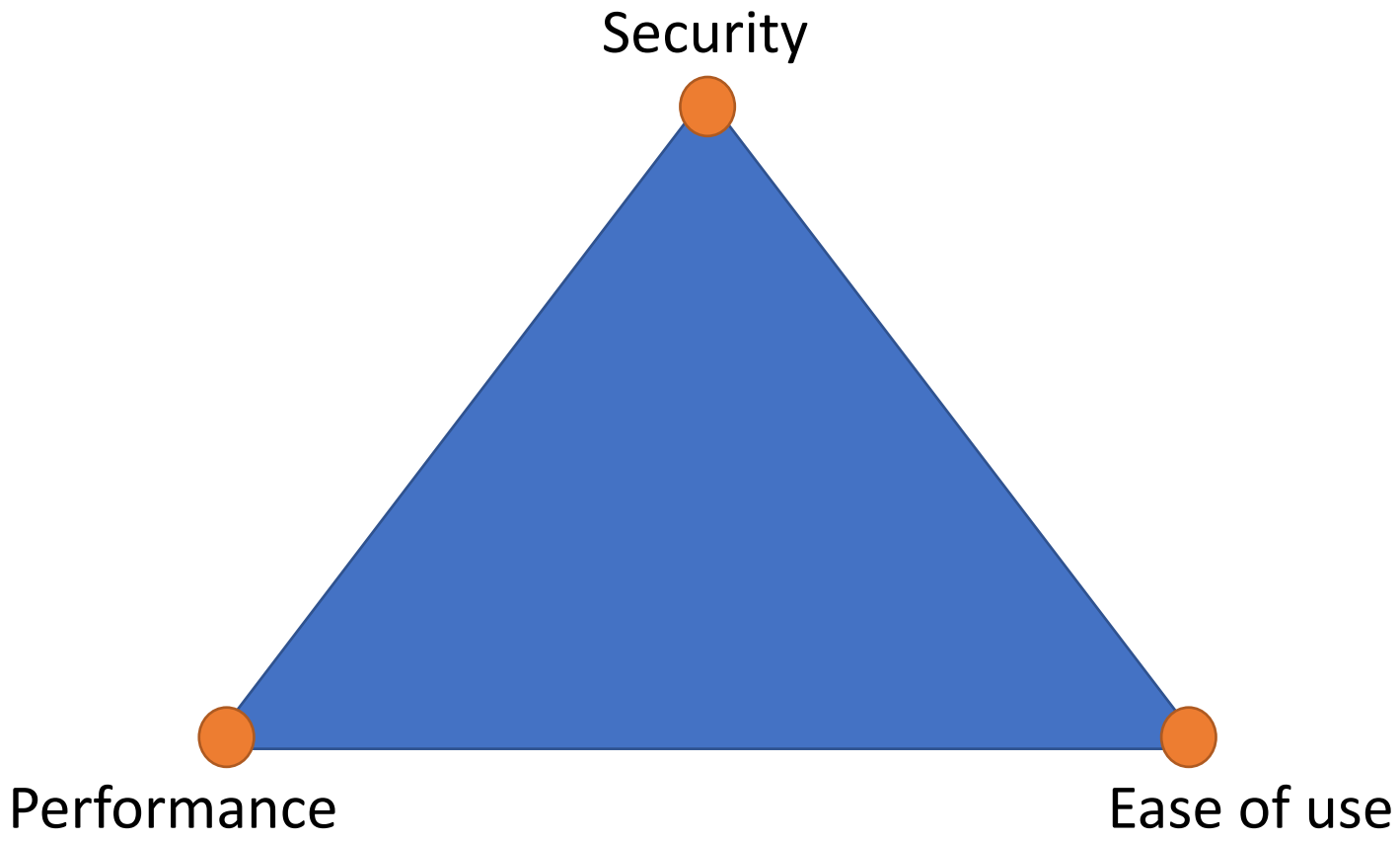
Security by Design

Harm Wibier

Where are your priorities?

