advania

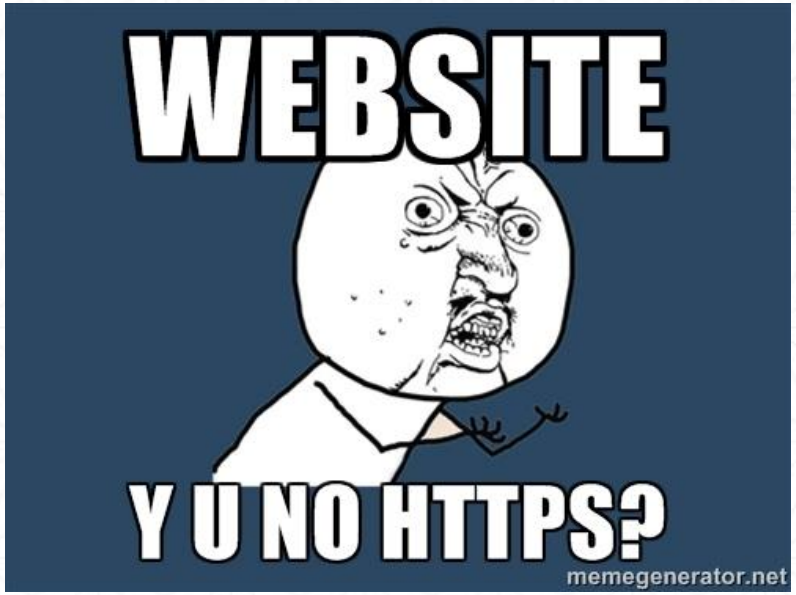
Welcome to IT

Hvernig auðkennum við vefi og notendur?

Sveinbjörn Óskarsson
Advania hf.

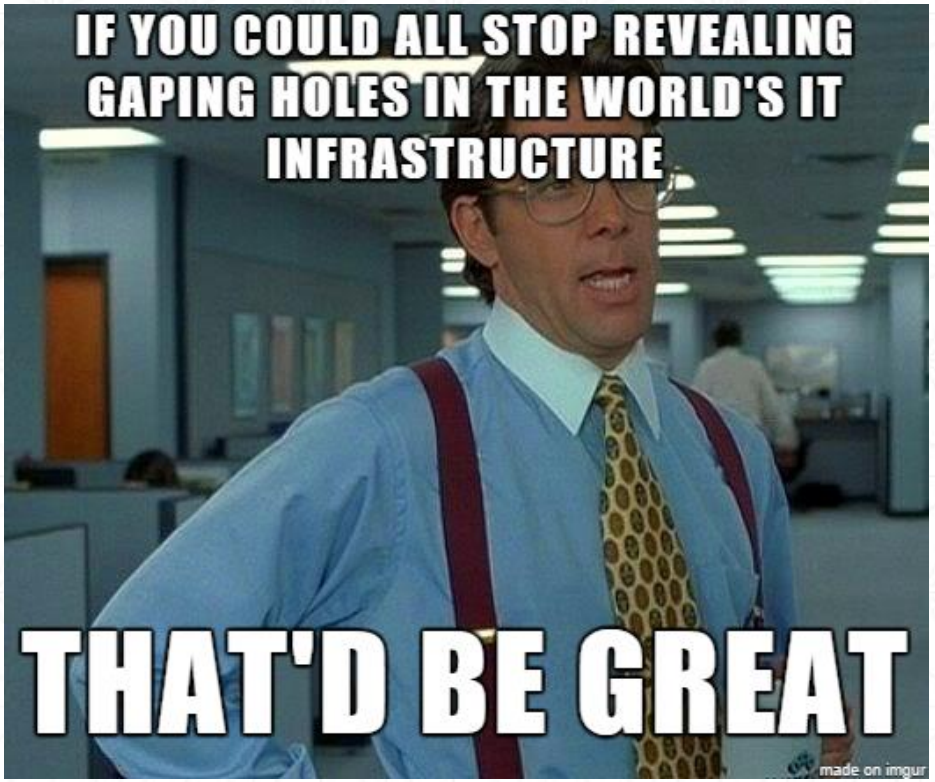
Hvernig auðkennum við vefi

- HTTPS!
- Tvö orð: rafræn skilríki („SSL skilríki“)
  - Votta eiganda léns
  - Dulkóða samskipti milli notanda og miðlara
- Hvað ertu að borga fyrir?
  - Startcom vs Verisign EV
  - Veiðkort eða vegabréf?
  - Vottun vottun og meiri vottun
  - ...síðan dreifing
  - letsencrypt.org



