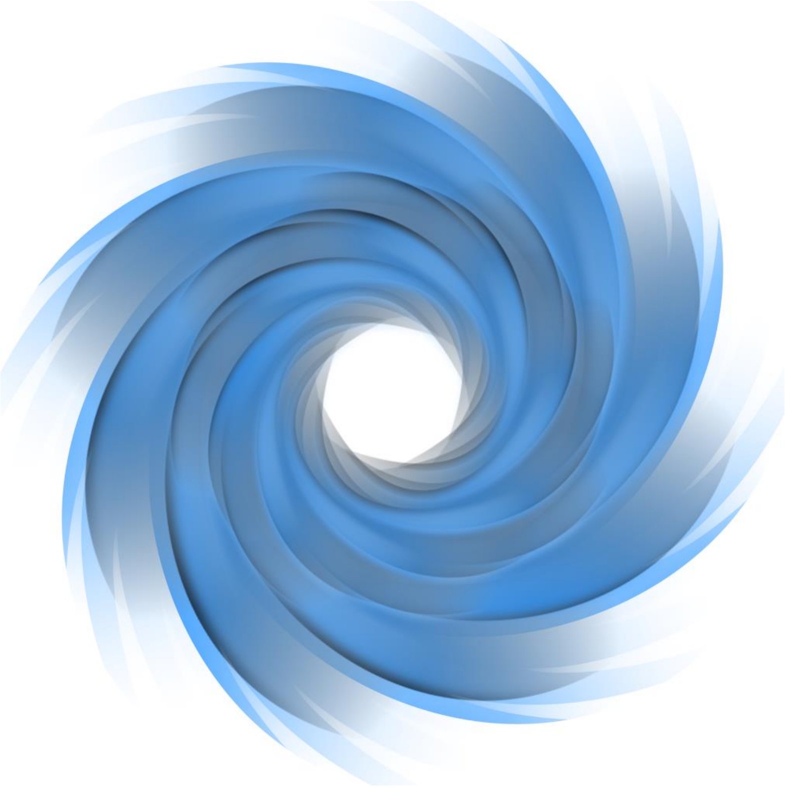
Aiming for a Safer Content Editor Web Part



Christophe Humbert

@PathToSharePoint on Github

@Path2SharePoint on Twitter

My Recently Published Solutions

- NPM modules (2022):
  - Property Pane Portal
  - Property Pane Wrap
- PnP SPFx (2022):
  - Cherry-Picked Content Web Part
  - React-PPP-*
  - React-PPW-*
- AppSource SPFx (2021):
  - inPerson (flexible office space booking)
- Github (PathToSharePoint)

It Started in Classic SharePoint

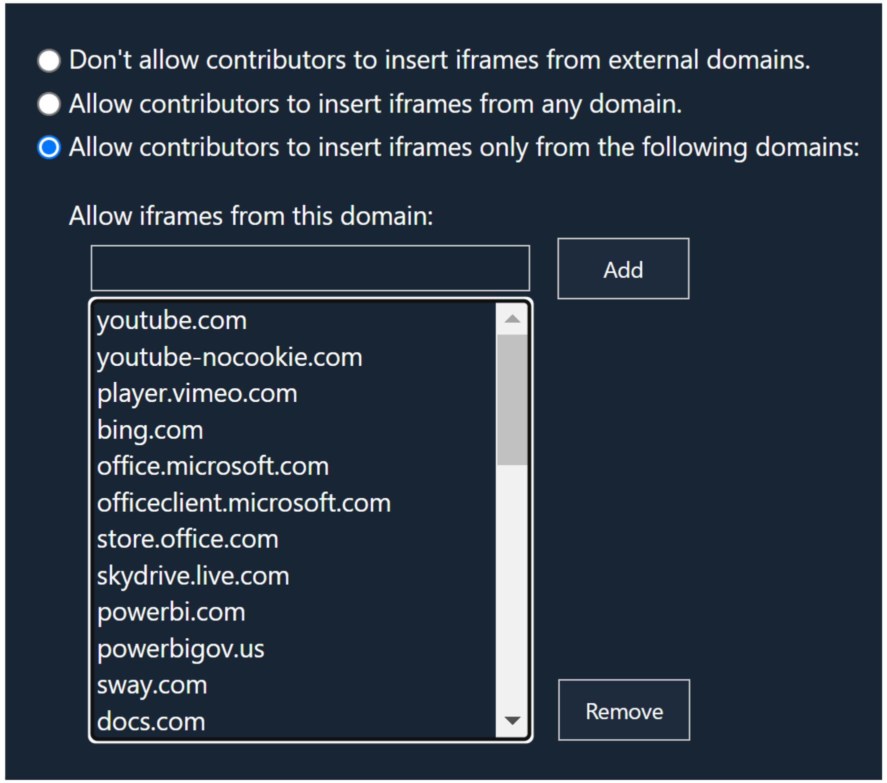
- Our custom connectors to external content and scripts
  - Content Editor Web Part
  - Page Viewer Web Part
  - Script Editor Web Part