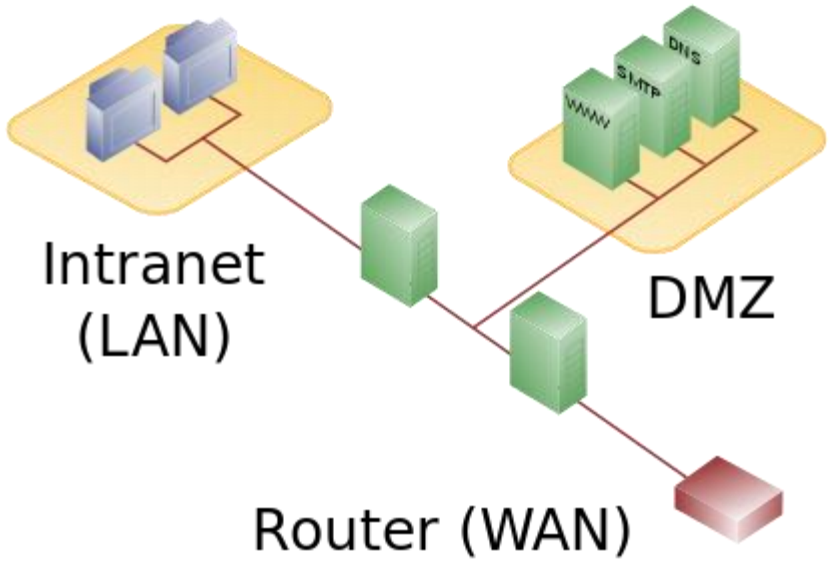


Layers of security

- Network configuration
  - SPLF
- Server configuration
  - Run webapps under a different windows user
- Application logic
  - New redaction layer
  - Xss Sanitizer
  - SQL Injection

SPLF?

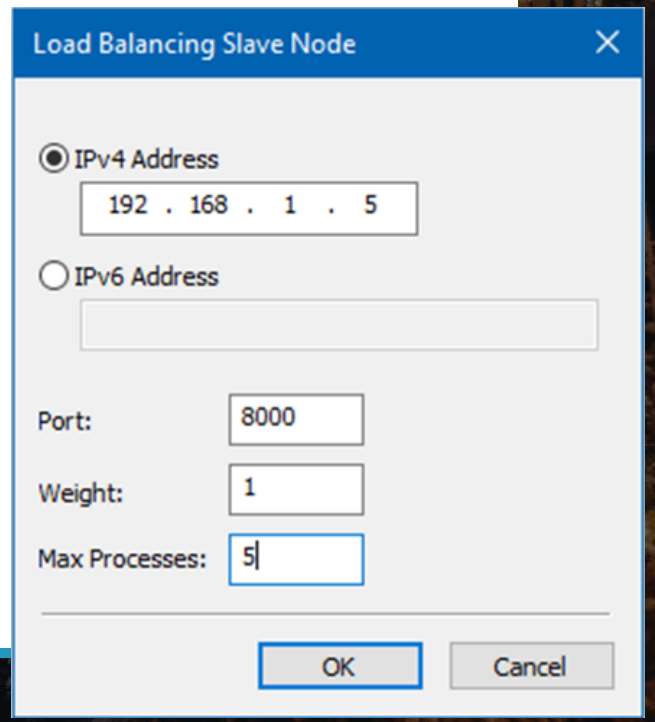
- Separate web server from application server
- Balance load over multiple application servers
- Web server is placed inside DMZ



Stability Feature

SPLF Improvements in DataFlex 2021

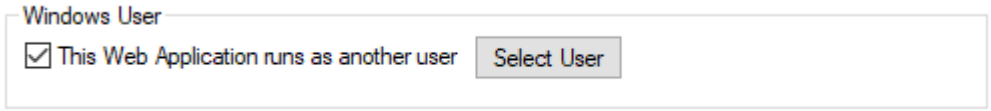
- Improved handling of starting and stopping application servers
  - Two way communication between master and application servers
  - Detection of irresponsive application servers
- Configure maximum amount of processes per application server
  - Prevents machine overload
  - Prevents potential licensing issues