Þurfum að vera vakandi

- Margir veikleikar komið í ljós síðustu ár
- Hearbleed
- Poodle
- Freak
- Crime
- BREACH
- Shellshock
- Logjam
- ...?
- www.ssllabs.com



Hvernig auðkenni ég notendur

- Notandanafn og leynorð
- Rafræn skilríki
- OTP auðkenning
  - Auðkennislykilinn
  - OTP í SMS
- Token auðkenning
  - Facebook
  - Google
  - Innskraning.island.is
- Gæði auðkenningar og vottunarstig
- Vil ég geyma þessar upplýsingar sjálfur

Notandanafn og leyniorð

- Ertu örugglega að gera þetta rétt?
- One way function
  - Við geymum staðfestinguna, ekki leyniorðið
- Ekki reyna að finna upp öryggið, notum reynslu/þekkingu annarra
  - OWASP
  - NIST
- Notum key derivation function
  - PBKDF2
  - scrypt
  - Bcrypt
- Leyfum sterk leyniorð
- Fólk endurnotar sömu leyniorðin

```
$result = mysql_query(
  "SELECT * FROM users " .
  " WHERE SHA1(username) = SHA1('" . $_REQUEST["username"] . "') " .
  "   AND SHA1(password) = SHA1('" . $_REQUEST["password"] . "')");
```

Rafræn skilríki

- Soft vs Hard?
  - Skilríki geymdi í afritanlegri skrá
  - Skilríki geymd á vottuðum miðli s.s. korti eða HSM
- Auðkenni
  - Rafræn skilríki á snjallkortum
  - Rafræn skilríki á SIM kortum
- Þurfum að staðfesta gildi þeirra í hvert skipti
  - CRL
  - OCSP
- Byggt á margreyndri tækni
- Keðja af trausti

Token auðkenning

- Oft er betra að láta aðra um að auðkenna
  - Þarf ekki að eltast við að styðja nýjustu auðkenni
  - Þarf ekki að geyma leyndarmál (leyniorð)
- Hversu viss vil ég vera um að notandi er sá sem hann segist vera?
- Helst staðlar
  - OAUTH2
    - Facebook
    - Google
  - SAML2
    - Innskraning.island.is
    - MS Federation Services
- Verðum að staðfesta(verify) þær upplýsingar sem við fáum
- Hvernig umgengst notandinn auðkenni sitt?

Gæði auðkenningar - QAA

- QAA – Quality Authentication Assurance
  - Level 1
    - Á við þegar skaði er lítill eða enginn við misnotkun
    - Engin eða lítil vottun
    - T.d. Facebook
  - Level 2
    - Á við þegar skaði er lítill við misnotkun
    - Ekki vottun í persónu en auðkenni gefið út á einstakling/fyrirtæki
    - T.d. Íslykill
  - Level 3
    - Á við þegar skaði er nokkur við mistnotkun
    - Hærra vottunarstig, vottað af stjórnvöldum
    - T.d. mjúk skilríki eða notandafn/leyniorð + OTP
  - Level 4:
    - Á við þegar skaði er mikill við misnotkun
    - Vottun í persónu í amk fyrsta sinn
    - Rafræn skilríki á vottuðum miðli

TL;DR

- Notum HTTPS
- Notum örugga staðla
- Notum okkur þekkingu annarra
- OWASP
- Ekki geyma leyniorð
- Staðfestum auðkenni
- Veljum viðeigandi auðkenningu