TECHNISCHE UNIVERSITÄT DRESDEN

Department of Computer Science Institute of System Architecture, Operating Systems Group

PROBLEMS IN PRACTICE: THE WEB

MICHAEL ROITZSCH

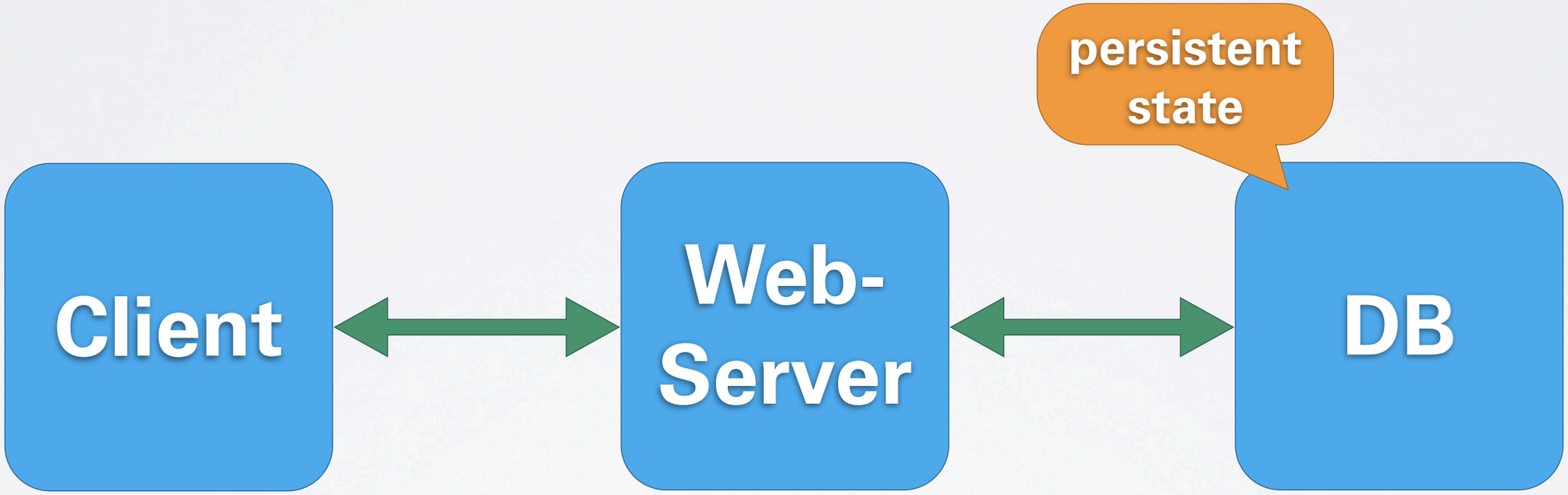
TECHNISCHE UNIVERSITÄT DRESDEN

