Rails Security

Lei Li

Agenda

- Session & Cookie
- User Input
- Database
- Configuration
- Rails & libs bugs

Session & Cookie

- Cookie based session
- Data in cookie

User Input

- CSRF - RESTful / csrf_token
- XSS - h / sanitize
- File download/upload
- System command - system()
- HTTP Request methods
- Redirection
- Regular Expression - /^$/ vs /\A\Z/

Database

- Mass assignment - attr_accessible, attr_protected
- SQL injection - use native method / sanitize sql
- Unscoped finds
- Batch update - update_all

Configuration

- Running environments
- Passwords
- Filter logs parameters - log / backtrace
- Routes - default routes

Rails & libs bugs

- …
- …

Thanks!

Lei Li