ALLAN THRAEN | 4 months ago | PDF |

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

CHRISTMAS COUNTDOWN: #7 DDOS? WHAT'S THAT? WHAT DO YOU MEAN 'PREPARED'?

Is your website ready to handle intense usage scenarios like DDoS attacks or black friday? Many people think that testing performance is the same as testing for load - but it's not and sometimes it might even work against each other.

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

7 days till Christmas, and the 3rd sunday of Advent. And while you might right now be comfortably sitting in front of the fireplace, enjoying the day with your family while sneaking a peak at this exciting Christmas Countdown post on your mobile device, others are not. Somewhere in a dark and cold basement an evil teenager/script kiddie who are afraid they won't get christmas presents this year, is coming up with another plan to cause havoc on your websites...

And since hacking is hard (except if it's a wordpress website, but I digress), they most likely will turn to a DDoS attack.

Ok. Maybe it's not an evil teen, but a professional paid by a foreign government or your competitor or .... but the result is the same.

By sending millions of requests your way simultanously they will basically overload your site until it breaks. Ever had that happen to you? Many have. Now, how can you prepare for it:

CDN

A Content Delivery Network (CDN) is almost always a must! It's your first line of defence, and can typically spot an attack within minutes and stop it before it takes down your server. There are many different CDN providers, Cloudflare, Akamei and Azure CDN being some good choices. Cloudflare is probably the market leader and also the CDN you get included when your site is hosted with Optimizely. If you host on-prem or in your own azure, make sure to always use a CDN!

Handle your weak points

Most often, the attacks are fairly 'dumb' - meaning they might just attack the start page of your website

(which I hope you've designed for high traffic) - but sometimes there is an attacker that has actually bothered taking a look at your website.
Here's a little exercise for you: Look at your website as an attacker would. And if they want to crash your server they would probably attack weak points that require a lot of server-side power or memory.

For example:

- Do you use dynamic image resizing? Dynamic image resizing, where images are resized on the fly is great and easy to work with. But every time an image has to be resized it takes resources from your server. And even though each resized format might be cached, what would stop the attackers from creating a million different sizes and formats of each image on your site?
  Easy way to check is to open an image url to your site, and try to append query parameters like "&width=100" or "&w=100" to see if it resizes to a width of 100px.
  Fix can either be to configure your dynamic resizing to only accept certain sizes/formats - or even better, let the CDN resize and optimize images and you won't have to worry about it.

- Do you have dynamic content listings? Like - do you have a list of the latest press releases on your front page? Or maybe a list of promoted products? How are those lists generated? Find-search? Content-graph query? Find-Pages-With-Criteria (I hope not)? something else? And are they cached, or is there a significant process going on every time the containing page is shown to find them?

- What about your search & result page? Did you think resilience into that? Do you cache queries? Have you setup rate-limiting or other means to prevent an attacker from doing a million searches at once, getting you locked out of Optimizely Search & Navigation service?
- Some attackers loves to auto-submit forms. Do you have forms on your website? do you store all submissions in the database? Do you have some kind of captcha or other mechanism preventing a lot of submissions or just regular spam?
  (If you don't like captcha's perhaps honeypotsis a good solution)
- Is some of your frequently used content - like the start page - very static and without personaliation? Then consider if maybe you can setup output caching to speed things up.

- Finally, if you have some really heavy functionality on your site. Maybe a complex calculator of some sorts or functionality that calls multiple 3rd party services - did you consider setting up a feature toggle switch to turn those features on/off in an emergency? It might not be a bad idea.
- You could also consider if perhaps it would be a good idea to have a static 'shadow' site - that your loadbalancer (or CDN) could direct traffic to, should you come under attack. Of course, if it's not attacks - but just regular heavy traffic, and you can't optimize your site further, then perhaps a queuing solution is not a bad idea? Or just scaling up and out on your servers.

Remember to test for load, not just performance

And finally, keep in mind that testing and optimizing for performance on your website isn't the same as testing and optimizing for high load. Both should be done, and often having a website with good performance helps to have a load-resistant website - but not always.

For example: A common way to provide a faster browser load experience is to do asynchroneous loading of the different elements on the page. Like - loading individual blocks indepentently - or sometimes lazy loading them only they they are shown (for example if the user scrolls to them). While this make sense for a 'perceived performance' point of view, it often has the effect that it puts more load on the server. What was 1 request before is all of a sudden a lot more requests - all of which has to load the current context and proper content models in Optimizely CMS to render the correct content.
I've seen implementations where the (more or less static content) front page of a website would consist of 20+ individual requests for content to the server - and trust me, these scenarios were struggling with any kind of traffic.

There are many tools you can use to test for load. Here at codeart we made our own tool last year, and while it may not be perfect, it has the ability to run purely through a browser, so you can easily try it out in any kind of environment.

Read about it **here** and try it **here**.

Often load measurements are counted as requests per second (RPS). I've seen live EPiServer/Optimizely CMS sites go all the way from 1.5 to 30 RPS after some of the above improvements. And while it on it's own might not completely stop a DDoS attack - it will certainly help a great deal on the way.

.NET Development | CMS | Optimizely (Episerver) | Website Improvements | Tips and Tricks | Tech Talk

RECENT POSTS