- My love story with CEWP & PVWP (“Path to SharePoint”):
  - The HTML Calculated Column (2008)
  - The Easy Tabs (2009)
  - Gantt, calendar, etc.

The Move to Modern SharePoint

- Didn’t make it:
  - Content Editor Web Part
  - Script Editor Web Part

- New: Embed Web Part
  - Restricted capabilities
  - <script> not allowed



○ Don't allow contributors to insert iframes from external domains.

○ Allow contributors to insert iframes from any domain.

● Allow contributors to insert iframes only from the following domains:

Allow iframes from this domain:

youtube.com
youtube-nocookie.com
player.vimeo.com
bing.com
office.microsoft.com
officeclient.microsoft.com
store.office.com
skydrive.live.com
powerbi.com
powerbigov.us
sway.com
docs.com

- SPFx, yay!
  - PnP: [samples/react-script-editor · GitHub]() (Mikael Swenson)
  - [GitHub - PathToSharePoint/dangerous-content-web-part]()
  - Etc.

Why no CEWP/SEWP ?

- Issues:
  - Risk of security breach (script injection)
  - Risk of broken web part page
  - Governance
- Same issues with modern SPFx-based CEWP
- Solutions?
  - Sanitizer: remove scripting parts
    - “Safe Content Web Part” (PathToSharePoint)
    - Reliable?
    - Useless result? The code can’t do anything anymore.
    - Still the governance question
  - @mikezimm’s idea on GitHub PnP

GitHub Idea (@mikezimm)

- restrict code to snippets stored in approved repositories
  - Edit access restricted to script owners
  - Read access: all users
  - A governance approach instead of a technical approach

- Common approach in content management. Examples:
  - Content owners in an intranet
  - Who can create Microsoft 365 groups
  - Embed web part

- Ref.: issue #2228 on PnP
  Make React-Script-Editor more secure · Issue #2228 · pnp/sp-dev-fx-webparts · GitHub

