Transaction Processing Engine Security Code Audit

1. Overview

This document summarizes the security audit of the Transaction Processing Engine (TPE) source code. The audit was conducted to identify potential vulnerabilities, insecure coding practices, and opportunities for strengthening the security posture of the engine.

2. Scope

- Authentication and Authorization Logic
- Input Validation and Sanitization
- Transaction Integrity
- Error Handling and Logging
- Sensitive Data Handling

3. Methodology

1. Manual code review
2. Static analysis by security tools
3. Business logic validation

4. Findings Summary

#	Risk	Description	Status
1	High	Insufficient input validation in transaction endpoint	Unresolved
2	Medium	Verbose error messages reveal sensitive info	In progress
3	Low	Lack of logging for failed authentication attempts	Resolved

5. Notable Code Sample

```
if(!isAuthenticated(user)) {
    console.log("Auth fail for user: " + user.username);
    throw new Error("Authentication failed");
}
// Missing input validation here!
processTransaction(txnData);
```

6. Recommendations

- **Sanitize all input:** Ensure all API endpoints perform schema validation before processing.
- **Review logging statements:** Avoid leaking sensitive data in errors and logs.

- **Strengthen authentication controls:** Implement account lockout and monitoring for repeated failures.

7. Conclusion

The audit revealed key areas for improvement in input validation and error handling. Remediation of the above findings is strongly recommended prior to production deployment.