THE WEB AS A DISTRIBUTED SYSTEM

TECHNISCHE UNIVERSITÄT DRESDEN

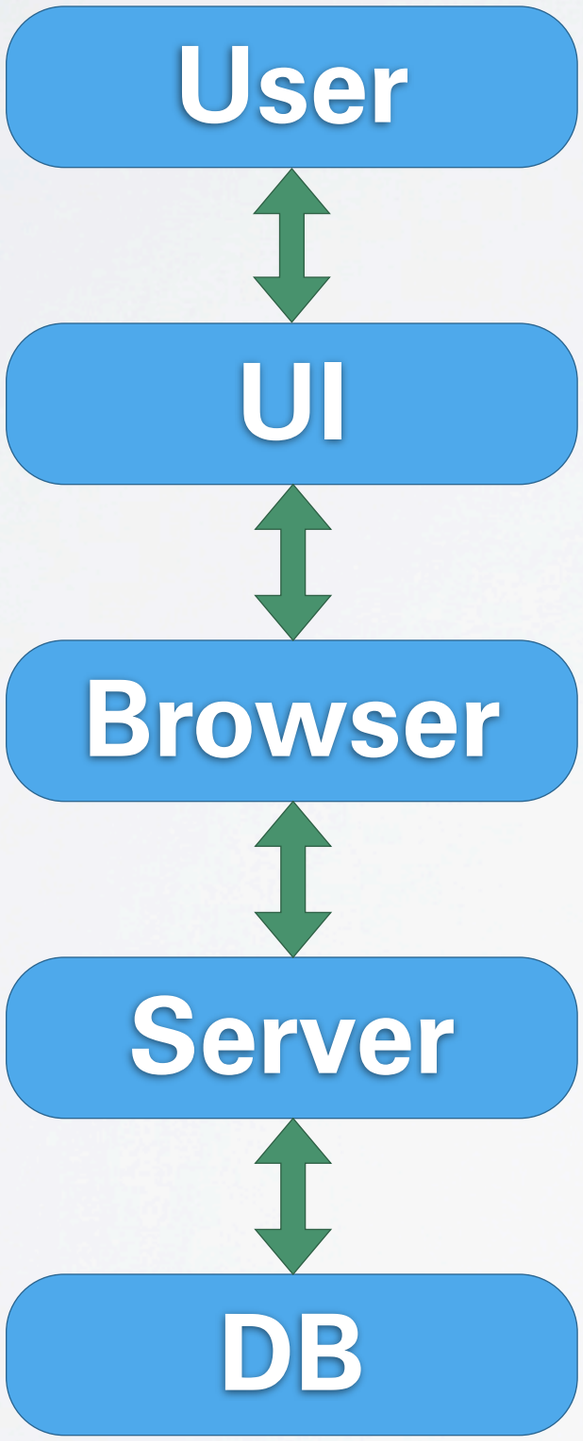
WEB HACKING SESSION

3-TIER



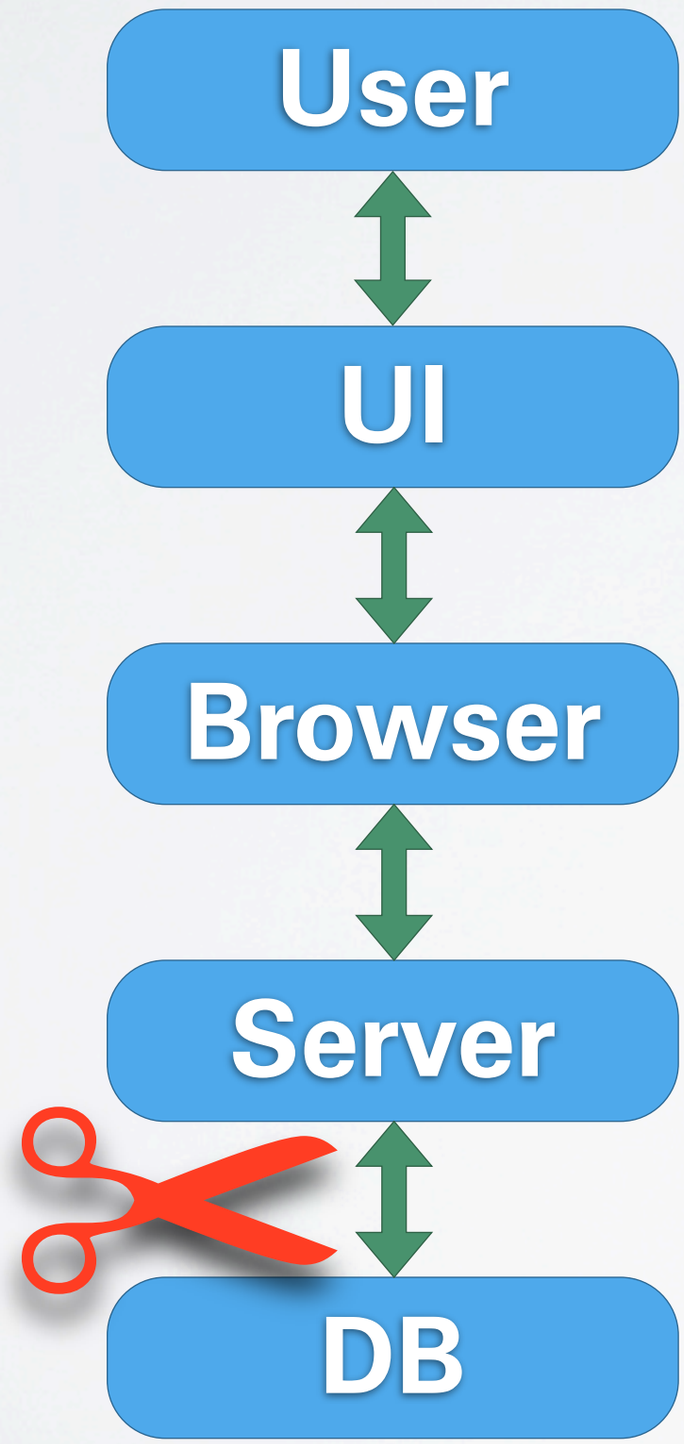
Presentation		Application Logic		Data
HTML JavaScript AJAX	HTTP	PHP EJB WebObjects	SQL	Relations

