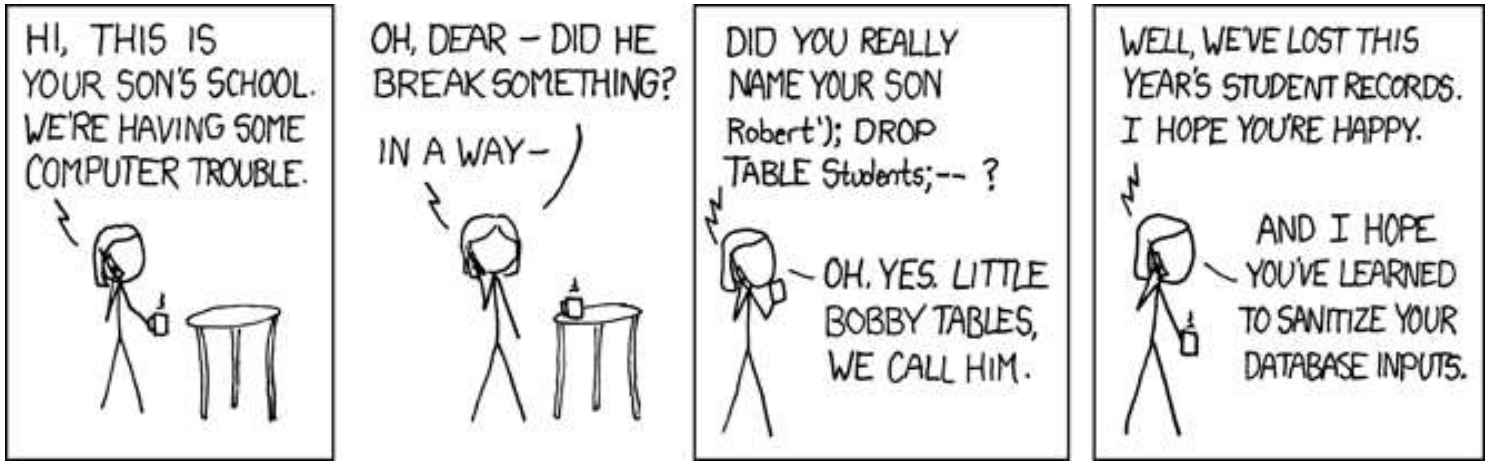
Attaques, menaces, tracking et failles de sécurité sur le Web



Attaques par injection de code

- Injection JavaScript (XSS)

  http://fr.wikipedia.org/wiki/Cross-site_scripting

  UTF-7: http://nedbatchelder.com/blog/200704/xss_with_utf7.html

  HTML5: http://www.dzone.com/links/r/html5_some_security_concerns.html

  HTML5 + CSS: http://fr.slideshare.net/x00mario/stealing-the-pie

  HTML5 + CSS: http://p42.us/css/

  Nom du DNS: http://www.skullsecurity.org/blog/2010/stuffing-javascript-into-dns-names

- Injection SQL

  http://fr.wikipedia.org/wiki/Injection_SQL
  https://www.mavitunasecurity.com/blog/sql-injection-vulnerability-history/

  http://www.databasetube.com/database/sql-injection-through-http-headers/

- Injection PHP, etc…

Attaques par injection de code

Protection:

- Toujours spécifier un encodage (UTF-8) au début du code HTML (et dans les headers HTTP)
  https://code.google.com/p/doctype-mirror/wiki/ArticleUtf7
- Filtrer systématiquement tout ce que les visiteurs peuvent uploader ou saisir dans les champs de formulaires. Echapper le code HTML/JS/PHP/SQL présent.
- Parser et valider les données sensibles (passwords, URLs, …) avant de les utiliser dans des requêtes en base de données ou pour lire des fichiers.

Tracking

http://en.wikipedia.org/wiki/Web_visitor_tracking
http://en.wikipedia.org/wiki/Ad_Tracking#Internet_tracking

Des cookies sans cookies

- Des « cookies » impossibles à supprimer, en JavaScript / Flash
  http://samy.pl/evercookie/

Des cookies sans JavaScript, et sans Flash

- Des « cookies » utilisant le cache navigateur
  http://korben.info/etag-tracking.html
  http://lucb1e.com/rp/cookielesscookies/

Votre navigateur est unique!

https://panopticlick.eff.org/index.php?action=log&js=yes

Tracking

http://en.wikipedia.org/wiki/Web_visitor_tracking
http://en.wikipedia.org/wiki/Ad_Tracking#Internet_tracking

Espionnage de l'historique de navigation

- Faire un lien vers un site et exploiter son état (« visited » ou non)

Site jamais visité / site déjà visité

http://linuxbox.co.uk/stealing-browser-history-with-javascipt-and-css.php
http://www.ieee-security.org/TC/SP2011/PAPERS/2011/paper010.pdf
http://contextis.co.uk/files/Browser_Timing_Attacks.pdf
http://sip.cs.princeton.edu/pub/webtiming.pdf
http://seclists.org/fulldisclosure/2013/May/12
http://lcamtuf.coredump.cx/yahh/

- Faire une requête vers un site et chronométrer l'accès au cache pour déterminer s'il a déjà été visité

http://sip.cs.princeton.edu/pub/webtiming.pdf
http://lcamtuf.coredump.cx/cachetime/

Chiffrements

- Crack du chiffrement SSL (2011, 2013):

  - http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/

  - http://arstechnica.com/security/2013/08/gone-in-30-seconds-new-attack-plucks-secrets-from-https-protected-pages/

- Crack du chiffrement AES (2011):

  http://www.developpez.com/actu/36169/Le-chiffrement-AES-cracke-par-des-chercheurs-francais-belges-et-de-Microsoft-la-methode-reste-tres-complexe/

- Crack du chiffrement DES (2013):

  http://www.developpez.com/actu/58806/Pirater-votre-carte-SIM-grace-a-un-SMS-serait-possible-le-hacker-pourrait-entre-autres-subtiliser-l-identite-du-proprietaire/

- Et la NSA…