Windows account

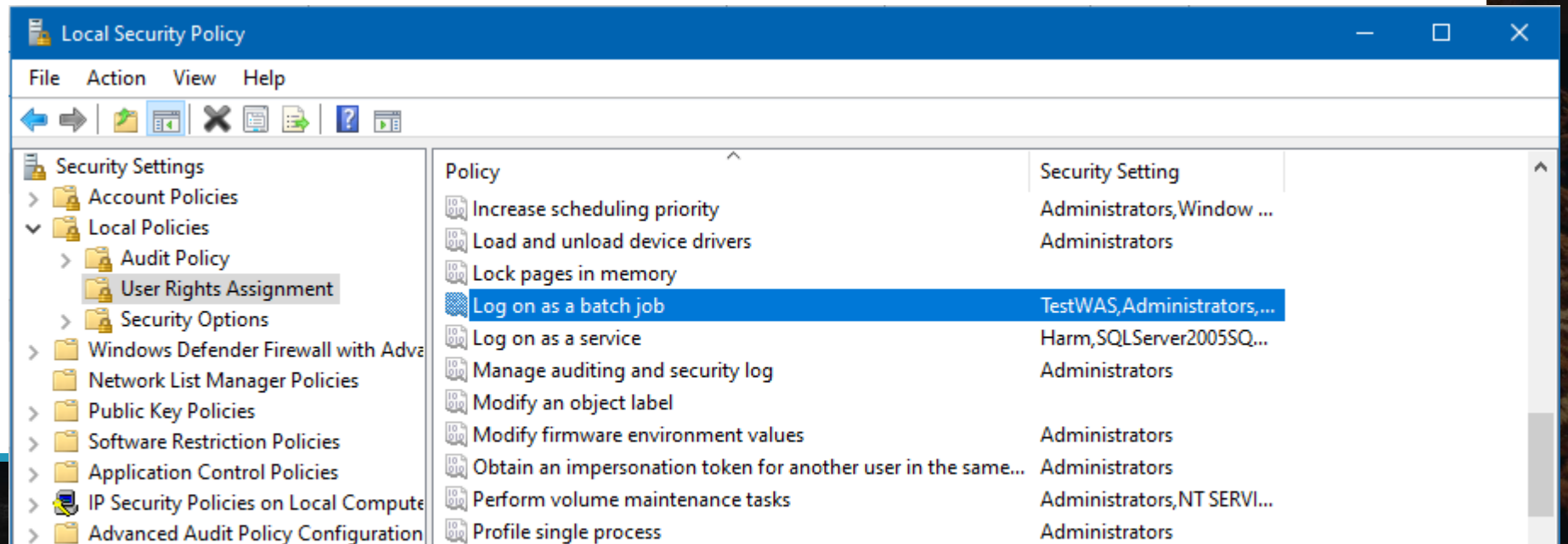
- Configure a windows account per WebApp
  - Used when starting processes
  - Allows tuning of machine rights
  - Better separations of webapps sharing a server
  - Use windows authentication on SQL Server
  - Access network shares

Type	Value
Current Sessions	0
Peak Sessions	0
Total Sessions	0
Current Processes	2
Peak Processes	2
Total Processes	2
Client Messages	0
Server Messages	0
Time	00:24:38
Last Accessed	00:24:36
Running as user	Harm



User Account Requirements

- Has the following group policies enabled
  - Log on as a batch job
  - Allow log on locally
- Has a functioning profile




Redaction

New security layer in DataFlex 2021

- Prevent unintended exposure of data and operations
  - Hidden / disabled controls
    - Controls with pbRender false are still sent to the client!
    - Developer tools can still expose data and operations!

User Interface Protection

- Prevent access to hidden & disabled controls
  - New layer on top of view access control
  - Stops communication between DEO and DD
  - Prevents server actions on hidden controls
- New Client Protected Web Property
  - Stored on the server
  - Sent to the client
  - Used for **pbRender**, **pbVisible**, **pbEnabled**

```
{ WebProperty=ClientProtected }
Property Boolean pbRender True
```

API - Server Action Accessibility

AllowServerAction (cWebObject)

- The actual check which can be augmented

pbNoAccessabilityCheck (cWebBaseUIObject)

- Turn off accessibility check

IsControlAccessible (cWebBaseUIObject)

- Check if control is accessible

API – DEO Operations

pbNoUpdateIfHidden (cWebBaseDEO)

