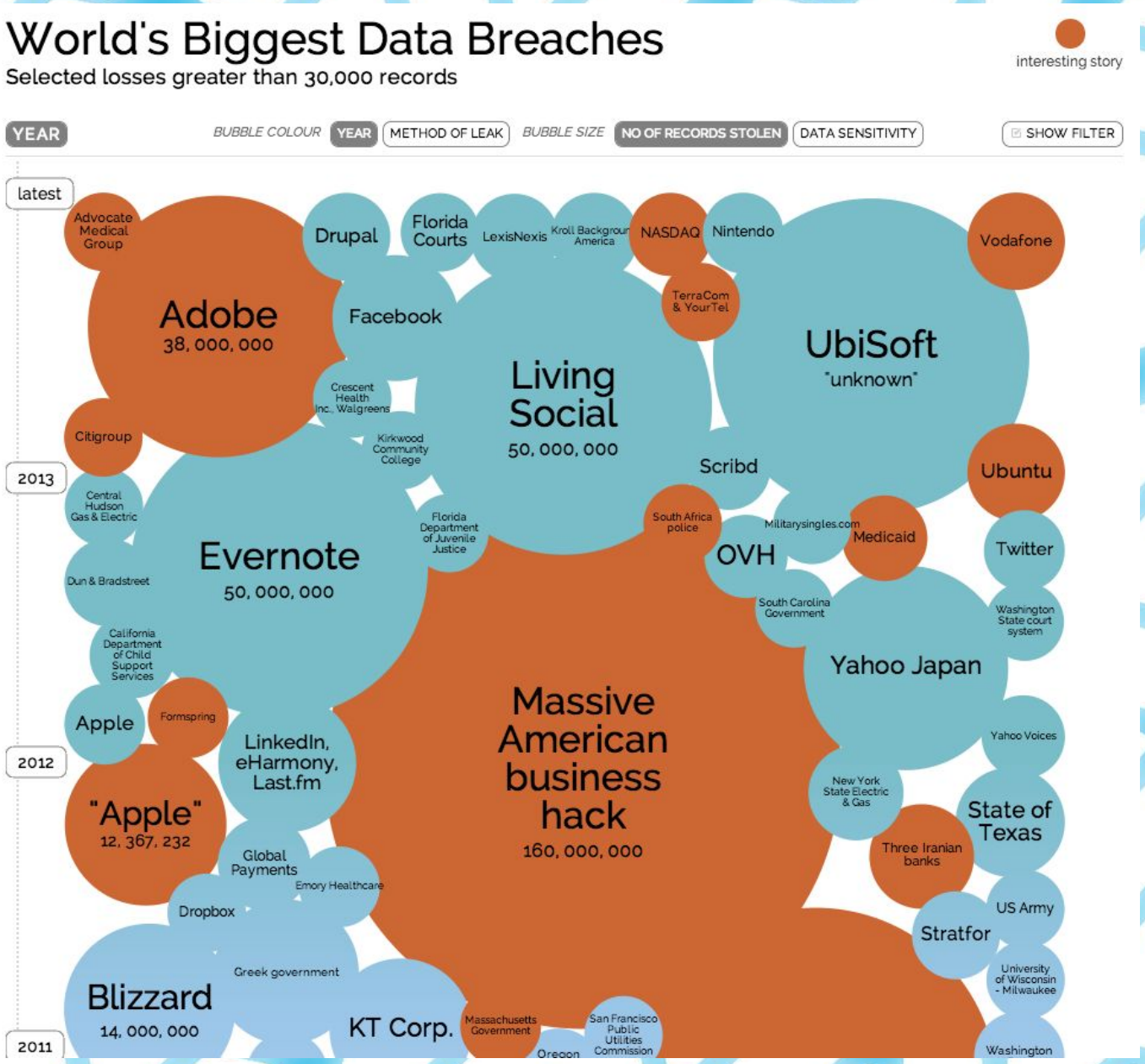

SYNDIS
Creative[in]Security

Yfirlit

- Markmið
- Threat Model
- Um OWASP samtökin
- OWASP Top 10 Most Critical Web Application Security Risks
- Niðurlag



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

SYNDIS
Creative in Security

Markmið

- Kynna ykkur fyrir öflugu verkfæri
- Stikla á stóru
- Gagnlegt fyrir:
  - DEV, OPS, QA, vefstjóra, stjórnendur…. Og hakkara

Threat Model

- Hvað þurfum við að verja?
  - Framendi, gagnagrunnar, skýjaþjónustur o.s.frv.
- Hverjir geta ráðist á okkur?
  - Samkeppnin, notendur, starfsmenn, botnet, hakkarar.
- Hvernig eru innviðir uppbyggðir?
  - Hvernig er kerfisrekstri háttað(dev, test, prod)?
  - Network segregation & segmentation?
- Hvað er í forgangi?