SCENARIO



- user accesses a sensitive 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 backend DB
- not directly accessible (hopefully)
- improper input checking in frontend server required
- nice: inconsistency is persistent

EXAMPLE IN PHP

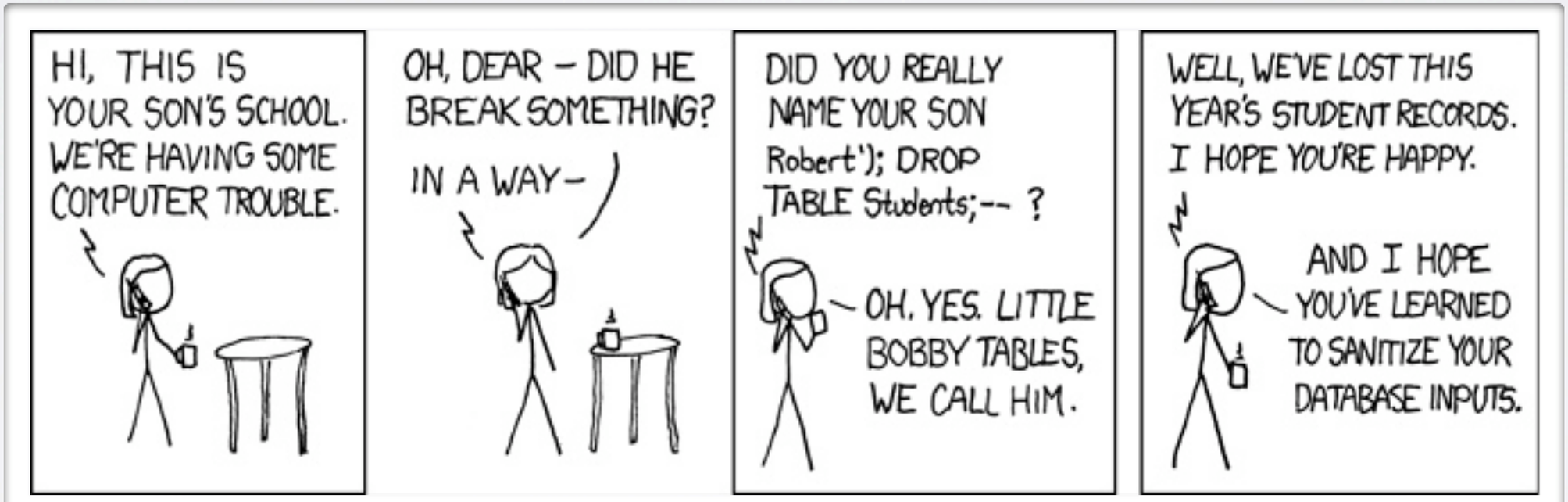
```
$password = $_POST['password'];

$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

TECHNISCHE UNIVERSITÄT DRESDEN

LICENSE PLATE

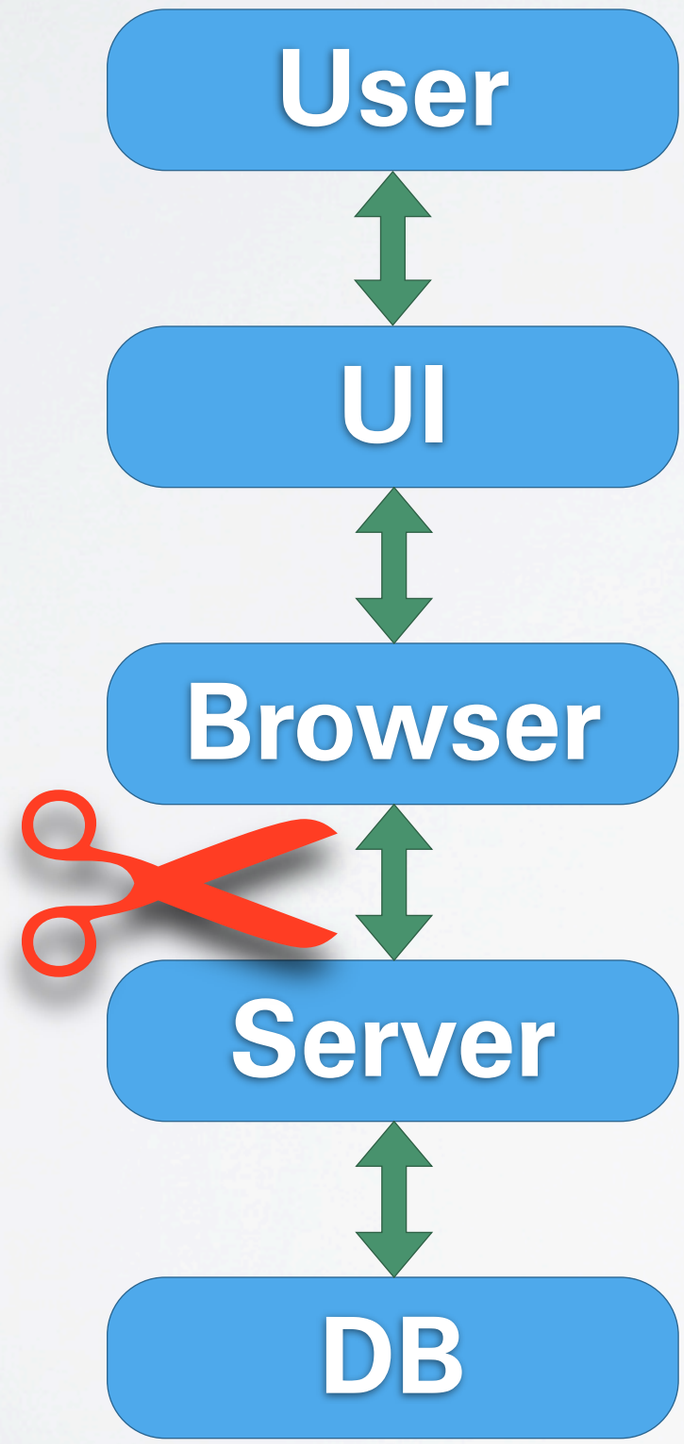
TECHNISCHE UNIVERSITÄT DRESDEN

VARIATIONS

- exploit other flaws in the application logic
- insufficient boundaries between users
