TECHNISCHE UNIVERSITÄT DRESDEN

Faculty of Computer Science Institute of Systems Architecture, Operating Systems Group

PROBLEMS IN PRACTICE: THE WEB

MICHAEL ROITZSCH

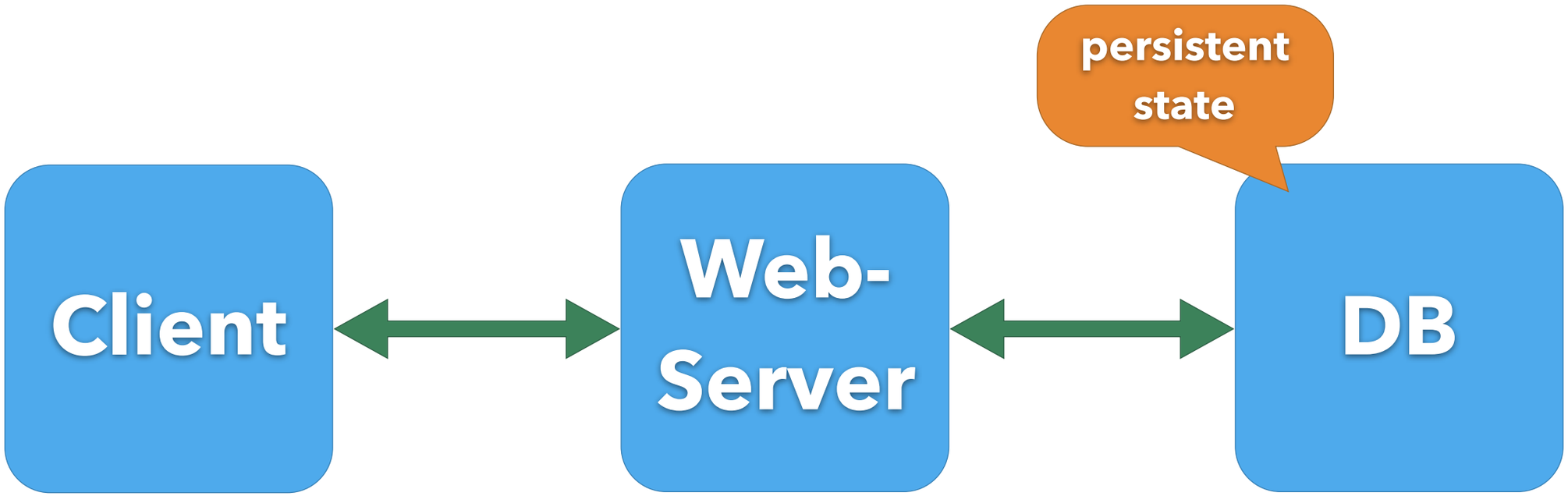
TECHNISCHE UNIVERSITÄT DRESDEN

THE WEB AS A DISTRIBUTED SYSTEM

TECHNISCHE UNIVERSITÄT DRESDEN

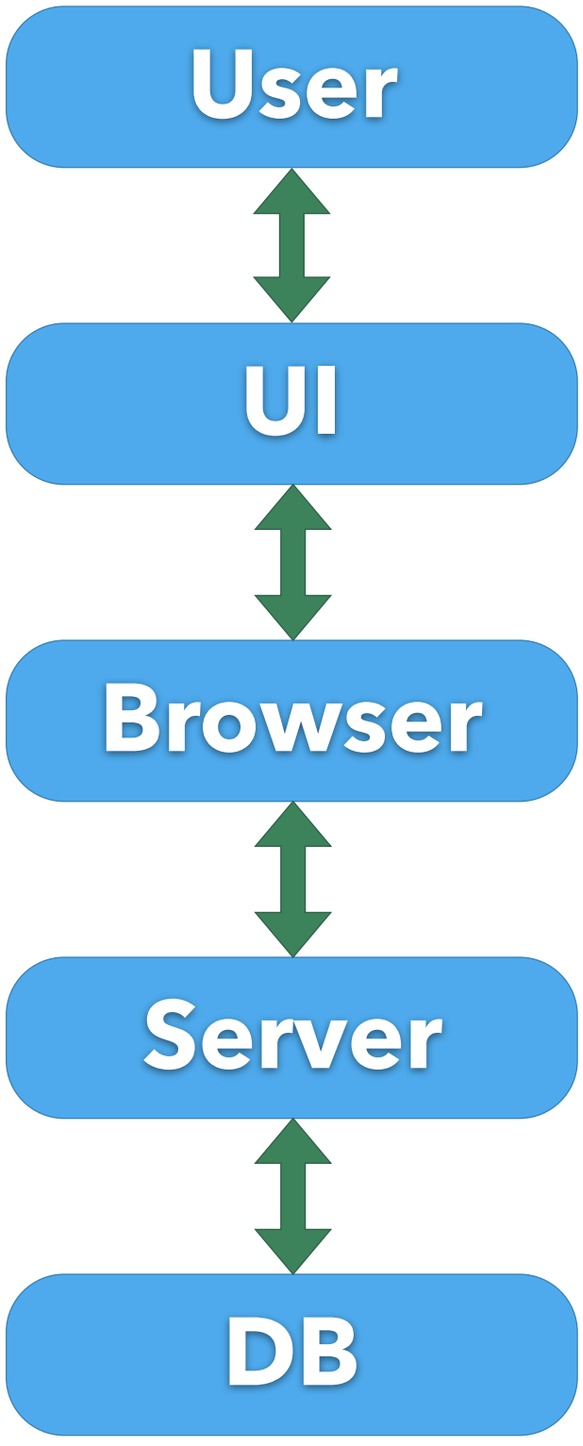
WEB HACKING SESSION

3-TIER



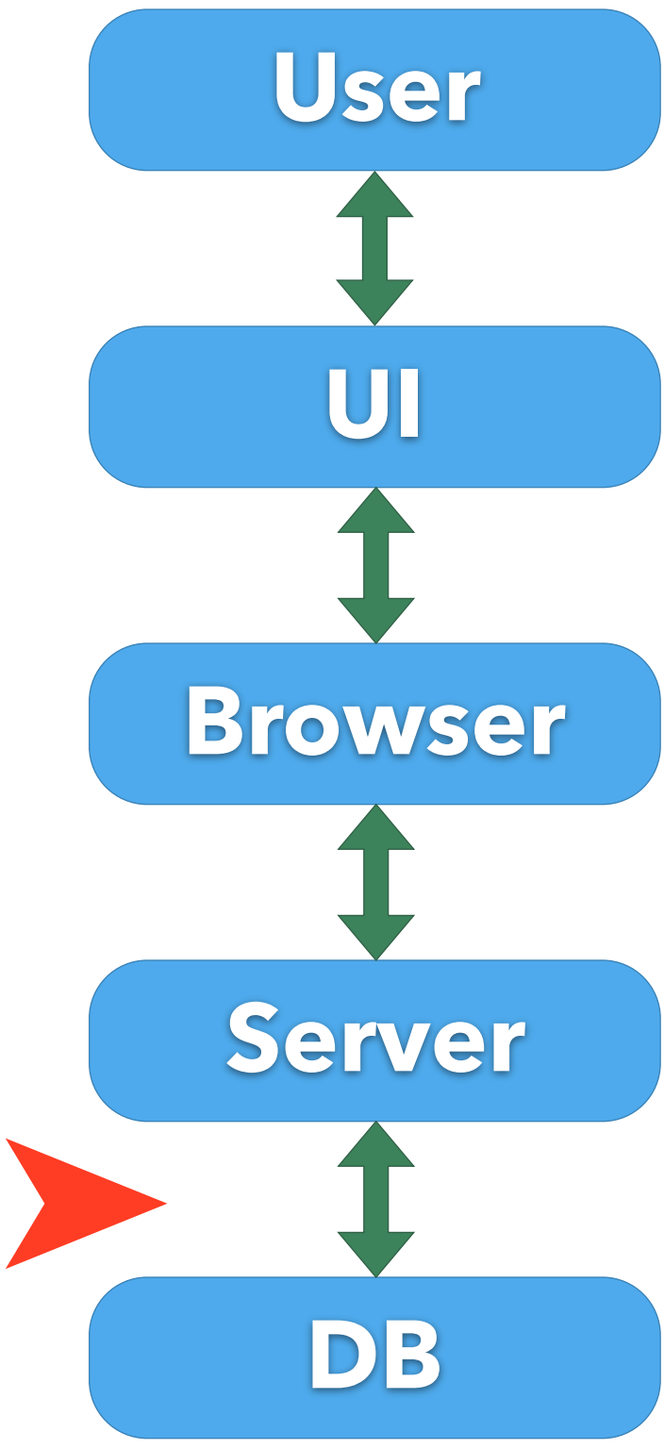
Presentation		Application Logic		Data
HTML	HTTP	PHP	(No)SQL	Relations
JavaScript		Rails		KVS
AJAX		Node.js		Documents

SCENARIO



