SINGU

Security Standards

VELIS
REAL ESTATE TECH

Security Standards

Author: Aleksander Procki, System Architect

Introduction

DOCUMENT SCOPE

This document describes application and infrastructure security standards delivered by Singu platform. It covers application security mechanisms, infrastructure security and security procedures.

Application Security

1. COMMUNICATION SECURITY

Encryption & SSL enforcement

System enforces communication encrypted via HTTP protocol. The usage of SSL 2, SSL 3 and TLS 1.0 is not allowed.

HTTP Headers

System adds the following HTTP headers to each non-static request:

- X-Frame-Options
- X-XSS-Protection
- X-Content-Type-Options
- Strict-Transport-Security
- Content-Security-Policy

2. SESSION SECURITY

Session termination

Session lifetime is limited and can be configurable.

Secure cookies only

System uses http-only and secure attributes for session cookies.

CSRF protection

Application uses CSRF tokens for certain type of requests to lower the risk of Cross-site request forgery attacks.

3. INPUT DATA FILTERING

XSS protection

Application filters user/API input data by stripping HTML by default to lower the risk of Cross-site scripting attacks.

Malicious email protection

Each e-mail message imported by Singu system is washed from potentially dangerous code.

4. REQUEST THROTTLING

Request limits

The administrator can optionally limit the number of client requests within a given time-frame. Requests are measured per IP address and per session id. There are different settings:

- Total request allowance
- Total login request allowance
- Total API requests allowance
- Penalty for exceeding the limit

5. ACCESS CONTROL LISTS

Privileges and roles

Singu has a role-based authorization process. Role is a set of privileges. Each user must be assigned to at least one role. External users (tenants, service partners) can only have one fixed role. For individual users some custom access settings may be applied (for example one can grant or revoke a privilege that is not part of user's role).

Extended business restrictions

Besides privileges management (ACL) other access and visibility restrictions are related with business data & settings of user account (limitation to access certain buildings, tenants etc).

Privilege verification

Each request not marked as public is checked against a required privilege.

6. DATA PROTECTION

SQL Injection prevention

Singu lowers the risk of SQL Injection attacks e.g. by using variable binding.

Download wrappers

File downloads requests use wrappers that check user privileges.

Mobile App encryption

Singu mobile application uses in-app database encryption.

7. AUTHENTICATION SECURITY

SAML authentication

Singu supports Single-sing-on user authentication by external IdP based on SAML protocol.

API security

Singu provides a REST API for certain requests. API calls require token-based authentication. Authentication token has expiration time and must be refreshed with a refresh-token. REST API client runs with the same user privileges as the web app.

Password security

In case SAML authentication or any other authentication service cannot be applied (i.e. for external users) Singu enforces the following password security policies:

- System requires strong passwords and password complexity may be individually configured. By default, system requires at least a 10 characters long password, with variable case letters, at least one digit and at least one special character. Password cannot contain user's login.
- Password has an expiration date (30 days by default) and must be changed after exceeding that period. You cannot reuse one of 10 passwords used before.
- Any authentication request is logged with information about who and when performed it
- There is a limit of 5 unsuccessful login attempts. After exceeding that limit account is locked and user must request administrator to unlock it
- Passwords are stored as hash encrypted with Blowfish algorithm

8. LOGGING MECHANISMS

Action logs

Singu logs user actions in several independent logs depending on action context.

There are:

- User Tracking Log - contains each client request sent to the server (including IP address, time, user agent etc). This log includes API call as well as regular web app request
- Authentication Log - system logs authentication requests, including failed or successful login, password change, mobile application login with authorization token
- ACL Change Log - system logs modifications of the ACL matrix (assigning/revoking a privilege to/from role, assigning/revoking a privilege to/from user, assigning/revoking a role to/from user)

Error logs

Singu report errors depending on their origin.

There are:

- Application Error Log - system logs exceptions, errors and warnings raised by application
- Database Error Log - system logs errors raised by database

System logs

Singu system has several additional system logs:

- Notification Log - contains every notification sent by Singu including recipient list
- Scheduled Jobs Log - system does have a schedule for cyclic jobs. Each automatic job execution is logged. Singu logs not only errors, but any successful job execution is also logged.

Logs are kept for a limited amount of time and can be accessed by Velis administrators.

Infrastructure Security

1. BACKUP POLICY

Continuous database backup

Application database is backed up with the possibility of PITR (Point-in-time recovery).

Files & Services configuration backups

Files uploaded by the users (attachments, etc.) are backed up periodically (by default every 24 hours but can be reduced to 1 hour by a configuration update).

OS services can be installed and configuration can be applied via automated scripts.

2. DATA RECOVERY

Disaster Recovery Plan

Singu has a DRP solution and backup (mirror) of whole application as well as database data. The DRP is checked with automated tests.

High Availability

Vertical High Availability is available by default. Horizontal High Availability can be implemented in the future and would include separation of web servers and permanent storage. Disaster Recovery is run on the machine where offline backups are hosted.

3. SANITY CHECKS

Continuous monitoring

There is uptime monitoring system installed off-site that constantly provides sanity checking and provides IM/ e-mail notifications in case of downtime.

4. SYSTEM AND FACILITIES

Application environment isolation

Each application instance (for a given client) is physically separated from other application (not including any virtualization level done by AWS). Vendor's staff has limited access to each instance, based on their competences and project assignment matrix. Each login to the application and created session id is logged. Access to the servers for maintenance is restricted to selected playbooks without root access.

Security Procedures

1. SERVICES SECURITY

Security updates

Security patches released by the vendor of the operating system are applied on a regular basis.

2. OWASP REGULAR AUDITS

Penetration tests

There are regular penetration tests conducted by independent external company. These tests are performed with use of OWASP Top 10 risks detection methodology.

Any issues reported during audit is being pathed and followed by Re-tests and Post-audit Report.

3. SYSTEM MONITORING

Incidents & Error logs monitoring

System logs are continuously monitored. Any unhandled application error is instantly reported to the support team which analyzes the issue. If it's a software application bug, then development team prepares a hot fix, which – after passing standard test and code review procedure – can be applied to production environment.

4. UPDATES SECURITY

Automated tests

Each source code update is followed by a series of automated tests that verify code standards and detect potential regression bugs.

Code review

Each source code update is followed by code review that includes security review.