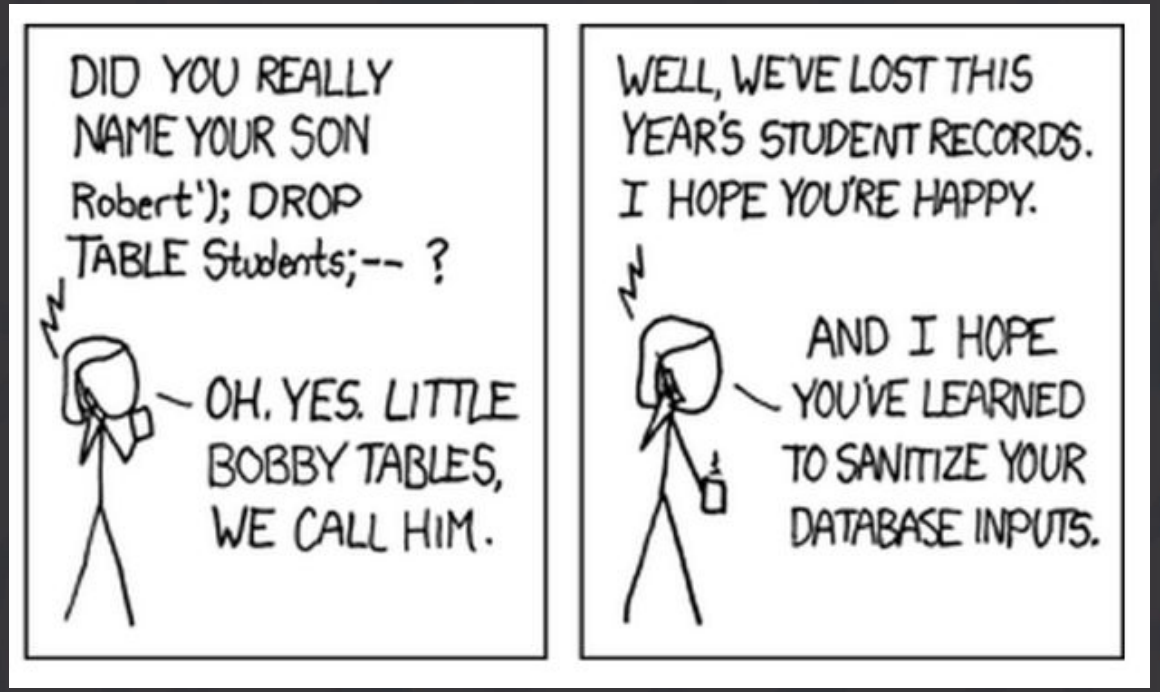
OWASP

- Stofnað árið 2001 - Open Source
- Brúar bilið milli öryggisrannsókna og vefforritunar
- Gefa út top 10 lista
- Nær líka yfir snjallsímaforrit
- OWASP 10 er ekki tæmandi

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.

A1 - Injection

- SQL, LDAP, OS injection o.s.frv
- Láta hugbúnað keyra skipanir
- Ekki treysta inntaki frá notanda



A2 - Broken authentication

- Notendur ekki auðkenndir með öruggum hætti
- Brute force
- Léleg lykilorð eða default(admin/admin)
- Session management - Timeout of langt

A3 - Sensitive Data Exposure

- Flutningur og geymsla viðkvæmra gagna óörugg
  - Cleartext, veik dulkóðun eða mannleg mistök
- GDPR(General Data Protection Regulation)
  - Persónugreinanleg gögn
  - Alvarleg brot varða sektum upp á 4% af heildarársveltu á heimsmarkaði (6 milljarðar hjá Icelandair Group)

A4 - XML External Entity attack (XXE) NEW

- Vefþjónustur sem þátta (e. parse) XML inntak
- Láta XML þáttarann keyra meinfýsinn kóða ($rm -rf /)
- Lesa viðkvæmar skrár, Denial of service

A5 Broken Access Control (Merged)

- Aðgengi og hlutverk
- Skýrar aðgangsstýringar
- Hvert kemst ég með að fikta í URL-inu?

A6 - Security Misconfiguration NEW

- Algengasta atriði á listanum
- Default settings
- Out of the box & plug and play
- Jenkins, Redis, MongoDB og fleira

A7 - Cross-Site Scripting (XSS)

- Láta síðu gera hluti sem hann á ekki að gera
- Hægt að breyta innihaldi síðu(JS, HTML)
- Endursenda (redirect) aðra notendur á meinfýsna síðu

A8 - Insecure Deserialization NEW

- Breyta upplýsingum
- Staðfesta inntak
- Ekki einfalt að misnota

A9 - Using Components with Known Vulnerabilities

- Öruggasti kóði heims getur fallið á veikleika í öðrum pakka
- Fara yfir úrelta pakka og fylgjast með umræðu
- Patch management

Security

Equifax CEO falls on his sword weeks after credit biz admits mega-breach

Well, what else could he do?

By John Leyden 26 Sep 2017 at 15:35

Equifax's chairman and chief exec today resigned, wee
consumer credit reporting agency admitted a massive

The Apache Software Foundation
http://www.apache.org/

Struts™

SYNDIS
Creative in Security

A10 - Insufficient Logging & Monitoring NEW

- Munurinn milli þess að uppgötva atvik og missa af því
- Munurinn milli þess að greina atvik og missa af því
- Hvenær uppgötvast atvik
- Hvernig var brotist inn
- Hversu lengi var viðkomandi með aðgang

RISK	Threat Agents	Attack Vectors	Security Weakness		Impacts		Score
		Exploitability	Prevalence	Detectability	Technical	Business	
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017-Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0

75% of All Attacks on Information Security Are Directed to the Web Application Layer

2/3 of All Web Applications Are Vulnerable

Gartner

90% of companies using DevOps consider security an afterthought.

— Gartner

AND YET…

90% of exploits are due to defective software.

— Homeland Security

SYNDIS
Creative in Security

Data Breach Costs

$7.2M average cost of a data breach

80 days to detect and **123 days** (4+ months) to resolve

Remediation Costs *(at each stage in the lifecycle)*

Sources: National Institute of Standards and Technology; Ponemon Institute

Niðurlag

- OWASP Top ten cheat sheet
- Öryggi varðar okkur öll
- Forðast snákaolíuna
- Stefnur og straumar (frítt viðvörunarkerfi)

Spurningar?

Heimildir

- The Open Web Application Security Project
- Verizon data breach report 2017
- Umsögn Persónuverndar um tillögu til þingsályktunar um fjármálaáætlun fyrir árin 2018-2022
- WEB APP SECURITY 101: KEEP CALM AND DO THREAT MODELING