- user visits a service
- attacker tries to disturb
- various complex layers
- independently developed technologies are being combined
- what you see may not be what you get…

BACKEND



- goal: manipulate state stored in the database
- not directly accessible (hopefully)
- improper input checking in frontend server required
- nice: inconsistency is persistent

EXAMPLE IN PHP

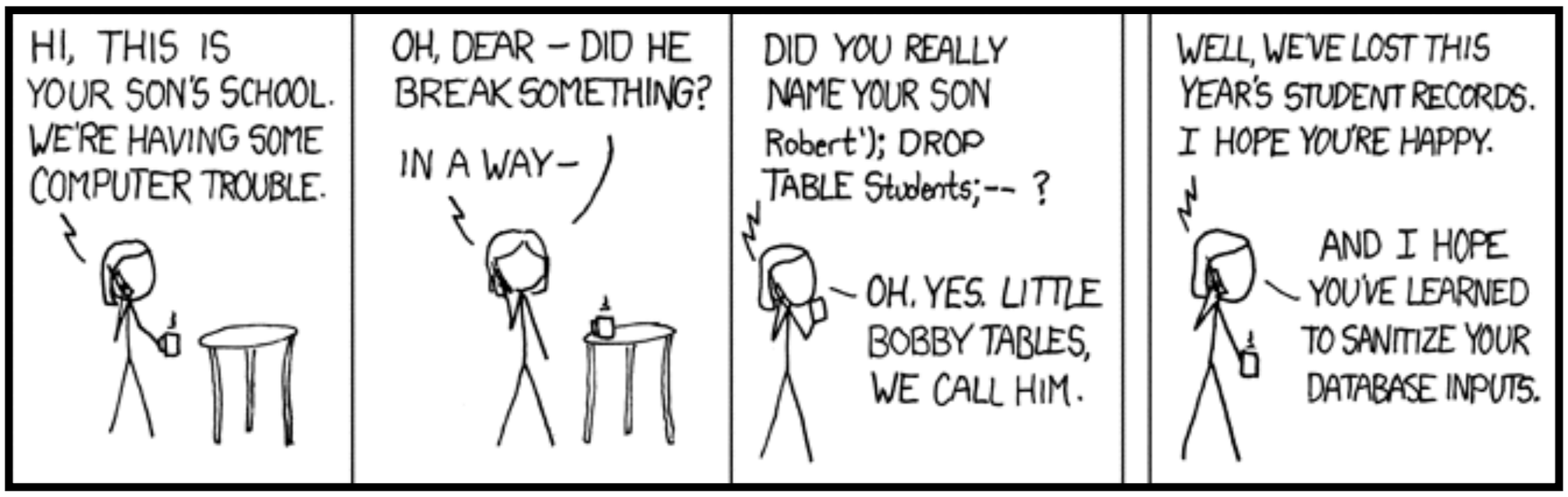
```
$password = $_POST['password'];
$id = $_POST['id'];
$sql = "UPDATE Accounts SET
   PASSWORD = '$password' WHERE
   account_id = $id";
```

