Some thoughts about security:
Know your URLs

achim.schermuly-koch@cassini.de

Background

- Launch of a new product
- Launch backed by *x*-million euro advertising campaign
- Thus quite some load expected
- Rough market, jealous competitors

cassini
TECHNOLOGY GUIDANCE

Talking with IT-security

[IT-security]
“Can‘t we just render some static HTML like in the good old days?”

[IT-security]
“Well... any suggestions?”

[CMS Expert]
“There is no static website anymore! Just think of a dynamically generated navigation component… And the old days were not that good ;-)“

[CMS Expert]
“Build a dynamic site that is 100% cached”

Basic Security

- Cache *everything* in the dispatcher
- Strict whitelisting with mod_security
- No whitelist patterns (except for the resource part in the URL)
- All URLs must be known in advance (except resource part)

Preventing Denial of Service Attacks

- Avoid requests hitting the CQ5 servers

Reminder:

- Even “http://www.mysite.com/index.html?” hits the CQ5 servers
- Users might add a “?” to any URL even if *you* don’t.

Solution:

- Strip off all query parameters with a rewrite rule
- Use (few) selectors where necessary
- Track number of requests per user per minute with mod_security

Cache Pollution

Your URL:

http://www.mysite.com/index.html

Their URL:

http://www.mysite.com/index.001.html
http://www.mysite.com/index.....html
http://www.mysite.com/index.999.html

Effect:

Content get‘s rendered again and again by CQ5. Cache is polluted.

Solution:

mod_security: No patterns in whitelists

Service Exposure

- Don‘t expose services in your URLs.

Your URL:

http://www.mysite.com/news/articlex/gfx.Services.png

Their URL:

http://www.mysite.com/gfxheadline.AAAA.png
http://www.mysite.com/gfxheadline.AAAB.png

Solution:

http://www.mysite.com/content/home/services.**navi**.png
=> The **navi** script knows which atom contains ”Services”.

Service Exposure

- Example: Render a 200px wide teaser image for the page “article”

Your URL:

http://www.mysite.com/news/article.teaserimg.200px.png

Their URL:

http://www.mysite.com/news/article.teaserimg.1px.png
http://www.mysite.com/news/article.teaserimg.2px.png
http://www.mysite.com/news/article.teaserimg.99999px.png

Solution:

http://www.mysite.com/content/article/teaserimg.**small**.png
=>Let the “teaserimg” script decide how big “small” is.

Conclusion…

- Know the risks
- Balance flexibility and security carefully

- ALWAYS filter parameters according to your business needs

AND

- NEVER pass a bare HttpServletRequest into a QueryBuilder ;-)

Cassini Consulting GmbH
Technology Guidance

Achim Schermuly-Koch

Halskestraße 46
40880 Ratingen
Deutschland

T +49 (0)151 11 44 38 18
F +49 (0)21 02 94 34 738
visit www.cassini.de

cassini
TECHNOLOGY GUIDANCE