- Controls if hidden DEO's write values to the DD

pbNoFillIfHidden (cWebBaseDEO)

- Controls if hidden DEO's read values from the DD

AllowFillDEO (cWebBaseDEO)

- The actual check which can be augmented in subclasses

AllowUpdateDD (cWebBaseDEO)

- The actual check which can be augmented in subclasses

Redaction on DataFlex 19.1

- Library available
  - https://www.dataaccess.eu/resources/downloads/download-category/download-subcategory-842?dagapsg=101
- Separate pbRedact property for manual redaction
  - (no ClientProtected web properties)


XSS

Cross Site Scripting (XSS)

- Injection of (Java)Script into stored data
  - Hacker insert script into data
  - User reviews data in webapp, script gets executed
    - Hijack sessions, cookies, local storage, …
- Cross-Site Scripting (XSS) attacks occur when:
  - Data enters a Web application through an untrusted source, most frequently a web request.
  - The data is included in dynamic content that is sent to a web user without being validated for malicious content.
- https://owasp.org/www-community/attacks/xss/

When is text shown as HTML in WAF?

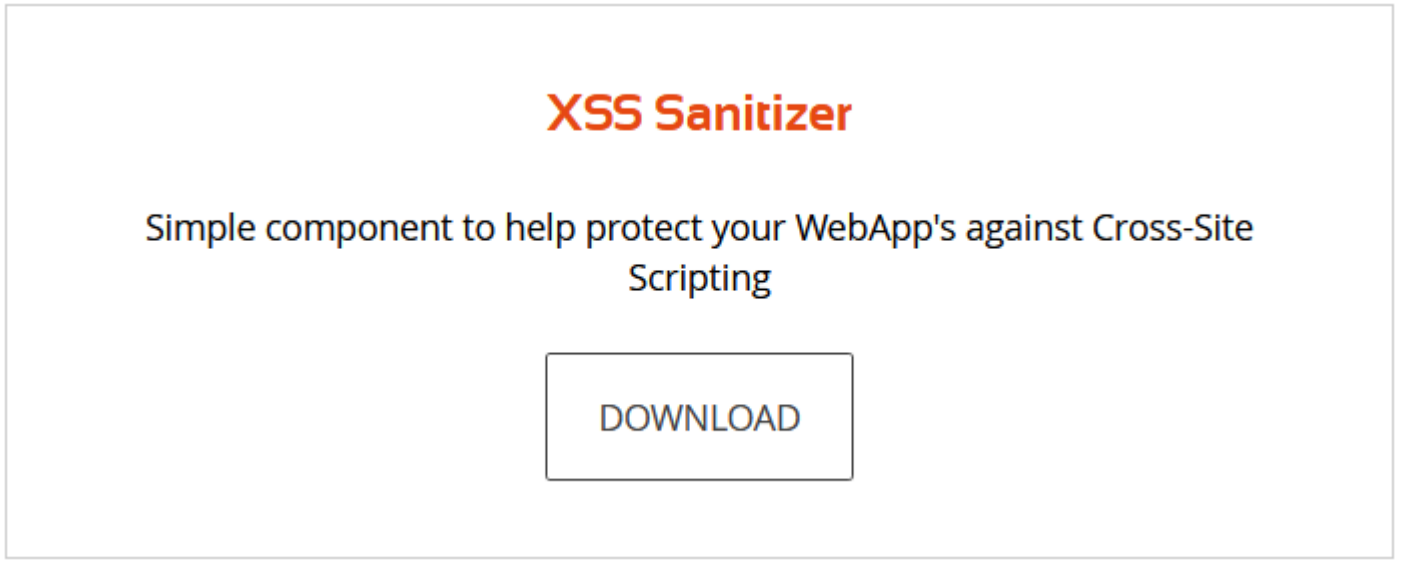
- cWebHtmlBox
- cWebHtmlList
- pbAllowHtml
  - cWebColumn, cWebTreeView, ..