Now imagine: password=';--

SQL injection

TECHNISCHE UNIVERSITÄT DRESDEN

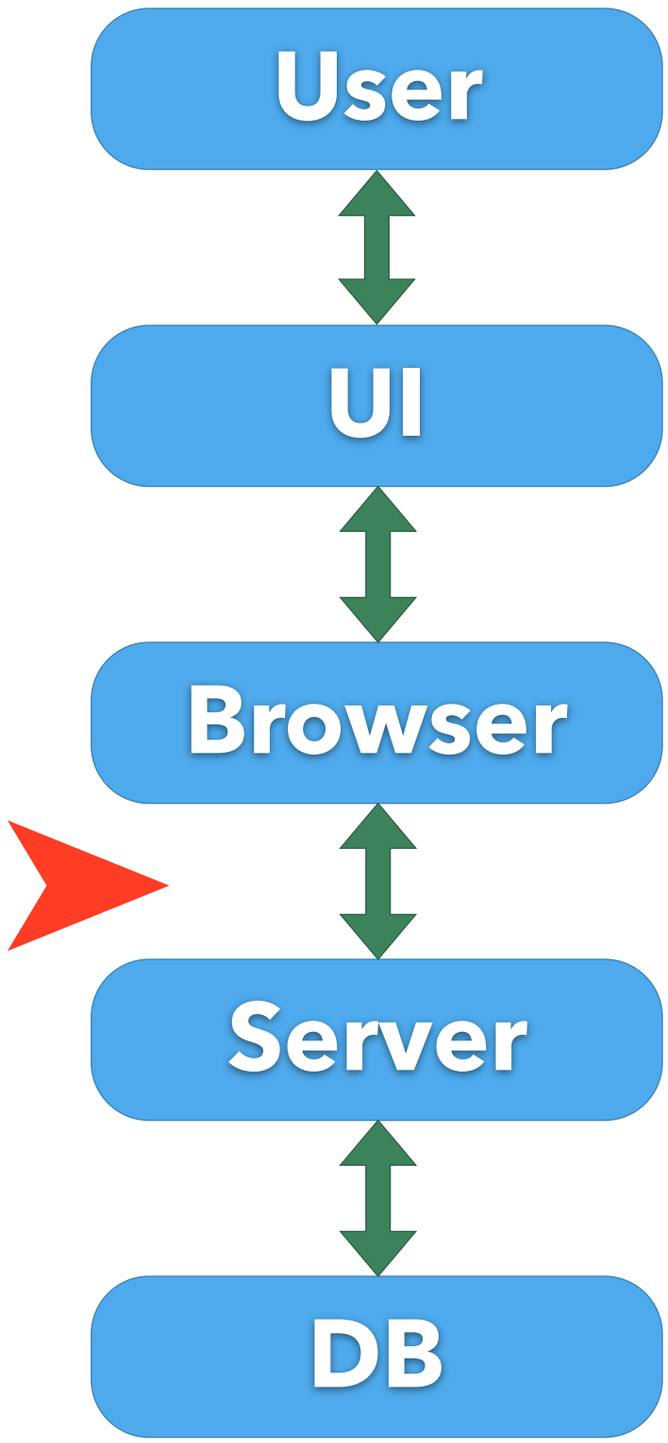
BOBBY TABLES



Comic by Randall Munroe, xkcd.com

LICENSE PLATE

FRONTEND



- goal: manipulate content delivered to the browser
- infrastructure attacks like DNS cache poisoning
- solution for this: make sure you use SSL
- improper input checking can still bite you

EXAMPLE

- http://example.com/?query=query string
- generates website containing:
  You are looking for: query string
- so how about that:
  http://example.com/?query=HTML code
- remember that?
  http://www.wolfgang-schaeuble.de/?search= …

TECHNISCHE UNIVERSITÄT DRESDEN

STEPPING DOWN

XSS

- can inject <script> code
- this code will run with the privileges of the embedding site (think IE zones)
- **cross-site scripting**

- Can you steal site credentials with this?
- imagine a bank website allowing injection
- How do you exfiltrate the password?

