Web 2.0 – A Security Nightmare?

SSL and Webapps
Webmontag Karlsruhe, 29.5.2006

Hanno Böck, http://www.hboeck.de/

Web 2.0 for everyone?

- Web 2.0 applications should be available for the common user
- »Blog in 1 minute«, »Get your own Wiki« etc.
- Apps are not »Secure by default«

Sniffing

Sniffing is easy

- ethereal
- ettercap
- dsniff
- Solution: Login via https!

No HTTPS

- Wikipedia
- digg.com
- plazes
- del.icio.us
- myblog.de

Have an own rootserver?

- Cool, make your app accessible with either http or https.
- Advanced: mod_rewrite to forward login-page to https.
- And the world is fine?

Problem: IP-Adresses

- One SSL-Cert per IP
- Domain in Cert
- IP-Adresses are always limited
- Strato max. 2, 1&1 max. 8
- IPv6?

Problem: Certificate

- Expensive cert by Verisign & Co?
- Self-signed?
- CAcert

Everything perfect?

- Own server
- App available via http or https
- Login-page forwards to https
- CAcert-signed cert
- IPv6-tunnel for server and client

Where's my cookie?

- Session-Cookie by default per domain – don't call your page via http after https.
- Workaround: https on other subdomain
- Secure webapps

Completely offtopic: Werbung

GPN 5

Gulasch Programmier Nacht

9. - 11.6.2006

CCC Karlsruhe/Entropia

www.entropia.de