Security Policy

This document describes our security policy. We cannot guarantee that no leak will ever happen, but we do our best to keep your data safe.

Your data

Please see our Privacy Policy concerning how we manage your data.

How we develop secure software

- We use code reviews to detect vulnerabilities before merging and delivering to customers,
- We ensure that we check for permissions for any resources we have, and we regularly review those permissions,
- We use Git to manage changes, so that any code that goes to production is easily auditable.

How we keep our communications secure

We make our best to use state-of-the-art techniques to keep the data safe:

- We use SSH keys to access our servers,
- We use HTTPS and SSL certificates to communicate between us and with you.
- We don't transfer data in clear-text over the network.

How we keep the data secure

Once again, we make our best to use state-of-the-art techniques to keep the data safe:

- Our main servers are hosted by Digital Ocean, which has extremely good security procedures: https://www.digitalocean.com/legal/data-security/
- The hard drives of our personal computers are encrypted (for example with Apple's FileVault 2),
- Our personal backup drives are encrypted (for example with Apple's FileVault 2 / Time Machine).

Where we host your data

Please see the Privacy Policy on where we store data.

How we ensure continued security

Whenever we are aware of a leak affecting the software we use (for example Heartbleed or Shellshock), we halt the service in emergency and upgrade our systems.

If you notice a vulnerability, please contact us at security@play-sql.com.