SAME ORIGIN

- JavaScript can access password fields
- you cannot use AJAX to send the password
- **same origin policy**
  - JavaScript may only connect back to the originating server (with some tolerance)
- can be defeated with <img> tags
  - encode password in URL to ping your server
- JavaScript can also read cookies…

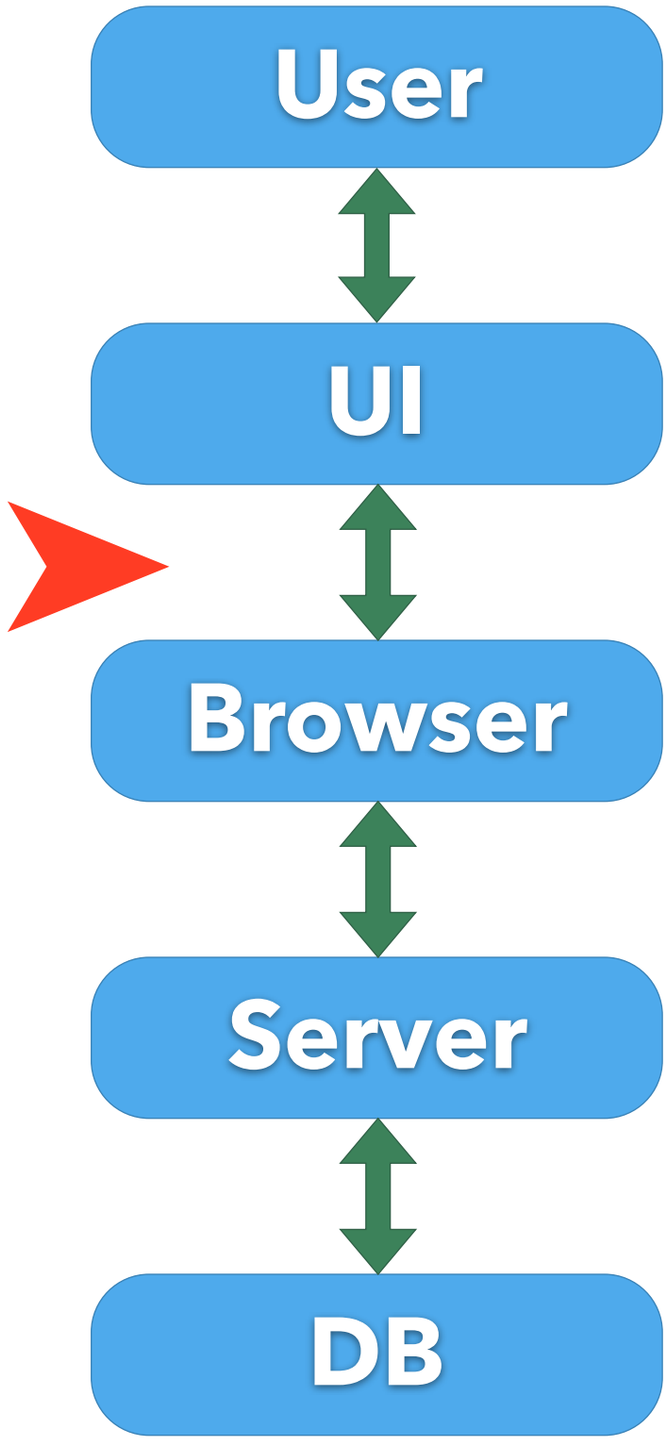
FIXES

- disallow cross-site image loading?
  - lots of sites use this
- no JavaScript access to password field?
  - AJAX logins need this
- fix web application
  - well…
- never click on suspicious links
- always use SSL

So you think SSL works?

- You explicitly type https://?
- Your site loads all JavaScript securely?
- Your platform checks for certificate revocation?
- … and for X.509 Basic Constraints?
- You trust all CAs on this planet to never issue broken certs?

REMOTE CONTROL



- goal: trick the browser to not show what's actually happening
- or: how to pull strings behind the user's back
- or: can one website control another one?
- no mischief with the server communication

SCENARIO

- user visits a regular website you control
- Can you use credentials of a different site?
- some preconditions
  - user is logged in to the target site in another browser tab
  - the target site identifies the user session with a cookie
- no cross-site cookie leakage in browser

CSRF

- same origin policy denies AJAX to target
- again, <img> is your friend
- one website can send arbitrary requests to another, unrelated site
- **cross site request forgery**
- a special case of the **confused deputy problem**
- requests are blindly operating the target