  - Hotmail hole exposes mails of other users
- security by obscurity
  - URL guessing can expose hidden resources
- logic bombs
  - Mikeyy worm on Twitter used code injection via custom CSS to replicate

always sanitize input

FRONTEND



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

EXAMPLE

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

TECHNISCHE UNIVERSITÄT DRESDEN

STEPPING DOWN

XSS

- sometimes this type of **HTML injection** is improperly called **cross-site scripting**
- injection (both HTML and SQL) can **become** cross-site scripting (XSS) attacks

- just embed `<script>` tags and send code
- this code will run with the privileges of the embedding site (think IE zones)
- the script can then operate the site for you

CREDENTIALS

- Can you steal site credentials with this?
- imagine a bank website allowing injection
- What do we have?
  - user needs to click attacker-provided link
  - you could display a fake login form
  - even with some JavaScript
  - the browser would indicate proper SSL
- How do you get the password?

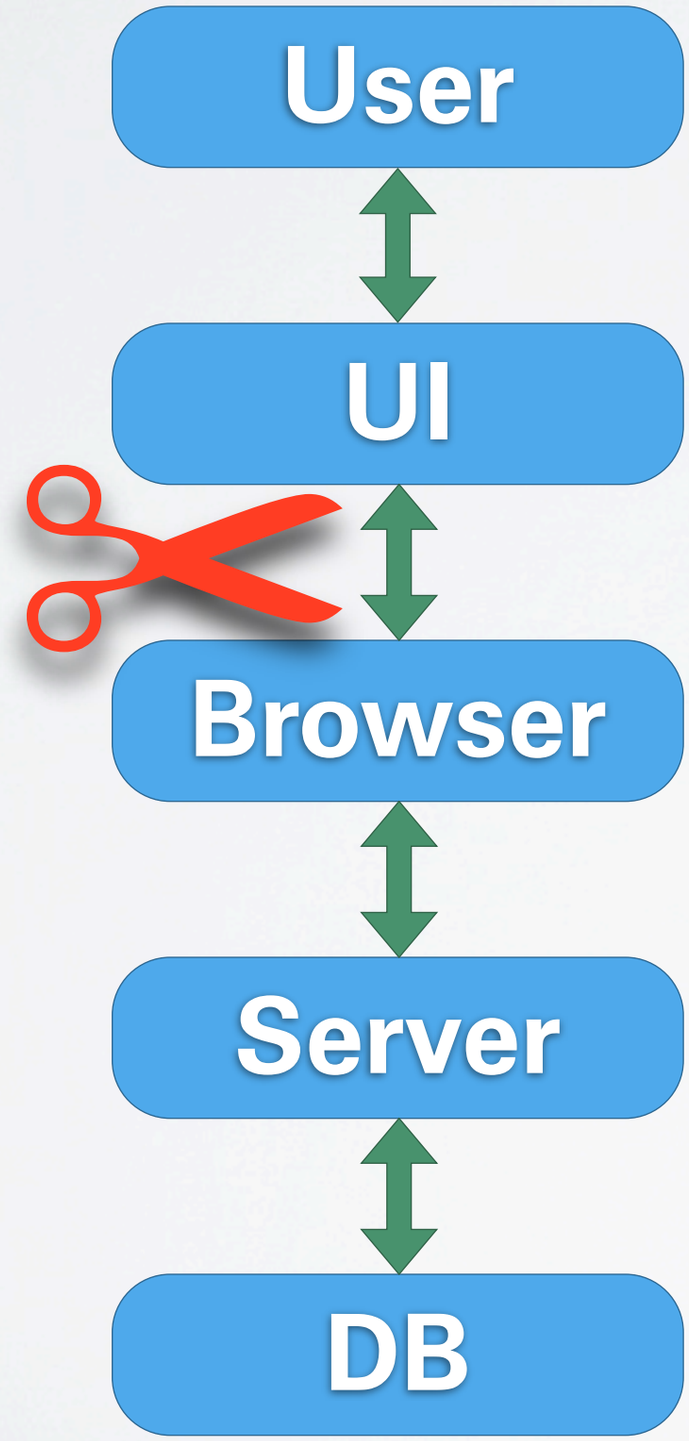
SAME ORIGIN

- JavaScript can access password fields
