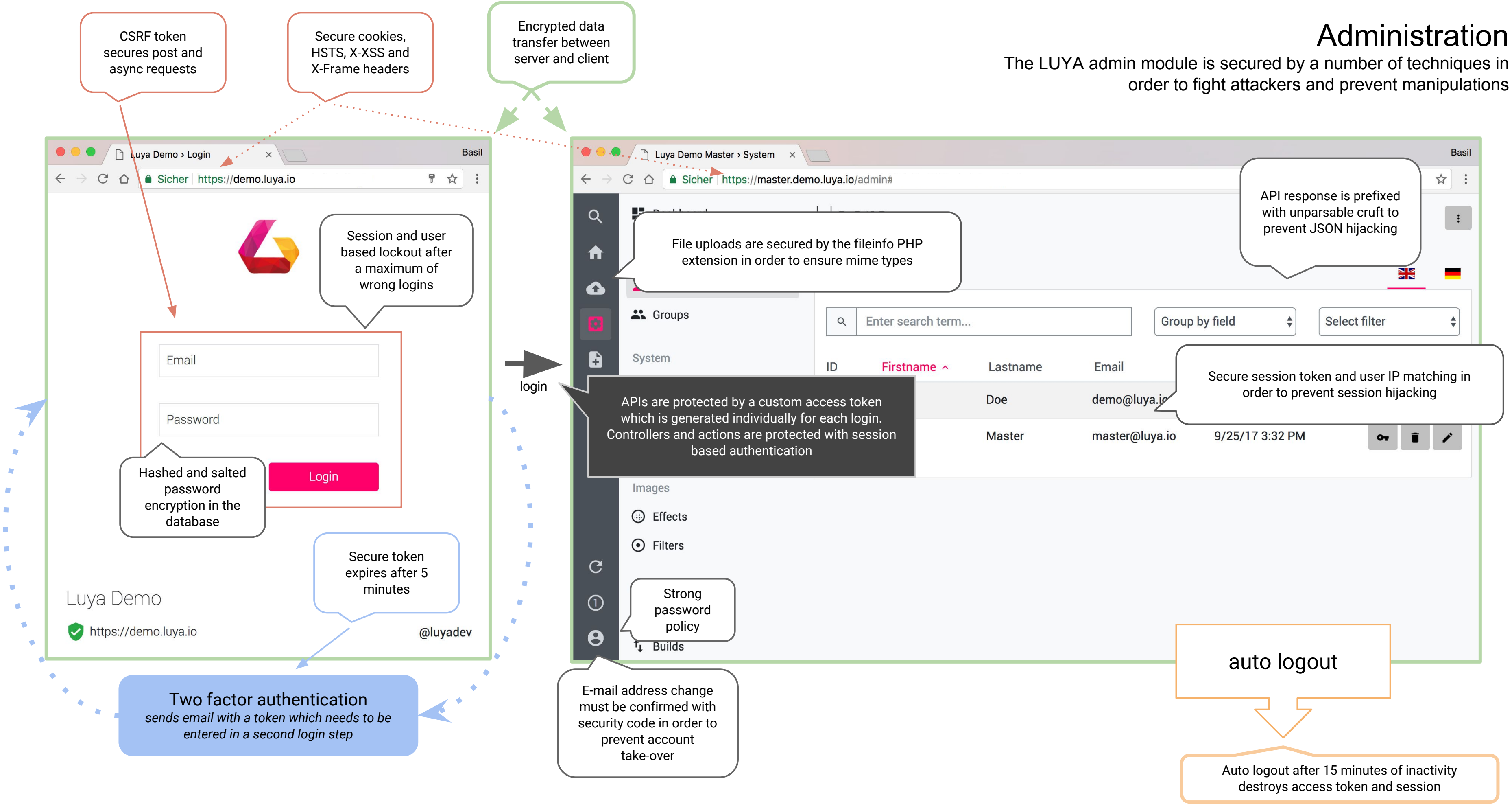
LUYA SECURITY

A brief visual overview of what we do in order to secure your web application

LUYA is powered by the Yii Framework which secures the application level implementations.
While we do everything to keep LUYA as secure as possible, no guarantee can be given and the system has to be used at your own risk.