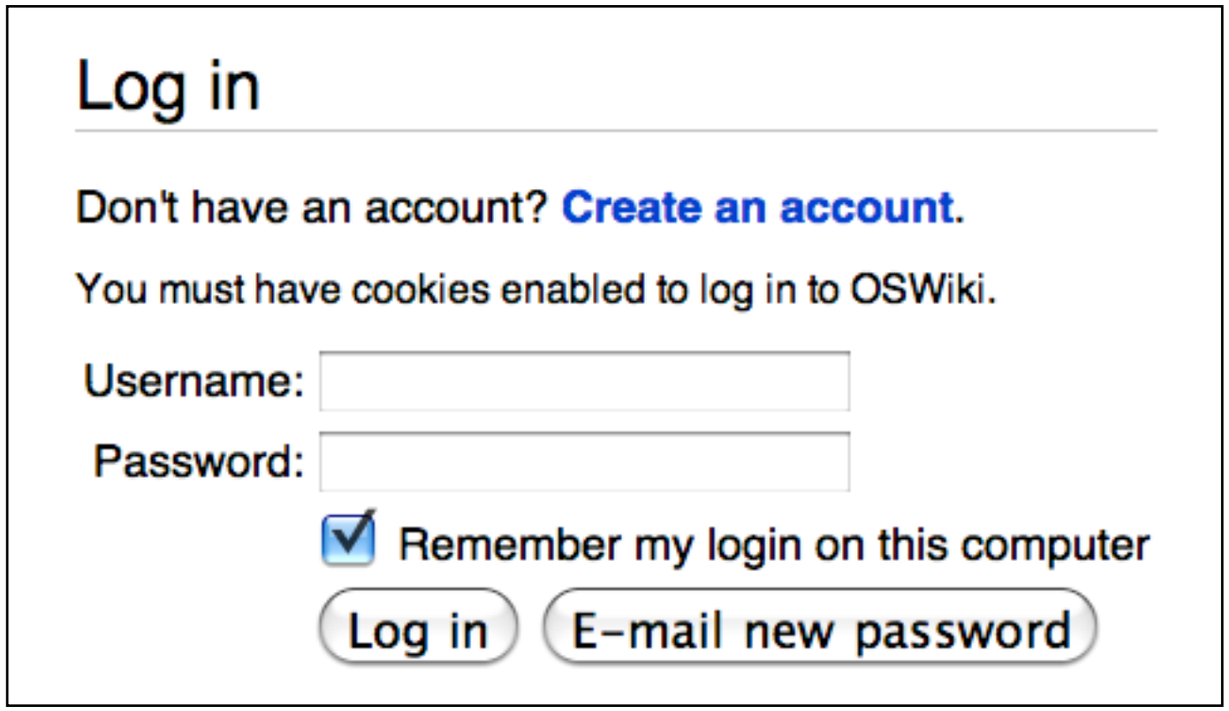
CAN DO

- send requests and GET parameters
  - click buttons in the UI of the target site
  - operate search fields and other text input
- basic or digest authentication? cookies?
  - browser automatically sends credential
  - session riding
- POST requests?
  - manufacture a <form> instead of <img>

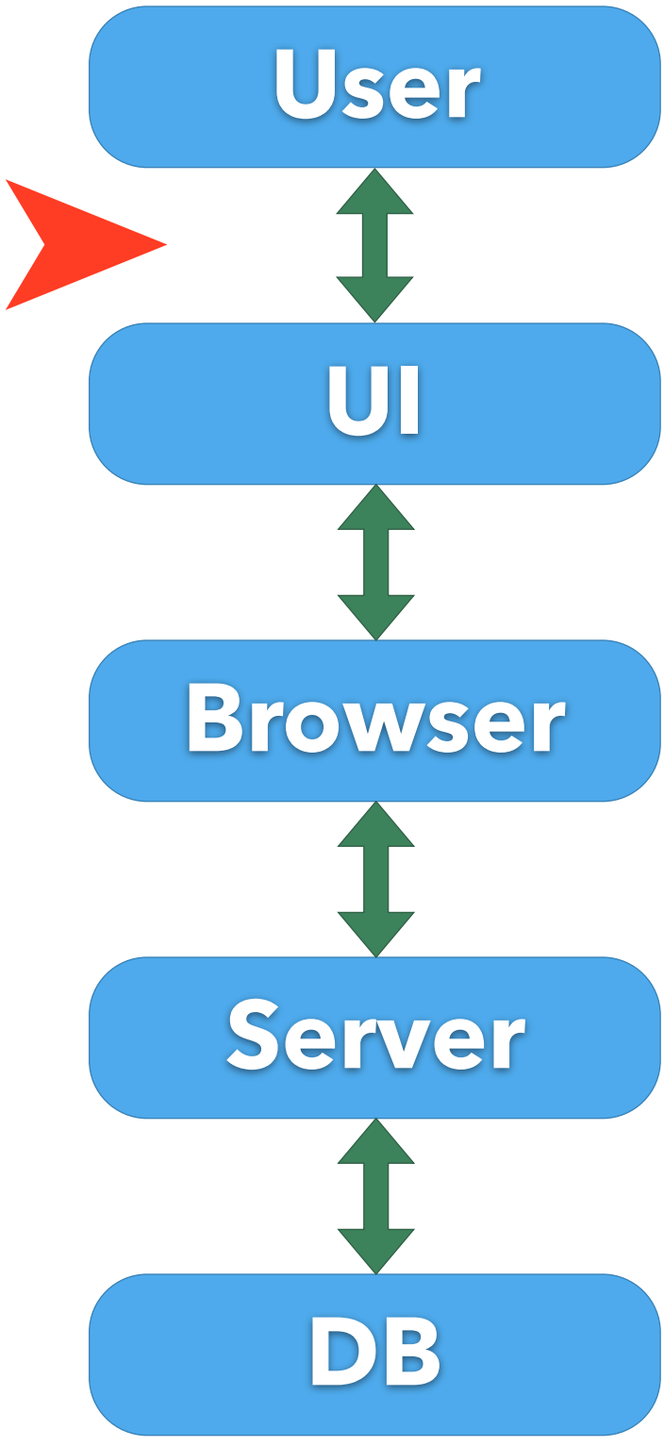
TARGETS

- study in late 2008: high-profile bank websites vulnerable
- browser-based port scanning
  - this is behind the corporate firewall
- WiFi routers with web interface
  - disable firewall
  - reset wifi protection
  - enable UPnP

- disable cross-site POST requests
  - GET requests should by definition never change persistent state
- never authenticate a change of persistent state by cookie only
- pass an additional credential
  - session ID in URL, edit tokens


