RSpace

Security Overview

Security in RSpace

This document explains some of the security procedures and strategies used to keep users' data and details secure.

Password security

In 'stand-alone' mode (i.e. not using an institution's SSO mechanism to authenticate users), RSpace maintains its own authentication mechanism and credentials database.

- Passwords created by the user must be at least 8 characters long, not be identical to the username, and not belong to a common password blacklist (e.g., 'password'). This blacklist is editable by system administrators.
- Passwords are salted with a unique 16 byte prefix generated by a cryptographically secure random number generator and hashed using the SHA-256 algorithm before persisting to the database. In this way the plaintext password is never stored, and, in the event of the password table becoming compromised, it is not immediately susceptible to dictionary or rainbow table attacks.
- To prevent brute-force password guessing attacks, accounts are locked out for a short time after a number of consecutive unsuccessful logins. All login attempts are logged to a security event log.
- Auto-completion of input fields is disabled for login and signup pages.
- We also recommend that for admin role accounts, end-users follow good practice by disabling password-storing in their browsers.
- After logout, sensitive pages are not cached in the browser.
- Plain-text passwords are never emailed to the user as a result of password reset / forgotten password workflows.

If RSpace is deployed in an institution using SSO, then it is the institution's responsibility to safeguard passwords.

Network security

We recommend that RSpace runs over a secure HTTPS connection which encrypts the communication channel between client and server and also verifies the identity of the endpoint by SSL certificates issued by a recognized Certification Authority.

Database security

- No direct access to the database is possible by end-users.
- All SQL queries use Prepared Statements to defend against malicious user input.
- The database itself is not encrypted, but OS-level encryption can be used if necessary.
- The RSpace database runs using limited permissions.

Resource Authorization

Privacy of the user’s content depends on RSpace's authorization policy. All access to ELN entries or resources requires authenticated access by default, and URL paths are protected by user roles.
At a fine-grained level, access to individual records is controlled by a combination of Access Control Lists (ACLs) and user-specific permissions. Every action (e.g., Read, Edit, Delete, Export, Copy) is authorized at the server level before proceeding - RSpace does not solely rely on controlling the actions available in the UI, as these may be circumvented by URL-guessing attacks.

For example, a user has authorization to edit content created by him/herself, but must be granted permission to access content created by other members of his/her group. To access content created outside a lab group, all PIs or RSpace managers of the groups concerned must accept the sharing request. Otherwise, the content is not accessible. A request to view a record, for example at '/notebook/view/123/' will check for the authenticated user's permission to access record 123 before proceeding.

For more coarse-grained permissions - for example, global admin permissions - we use Role Based Access Control (RBAC) to restrict the available functionality to the user’s role.

Defence against malicious use

We are guided by OWASPs guidelines on securing web applications and aim to be at least level 1 compliant in their Application Security Verification Standard (ASVS). Here, we briefly enumerate our policies in the following Control areas:

Authentication & session management (A2)

- Failed logins give no information about reason for failure.
- User names are never used in URLs.
- Users are informed at each login when their last login was, so they can see if anyone has impersonated them since their last session.
- A security event logs all login attempts.
- To minimize brute force attacks, accounts are temporarily locked after 3 unsuccessful logins.
- RSpace uses secure random number generators to generate session keys.
- Sessions expire after a short time of inactivity. Users performing sensitive operations must re-authenticate at the time of the operation (e.g., password resets, signing documents, etc).
- **Browser caching** - Our policy in this are is guided by OWASP's guidelines at (https://www.owasp.org/index.php/Testing_for_Logout_and_Browser_Cache_Management_%28OWASP-AT-007%29). In brief, sensitive data such as login pages, signup pages, user profile pages, and any pages only accessible to a ROLE_ADMIN or ROLE_SYSADMIN are returned from the server with HTTP headers set to prevent browser caching. When a user logs out (or his session expires due to inactivity) the session is invalidated, and clicking on the browser's 'Back' button will trigger a reload from the server for these pages, which will redirect to the login page.

Authorization of resources

Access to resources is controlled by a combination of Role Based Access Control and instance-based permissions (Access Control Lists).

Cross-Site Request Forgery

Only same-origin POST requests are permitted.

Cross-site scripting

All user input submitted to the server is filtered before being sent back to the client for display.

Client side libraries use ‘safe’ Javascript methods to manipulate user input - e.g., jQuery’s text() method.

Injection

User input is validated.

Exclusive use of prepared statements guards against SQL injection attacks.

Current libraries -A9

We regularly update libraries and 3rd party software components to ensure the latest security fixes are in place.

Security event logging

All security events are logged to a dedicated Security log whose output can be consumed by a SEM tool.

Revision history and audit trail

The revision history records all changes made to research records over time. RSpace keeps a full record of this, including timestamps. The audit trail records events on the system - document edits and updates are recorded.

Testing and audits

We regularly get CREST-accredited independent penetration testers to evaluate RSpace using manual and automated methods. The latest test was May 2017. We are happy to discuss findings with customers or serious potential customers.