- Prevents students from accessing admin or teacher functionality.

Security Analyst and Red team lead

- Limits potential damage from compromised accounts.
- Ensures only authorized users can mark attendance or perform overrides, reducing fraud.

2. **Attendance Data Policy**
   Policy:

- Attendance records are stored in a secure database (source of truth), not directly in Excel.
- All changes are logged, including timestamps, user, and reason.
- Access to attendance data is restricted to authorized roles.

How it Helps:

- Protects the integrity of attendance records from tampering.
- Ensures transparency and accountability for all changes.
- Maintains privacy by limiting access to sensitive data.

3. Device & Network Policy
   Policy:

- Each student account must be linked to one registered device only.
- Attendance submissions are allowed only when connected to the school's approved Wi-Fi network.
- Device sharing between students is strictly prohibited.
  How it Helps:

- Prevents students from marking attendance using another student's device.
- Ensures attendance reflects actual physical presence on campus.
- Reduces risk of spoofing or remote check-ins.
- Helps the system accurately detect and flag suspicious activity if multiple accounts attempt to use the same device or network.

4. **QR Code Policy**
   Policy:

- Static QR codes are assigned per venue.
- QR codes cannot be copied, shared, or reused outside the allowed session.
- QR codes are valid only during the allowed attendance window.

How it Helps:

Security Analyst and Red team lead

- Prevents students from using QR codes to mark attendance fraudulently.
- Enforces session-specific timing so only valid check-ins are accepted.
- Simplifies attendance tracking while maintaining security.

5. Audit & Logging Policy
   Policy:

- All actions—manual overrides, failed attempts, and suspicious activity—are logged.
- Logs are tamper-proof and regularly reviewed by authorized personnel.

How it Helps:

- Creates accountability for teachers, admins, and students.
- Detects and investigates suspicious behavior or attempted fraud.
- Supports compliance with institutional and legal auditing requirements.

6. **Fraud Prevention Policy**
   Policy:

- Duplicate submissions are blocked.
- Attendance submissions from unregistered devices or off-campus networks are rejected and flagged.
- Only one device per student is allowed.
- Rule-based enforcement for timing, network, and device constraints.

How it Helps:

- Stops students from marking attendance multiple times or from unauthorized devices.
- Alerts teachers to unusual activity before it becomes an issue.
- Maintains system integrity without requiring manual monitoring.

7. **Manual Override Policy**
   Policy:

- Only authorized teachers or admins can perform overrides.
- A reason must be provided for all manual changes.
- All overrides are logged in the audit system.

How it Helps:

Security Analyst and Red team lead

- Ensures overrides are justified and accountable.
- Prevents unauthorized manipulation of attendance records.
- Maintains a clear audit trail for compliance and review.

8. Red Team Testing Policy
Policy:

- Simulated attacks are conducted in a controlled environment.
- Real student data cannot be corrupted.
- All findings, including vulnerabilities and attempted exploits, are documented and shared with developers.
  How it Helps:
- Identifies weaknesses before students or attackers can exploit them.
- Ensures security controls are working as intended.
- Provides actionable insights for system improvements.

9. Security Review Policy
Policy:

- Logs, flagged activity, and Red Team findings are reviewed regularly.
- Security rules and controls are updated as needed.
- Continuous monitoring ensures the system adapts to evolving threats.
  How it Helps:
- Keeps the system resilient against new attack techniques.
- Detects and prevents emerging fraudulent behaviours.
- Supports ongoing improvement of security and reliability.

Summary:
These policies collectively ensure the attendance system is:

- **Accurate** – only valid students can mark attendance
- **Secure** – prevents unauthorized access and fraudulent activity
- **Auditable** – all actions are traceable and transparent
- **Reliable** – system functions automatically without daily intervention
- **Maintainable** – security is proactive, not reactive