

Application Architecture

Security Review - Findings (2/3)

- Access controls
 - feasibility of using ip filters, client certificates for Client PC access control
 - application architecture does not specify User authentication and authorisation details
 - ➡provide authentication, authorisation policy details
- Database security
 - ➡use an encrypted connection (SSL/TLS) and mutual authentication
 - ➡missing information for data backups

Application Architecture

Security Review - Findings (3/3)

- Secret management
 - the details regarding secret management are not available
 - ➡ provide information for secret management -> rotation, backup, access.
- Logging and monitoring
 - important to log and monitor all access and activity related to the web application and database to detect and respond to any security incidents
 - ➡ provide log format details and monitoring setup