Log in
Don't have an account? Create an account.
You must have cookies enabled to log in to OSWiki.
Username:
Password:
Remember my login on this computer
Log in
E-mail new password

BLINDNESS



- goal: mislead the user to not seeing what's actually happening
- nothing going on behind your back
- the internal state of the browser is properly displayed
- but you don't notice…

PICK ONE

www.paypal.com

CYRILLIC SMALL LETTER A (U+0430)

LATIN SMALL LETTER A (U+0061)

www.paypal.com

homograph attack

GENERALIZE

FRACTION SLASH (U+2044)

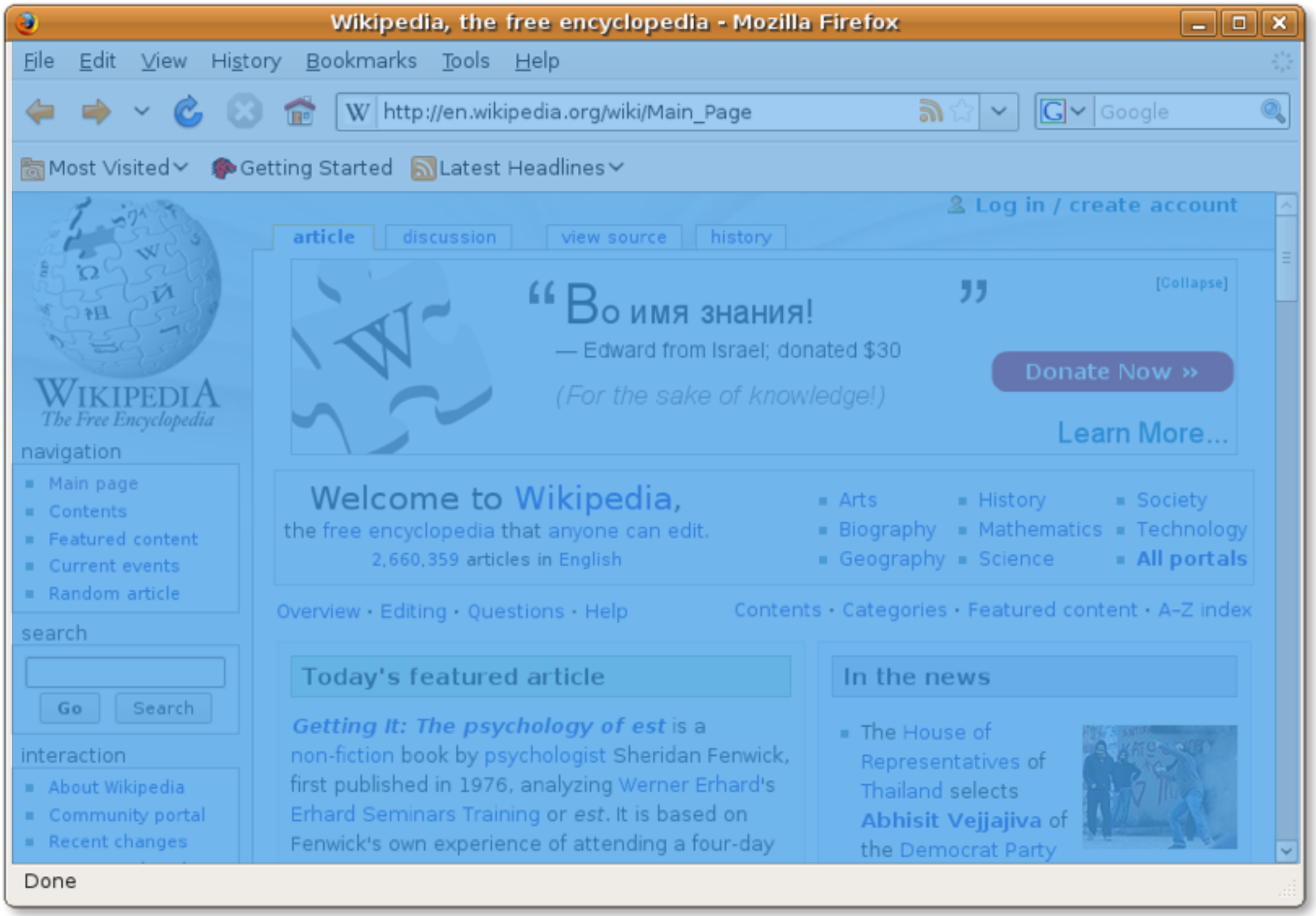
https://www.bank.com/account/login.ab.cd