- you cannot use AJAX to get 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…

FIX

- fix web application
  - well…
- disallow cross-site image loading?
  - lots of sites use this
- no JavaScript access to password field?
  - AJAX logins need this

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 obtain 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 prevents 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**
- the requests are made blindly

CAN DO

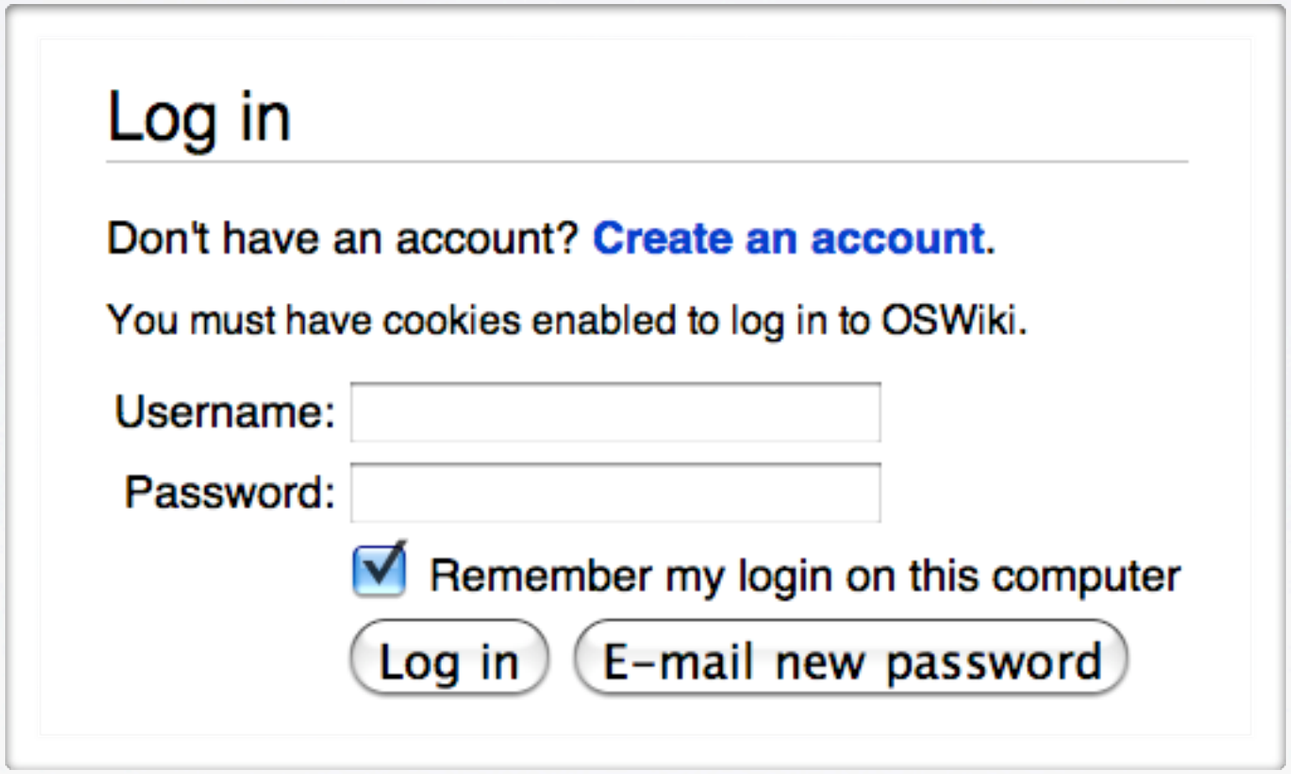
- send requests and GET parameters
  - click buttons in the UI of the target site