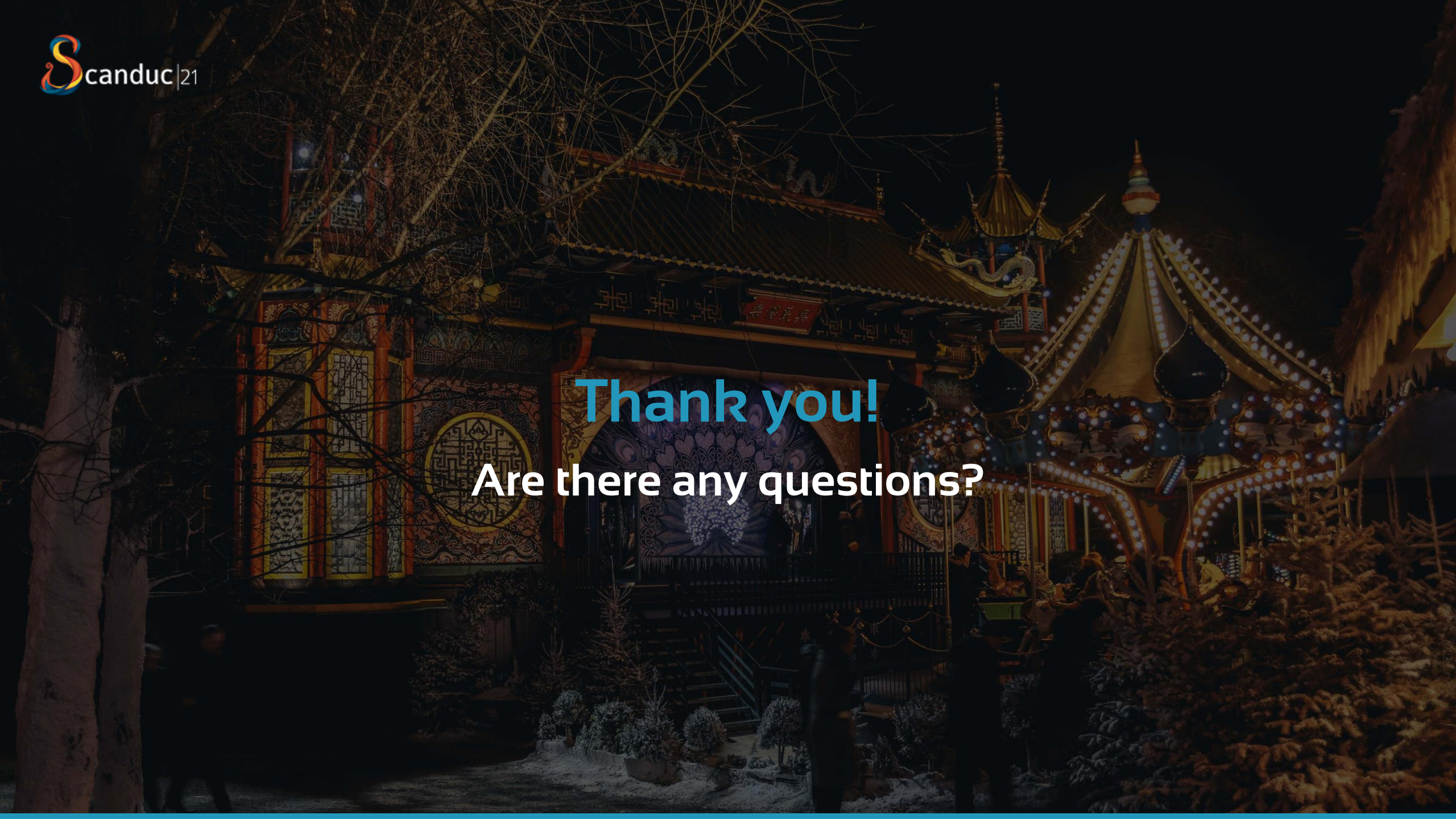
Sanitizing

- HtmlEncode
  - Will escape any HTML
    - < is changed into <
  - Use this if data is not supposed to have markup
- cXssSanitizer
  - Will cleanup HTML
  - Use this if you want allow some markup (but control what is allowed)

XssSanitizer

- Library available at www.dataaccess.eu
- Configure exactly which HTML elements and attributes you want to allow




Scanduc|21
Thank you!
Are there any questions?