Demo

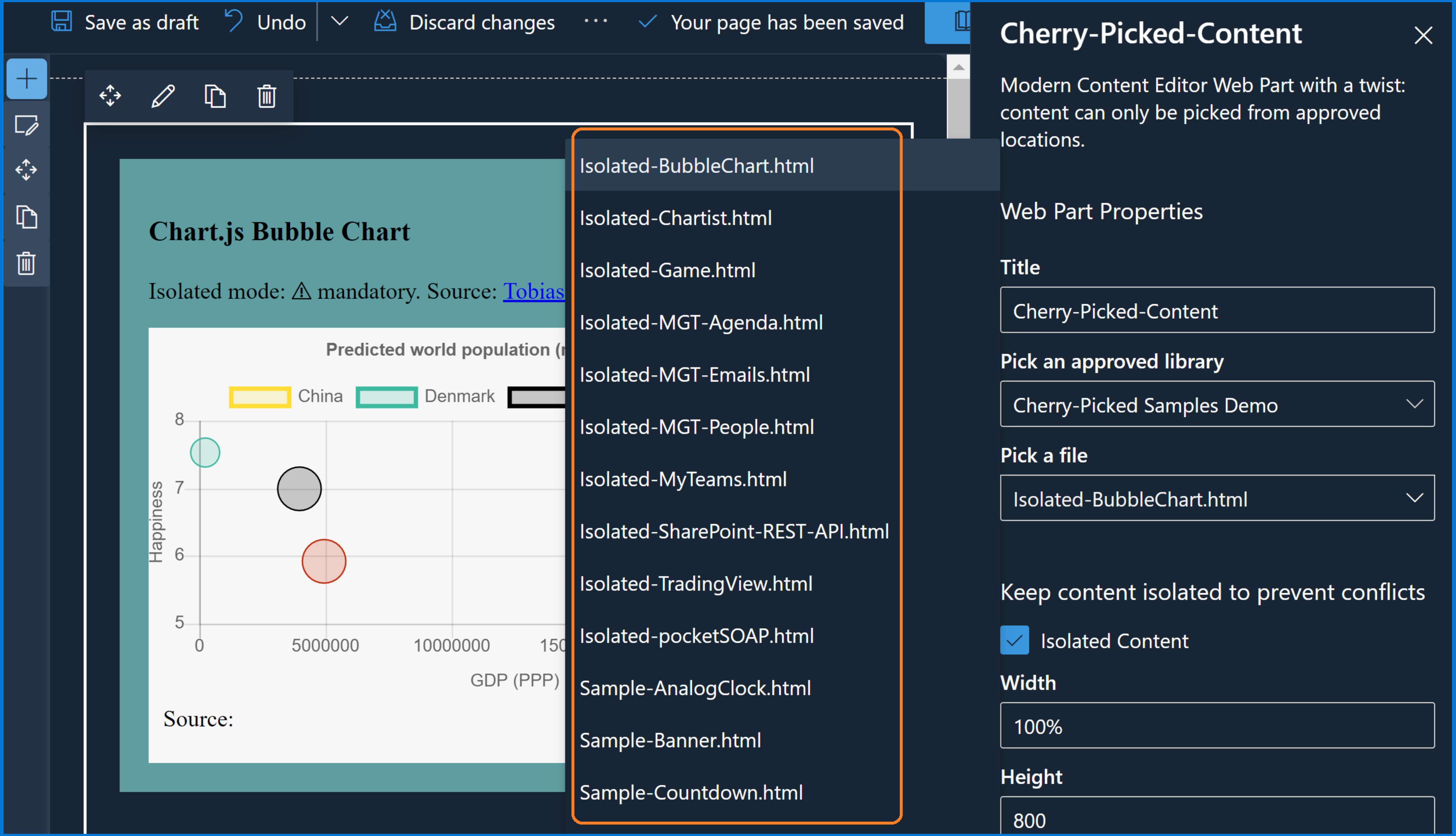


Chart.js Bubble Chart

Isolated mode: ⚠ mandatory. Source: Tobias

Source:

Cherry-Picked-Content

Modern Content Editor Web Part with a twist: content can only be picked from approved locations.

Web Part Properties

Title
Cherry-Picked-Content

Pick an approved library
Cherry-Picked Samples Demo

Pick a file
Isolated-BubbleChart.html

Keep content isolated to prevent conflicts

☑ Isolated Content

Width
100%

Height
800

Code

The Code Revealed

- Element.**innerHTML**
  - HTML5 specifies that a <script> tag inserted with innerHTML should not execute.

- Element.**setHTML()**
  - Experimental
  - Sanitizer

- **createContextualFragment()**
  - Parses tag string to convert it into a document fragment

More Code

- Approved libraries: static array
  - Could be replaced with a dynamic rule
  - Validation during editing and rendering
- Memoization: React.memo()
  - Prevents excessive re-rendering
- Two rendering modes
  - Directly in the web part
  - iframe. In this case the web part context is passed to the code snippet.
- Cascading selection in the Property Pane
  - Leverages the built-in **onPropertyPaneFieldChanged()** method

Thank you!

Special thanks to:

- Mikael Swenson
- @mikezimm on GitHub

Cherry-Picked Content Web Part – PnP Sample

sp-dev-fx-webparts/samples/react-cherry-picked-content at main · pnp/sp-dev-fx-webparts · GitHub

Path to SharePoint blog post

https://blog.pathtosharepoint.com/2022/04/19/aiming-for-a-safer-content-editor-web-part/

Dangerous Content Web Part – PathToSharePoint on GitHub

GitHub - PathToSharePoint/dangerous-content-web-part

GitHub request by @mikezimm

Make React-Script-Editor more secure · Issue #2228 · pnp/sp-dev-fx-webparts · GitHub

Microsoft Graph Toolkit Playground

https://mgt.dev

@PathToSharePoint on Github

@Path2SharePoint on Twitter