Administration

The LUYA admin module is secured by a number of techniques in order to fight attackers and prevent manipulations



CSRF token secures post and async requests

Secure cookies, HSTS, X-XSS and X-Frame headers

Encrypted data transfer between server and client

Session and user based lockout after a maximum of wrong logins

Hashed and salted password encryption in the database

Secure token expires after 5 minutes

Two factor authentication

sends email with a token which needs to be entered in a second login step

File uploads are secured by the fileinfo PHP extension in order to ensure mime types

API response is prefixed with unparsable cruft to prevent JSON hijacking

Secure session token and user IP matching in order to prevent session hijacking

APIs are protected by a custom access token which is generated individually for each login. Controllers and actions are protected with session based authentication

Strong password policy

E-mail address change must be confirmed with security code in order to prevent account take-over

auto logout

Auto logout after 15 minutes of inactivity destroys access token and session

LUYA is powered by the Yii Framework which secures the application level implementations.
While we do everything to keep LUYA as secure as possible, no guarantee can be given and the system has to be used at your own risk.

Administration Infos

In addition to security techniques LUYA also keeps track of what is done by whom and when

- Any data change in the administration is logged with information about who changed what and when.
- Any user login is documented, with the user’s IP address and access token.
- A user can only be logged in once. Concurrent logins by the same user are avoided by terminating the previous session.
- The two-way factor authentication sends a custom token to the user’s email which has to be entered to complete login, therefore brute forcing is hindered and insecure passwords become less of a risk.
- We do not provide extension installation via a web interface – all extensions and modules are implemented via composer, therefore versioning and bug fixing is enforced.
- LUYA stores configurations and data in files so they can be tracked via VCS systems like GIT and a full change history is provided.

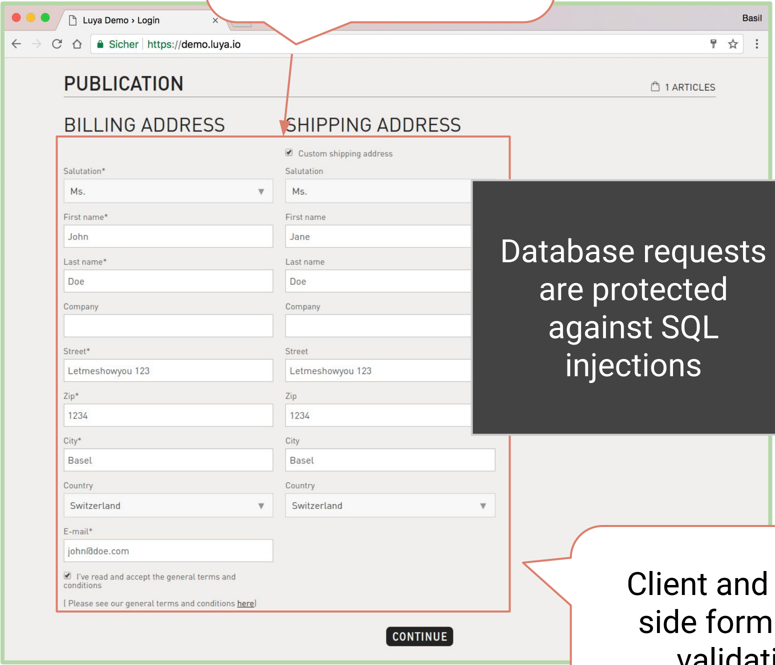
Read more about how to configure a secure LUYA application:

https://luya.io/guide/app-security

Frontend

Security measures of the website's frontend

CSRF token secures requests



Luya Demo › Login ×

Basil

Sicher | https://demo.luya.io

PUBLICATION

1 ARTICLES

BILLING ADDRESS

SHIPPING ADDRESS

	☑ Custom shipping address
Salutation*	Salutation
Ms. ▼	Ms.
First name*	First name
John	Jane
Last name*	Last name
Doe	Doe
Company	Company
Street*	Street
Letmeshowyou 123	Letmeshowyou 123
Zip*	Zip
1234	1234
City*	City
Basel	Basel
Country	Country
Switzerland ▼	Switzerland ▼
E-mail*	
john@doe.com	