www.bank.xn--comaccountlogin-uh0iha.ab.cd

https://www.bank.com/account/login.ab.cd

www.bank.com

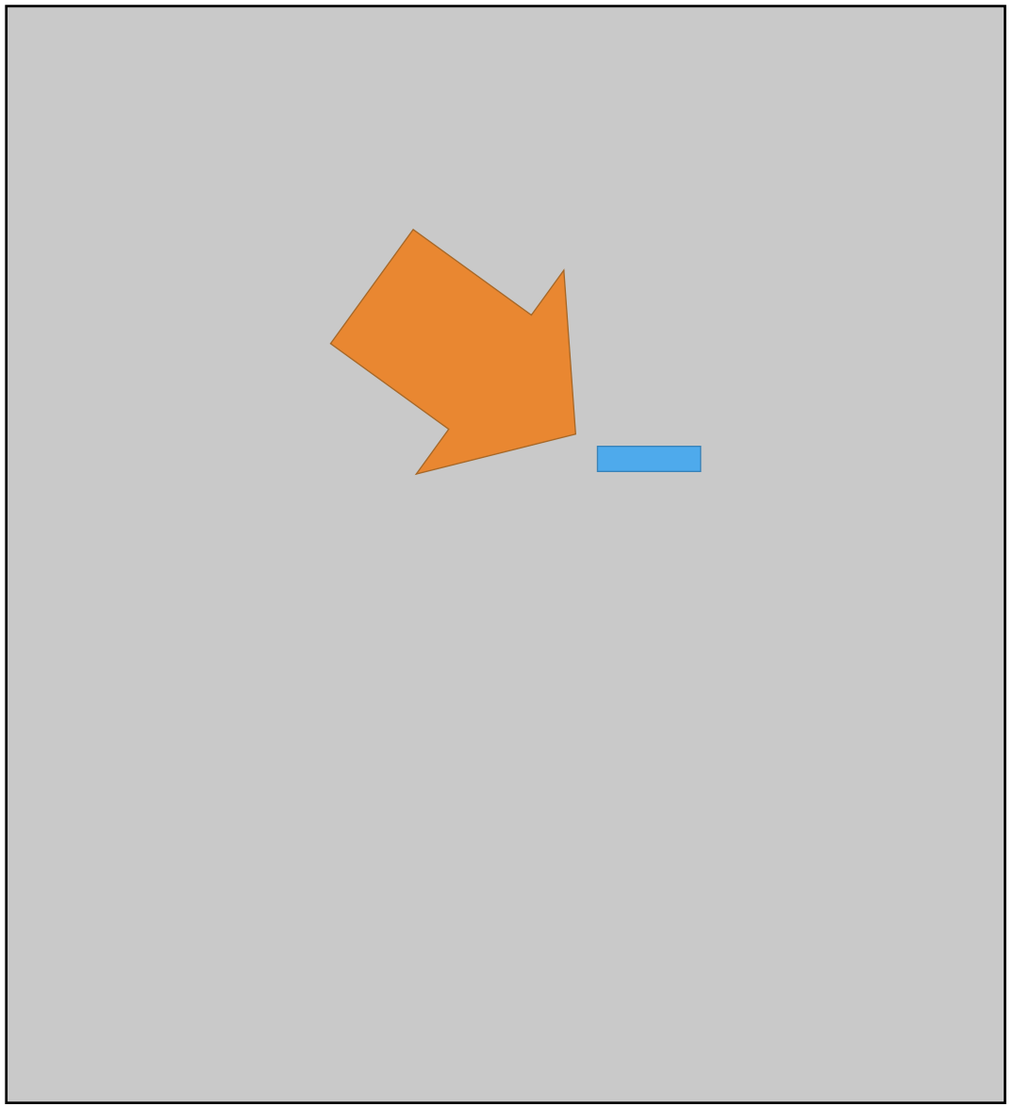
CONTENT

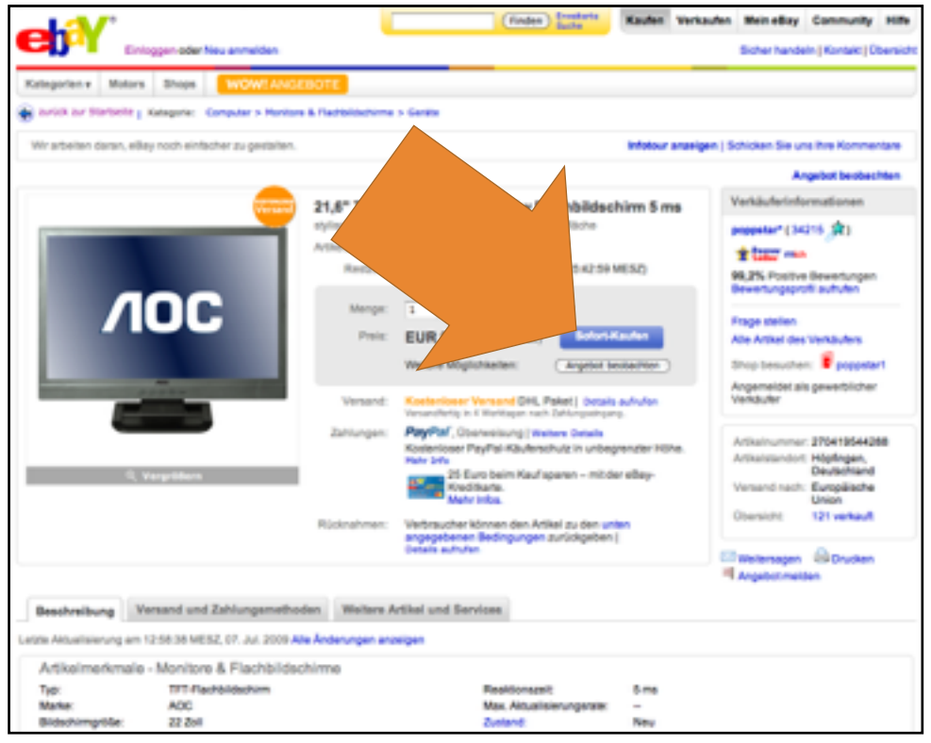

Wikipedia, the free encyclopedia - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://en.wikipedia.org/wiki/Main_Page
Google
Most Visited
Getting Started
Latest Headlines
Log in / create account
article
discussion
view source
history
WIKIPEDIA
The Free Encyclopedia
"Во имя знания!"
— Edward from Israel; donated $30
(For the sake of knowledge!)
[Collapse]
Donate Now »
Learn More...
navigation
Main page
Contents
Featured content
Current events
Random article
search
Go
Search
interaction
About Wikipedia
Community portal
Recent changes
Welcome to Wikipedia,
the free encyclopedia that anyone can edit.
2,660,359 articles in English
Arts
Biography
Geography
History
Mathematics
Science
Society
Technology
All portals
Overview · Editing · Questions · Help
Contents · Categories · Featured content · A–Z index
Today's featured article
Getting It: The psychology of est is a non-fiction book by psychologist Sheridan Fenwick, first published in 1976, analyzing Werner Erhard's Erhard Seminars Training or est. It is based on Fenwick's own experience of attending a four-day
