Data protection in web development made easy

Amelia Andersdotter & Anders Jensen-Urstad
DrupalCamp Baltics
August 28, 2015

“Our freedom is built on what others do not know of our existences.”
—ALEKSANDR SOLZHENITSYN

dataskydd.net
“Everyone has the right to respect for his private and family life, his home and his correspondence.”

—EUROPEAN CONVENTION ON HUMAN RIGHTS, ARTICLE 8
Data protection
A collection of tools for achieving privacy.

Data security
When procedures work as foreseen.
How to be excellent
to each other

How we defeat NSA/GCHQ/whoever
Do your *visitors* have an *obligation* to help you or your client out?
Right to know

Right to consent

User-centric

Data minimization

Effective sanctions
Right to know
Right to consent
User-centric
Data minimization
Effective sanctions
Right to know
Right to consent
User-centric
Data minimization
Effective sanctions
Right to *know*
Right to *consent*
User-centric
Data minimization
Effective sanctions
Right to know
Right to consent
User-centric
Data minimization
Effective sanctions
Public sector websites

Private visits

Governing vs. governance
99% of Swedish municipalities use either...
- third-party trackers
- tracking cookies
- third-party service behaviors
European Union Law

Present:
Directive 1995/46/EC *Data Protection*
Member State laws on public administration

Coming:
General Data Protection Regulation (GDPR)
Law Enforcement Data Protection Directive
So what to do?

1. Encrypt *all* the things.
2. Don’t expose your visitors to others. *(At least not without consent!)*
Getting help for domestic violence

One woman in four (and one man in six) in the UK will be a victim of domestic violence during their lifetime, according to research estimates. Two women a week are killed by a current or former partner.
HTTP

Hypertext Transfer Protocol

GET /Livewell/abuse/Pages/domestic-violence-help.aspx HTTP/1.1
Host: www.nhs.uk
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_3) AppleWebKit/5
HTTPS

- Server Name Indication extension
  - Server Name list length: 13
  - Server Name Type: host_name (0)
  - Server Name length: 10
  - Server Name: www.nhs.uk
- Extension: Extended Master Secret
  - Type: Extended Master Secret (0x0017)

| 0060 | c5 8d d4 72 13 85 96 68 34 d4 b1 59 94 00 00 22 |
| 0070 | c0 2b c0 2f 00 9e cc 14 cc 13 cc 15 c0 0a c0 14 |
| 0080 | 00 39 c0 09 c0 13 00 33 00 9c 00 35 00 2f 00 0a |
| 0090 | 00 ff 01 00 00 7b 00 00 00 0f 00 0d 00 00 0a 77 |
| 00a0 | 77 77 2e 6e 68 73 2e 75 6b 00 17 00 00 00 23 00 |
| 00b0 | 00 00 0d 00 16 00 14 06 01 06 03 05 01 05 03 04 |
| 00c0 | 01 04 03 03 01 03 03 02 01 02 03 00 05 00 05 01 |
| 00d0 | 00 00 00 00 33 74 00 00 00 12 00 00 00 10 00 1d |
| 00e0 | 00 1b 08 68 74 74 70 2f 31 2e 31 08 73 70 64 79 |
| 00f0 | 2f 33 2e 31 05 68 32 2d 31 34 02 68 32 75 50 00 |
| 0100 | 00 00 0b 00 02 01 00 00 0a 00 06 00 04 00 17 00 |
• SSL certificates are cheap
• Let’s Encrypt (letsencrypt.org) will make them free and automated:
  $ sudo apt-get install lets-encrypt
  $ lets-encrypt example.com
• Use HTTP Strict Transport Security (HSTS)

(Bonus: HTTPS now used as a ranking signal by Google.)
Referrers

Other channels

Follow us on Twitter
Facebook
YouTube
Video library
Links library
NHS Choices Training

*click*
Don’t tell other websites about your visitors

I don’t leak referrer information.

W3C HTML5 Recommendation, 4.8.4.8

(Plugin: https://drupal.org/project/noreferrer)
Referrer Policy, W3C draft

Firefox, Chrome, Safari, Microsoft Edge:

<meta name="referrer" content="never" />

Soon:

<a href="http://whitelist.me" referrerPolicy="unsafe-url">Send referrer, always</a>
No More Shall We Third-Party
Google Analytics usage among Swedish municipalities

Uses Google Analytics: 233

Doesn't use Google Analytics: 57
Piwik

- Open source, PHP + MYSQL
- You own the data
- Various privacy options
- Can be used without cookies

Totally radical alternative: don’t track.
Third-parties: Comment platforms

Disqus:
• Anonymity
• Control
• Rights
• Privacy
The Quest for a Disqus alternative

• Plain ol’ built-in comment system
• Self-hosted open-source Disqus-like software (e.g., Isso, HashOver)
• Integration with forum software (e.g., Discourse, Vanilla Forums)
Third-parties: Social media

• Vendor-provided embedded like/share buttons track people
• Use **locally hosted** images/fonts instead!
• *Or...* two-click solution:
Third-parties: Fonts

Request URL: https://fonts.googleapis.com/css?family=Open+Sans:400,
Request method: GET
Remote address: 74.125.136.95:443
Status code: 200 OK
Version: HTTP/2.0

Filter headers

Response headers (0.451 KB)

Request headers (0.422 KB)

Host: "fonts.googleapis.com"
User-Agent: "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:40.0) Gecko/20100101"
Accept: "text/css,*/*;q=0.1"
Accept-Language: "en-US,en;q=0.5"
Accept-Encoding: "gzip, deflate"
DNT: "1"
Referer: "https://www.afsp.org/preventing-suicide/find-help"
Once More, with Feeling

Use HTTPS.
Don’t leak referrers.  
No third-party resources without consent. *Self-host* when possible.  

https://dataskydd.net/dcbaltics2015
In conclusion...

Individuals matter.

*It’s possible to protect privacy.*

Join us! 💌
Amelia Andersdotter
amelia@andersdotter.cc
@teirdes
ameliaandersdotter.eu

Anders Jensen-Urstad
anders@unix.se
@ndrsju
anders.unix.se

Slides, references, code, etc.:
https://dataskydd.net/dcbaltics2015

dataskydd.net
THANK YOU!
Q&A