ALLAN THRAEN | 4 months ago | PDF |

Tech Talk Tips and Tricks Website Improvements Optimizely (Episerver) CMS

CHRISTMAS COUNTDOWN: #10 IF IT'S OUT THERE, GOOGLE WILL EVENTUALLY FIND IT

Have you ever forgotten to protect stuff that wasn't meant to be public? If no, then you are probably a better person than me and most others - both developers and editors alike.

The 2023 Christmas Countdown: 12 Common Pitfalls in Optimizely CMS - and how to avoid them

> *This blogpost is part of the 2023 Christmas Countdown series where I each day for the last 12 days before Christmas go through my Top 12 list of the most common and dangerous pitfalls I typically see in Optimizely (EPiServer) CMS 12 Implementations. If you want to learn more and perhaps have your own site evaluated feel free to reach out to us here at CodeArt.*
> Here are links to all the posts in this series as they are published:
> 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1

Welcome once again, dear reader to this the 10th day before Christmas - and no. 10 on my Top 12 list of common EPiServer/Optimizely CMS pitfalls.

Let's try a fun experiment:

1. Open an incognito browser. Go to the url of your integration or preprod environment. Does any of them work without login or access control? If they do, then try to google "site:[insert your environment hostname here]" and see if there are any results. If there are, you might want to think really hard if that is content you want indexed and competing for your SEO ranking. Or even if it's not indexed by Google - is this content you want everybody to see?
   One of the typical mistakes I see in many, many places are unsecured and unrestricted development, test and staging environments - best case they might have robots.txt that prevents indexing for crawlers respecting that.
   But don't worry - usually access control can be really easy - it can often be as easy as removing the "Read" access for the "Everyone" role on the root node.

2. Next, log into edit-mode on your production environment. Look at the page tree. Are there any areas that are not supposed to be public? Maybe an "[editor name] Test Area" page with a bunch of pages below? Or how about in the media library? Any large PDF's or other docs that are not supposed to be public just yet?
   Try the urls to those assets & pages in an incognito browser and see what pop's up. And they are not protected, see if you can find them on google - they tend to have a way to find their ways into autogenerated sitemaps and then directly into indexing.
   Using a "secret" url is not a way to secure content.
   I don't think I've ever seen a production site where the editors didn't have a 'playground' area. And I get it. It's great to have a place to try out certain content types. Or even all through the site - half-finished content published by default and just not linked until it's ready. But Google sees it all.
   My recommendation: Avoid publishing content that's not ready to be published. In fact, ideally limit how many editors can publish and make publishing a controlled process. Instead use projects to bundle and schedule publishes, use access control as described above to remove "Everyone" from test areas and playgrounds - and if you need to show something unpublished to your CEO that doesn't know how to log into Episerver - use the "Advanced Reviews" add-on to make an external url with a managed lifespan for them to see.

3. Ok - this last one gets a bit more technical. Do you have any custom built add-ons? Take a look at your codebase - especially the controllers. Any of them that are for internal/editorial/development use? Editorial helpers, cache-controllers, developer debug tools?
   If so, see if you can figure out the route to them - and if any of them is outside the usual edit-mode (/episerver/) path? Do they use any authorization attributes or other stuff preventing public access?
   Once again, do the test of starting an incognito browser, pretend you are an evil russian mastermind that can guess any url in the world - and see if you get access to stuff you shouldn't have.
   In my experience, many developer/editorial tools are made on-the-fly to help solve an urgent here-and-now problem. Often quick-and-dirty code. And I've seen a lot that wasn't properly protected.

Ok. Experiment over.
Did you succeed? Did you win and have a website that with none of the above problems? Great! Congratulations. Pour a glass of Gløgg and take the rest of the day off. If not: Well, then you have work to do my friend. This probably shouldn't wait till 2024 to get fixed.

Tech Talk Tips and Tricks Website Improvements Optimizely (Episerver) CMS

RECENT POSTS

CodeArt ApS

Teknikerbyen 5, 2830 Virum, Denmark
Email: info@codeart.dk
Phone: +45 26 13 66 96
CVR: 39680688