In the news
The House of Representatives of Thailand selects Abhisit Vejjajiva of the Democrat Party
Done

PADLOCKS


PayPal
Startseite
Privatkunden
Geschäftskunden
Shopping-Portal
Konto-Login
E-Mail-Adresse
PayPal-Passwort
Einloggen
E-Mail-Adresse oder Passwort vergessen?
Neu bei PayPal? Neu anmelden
Das Prinzip PayPal.
Online zahlen – einfach und sicher.
PayPal
giropay
VISA
Über uns | Impressum | Kontotypen | Gebühren | Datenschutz | Sicherheit | Kontakt | AGB | Jobs | Sammelzahlung |
VeriSign Identity Protection
Copyright © 1999-2009 PayPal. Alle Rechte vorbehalten.

CLICKJACKING

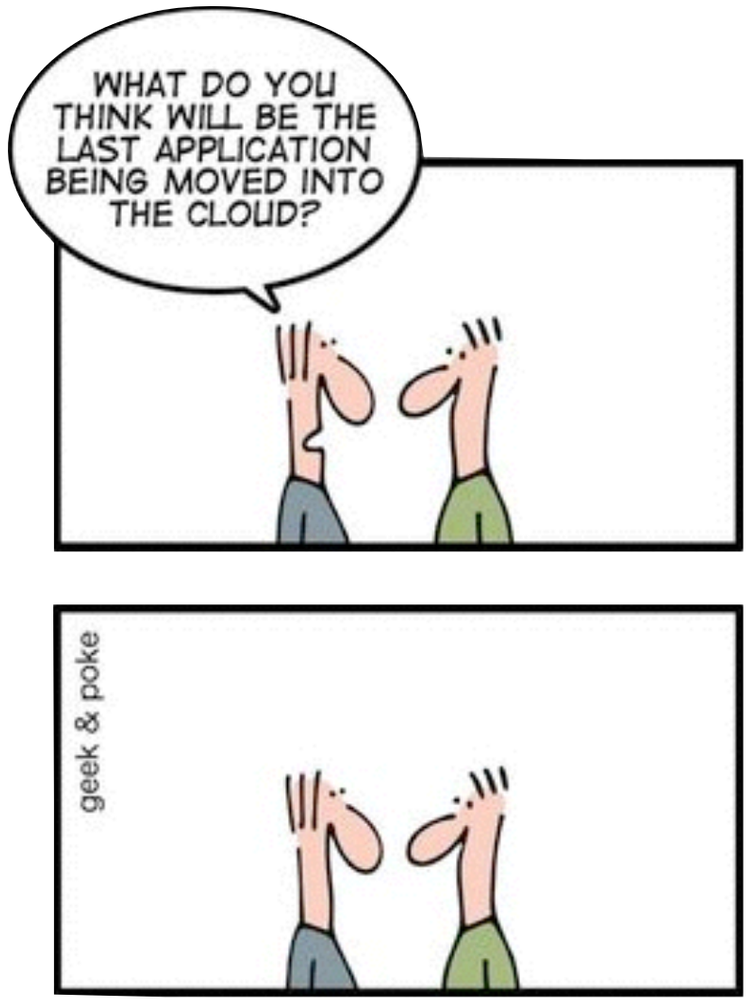


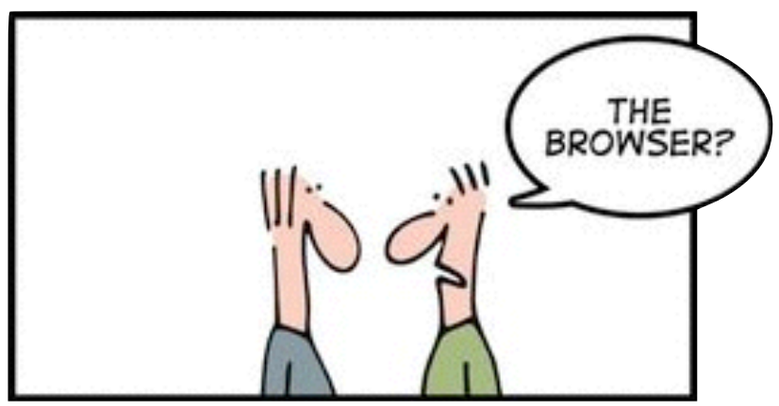


- this only works when logged in
  - always log out explicitly
  - do not use persistent logins
- you may want to check wether your password manager autofills inside frames

CONCLUSION

- web standards have gotten complex
- even bug-free behavior is vulnerable
- browsers are a bad application platform
- we did not even talk about WebSockets, WebGL, WebRTC, …





SUMMARY

Is everything lost?

Yes