☑ I've read and accept the general terms and conditions

(Please see our general terms and conditions here)

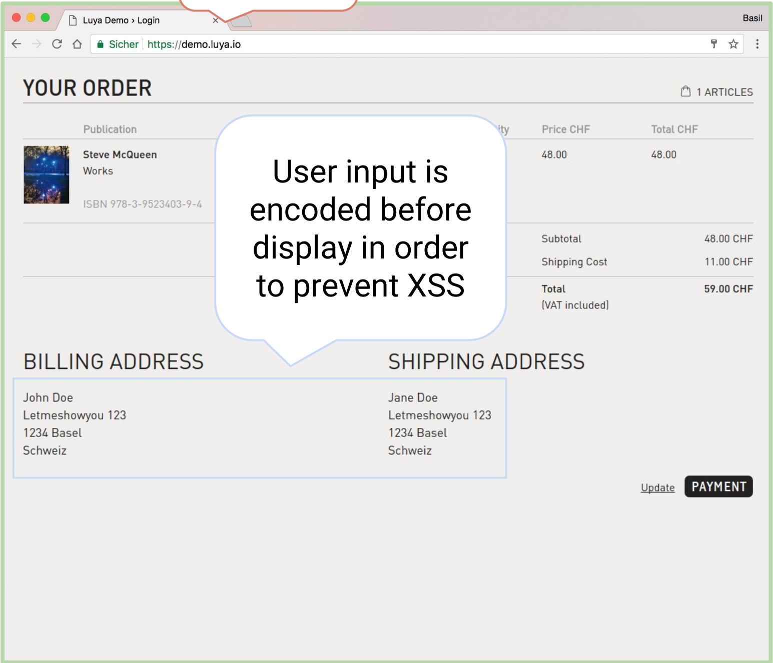
CONTINUE

Database requests are protected against SQL injections

save

Encrypted data transfer between server and client

Secure cookies, HSTS, X-XSS and X-Frame headers



Luya Demo › Login ×

Basil

Sicher | https://demo.luya.io

YOUR ORDER

1 ARTICLES

Publication	ity	Price CHF	Total CHF
Steve McQueen Works ISBN 978-3-9523403-9-4		48.00	48.00
		Subtotal	48.00 CHF
		Shipping Cost	11.00 CHF
		Total (VAT included)	59.00 CHF

BILLING ADDRESS

John Doe
Letmeshowyou 123
1234 Basel
Schweiz

SHIPPING ADDRESS

Jane Doe
Letmeshowyou 123
1234 Basel
Schweiz

Update PAYMENT

User input is encoded before display in order to prevent XSS

Client and server side form input validation

LUYA is powered by the Yii Framework which secures the application level implementations.
While we do everything to keep LUYA as secure as possible, no guarantee can be given and the system has to be used at your own risk.

Prevention technics in depth

The frontend technics used to protect the application.

- All database requests are protected against SQL injections by the Yii 2 database abstraction layer, **data binding (filtering out malicious inputs) is used for all SQL statements**.
- CSRF: Cross-site request forgery (CSRF) is a typical web application vulnerability. It is based on the assumption that a user is authenticated at a legitimate website. Then he's visiting an attacker's website which issues requests to the legitimate website using JavaScript code, a form, <img src=""> tag or other means. This way, attackers could, for example, reset a victim's password or transfer funds from his bank account (in case the bank’s website isn't secure, of course). In order to prevent such request forgery, **we use an encrypted token which is stored on the server and client side and is compared on each request**.
- MITM: Man in the middle attacks are prevented by using encrypted data transfers between client and server as **we use SSL**.
- XSS: Cross site scripting is commonly a problem when user data is returned, therefore **we use an encoding and HTML purifying technique**.
- To prevent attackers from stealing the cookie used to authenticate the user on the remote server and create a false identity to take over the user’s session, **we store the access token in combination with the IP address and compare those values on each request.**
- File uploads to the storage system can contain dangerous files which then expose system informations. **We prevent this with a secure file upload which uses the PHP fileinfo extension to deep check mime types.**

LUYA is powered by the Yii Framework which secures the application level implementations.
While we do everything to keep LUYA as secure as possible, no guarantee can be given and the system has to be used at your own risk.