  - operate search fields and other text input
- basic or digest authentication? cookies?
  - browser automatically sends credential
  - **session riding**
- POST requests?
  - manufacture a `<form>` instead of `<img>`

TARGETS

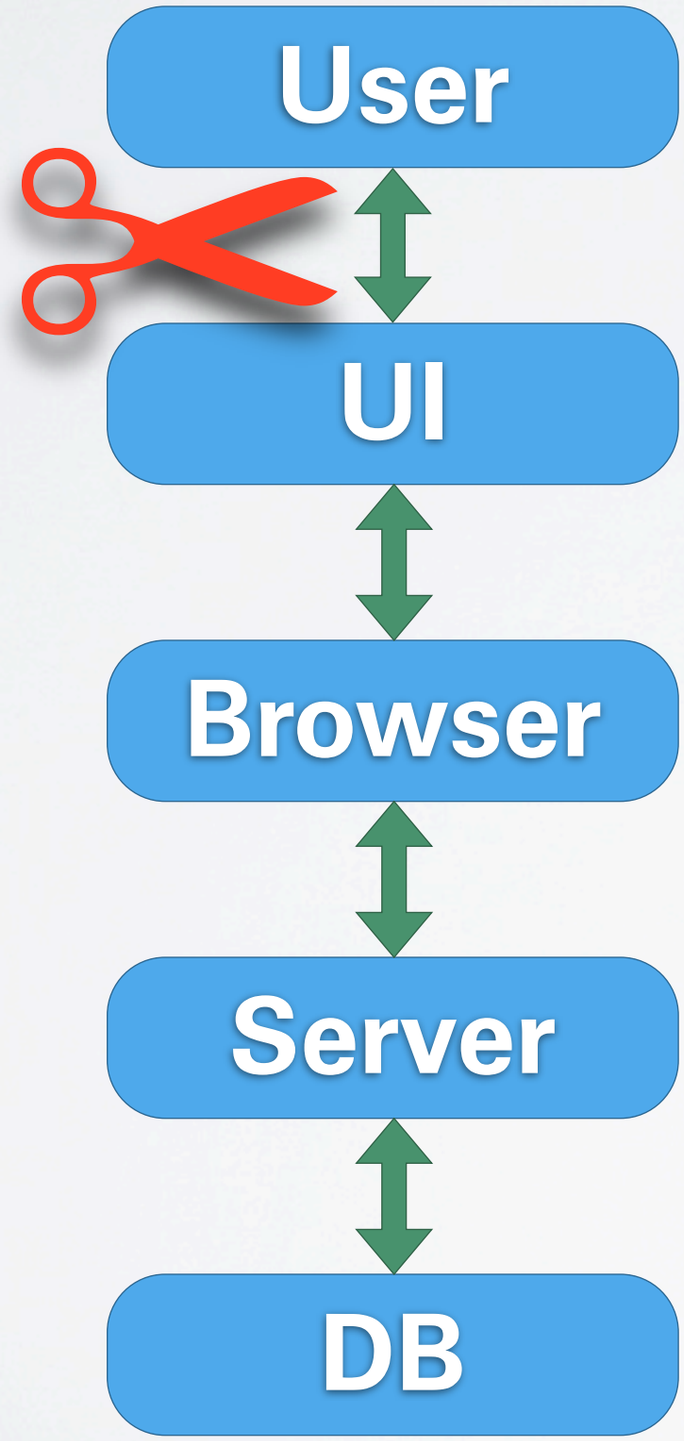
- study in late 2008: high-profile bank websites vulnerable
- DSL-Routers
  - disable firewall
  - reset wifi protection
  - enable UPnP
- browser-based port scanning
  - this is behind the corporate firewall

FIX

- disable cross-site POST requests
  - GET requests should by definition never change persistent state
  - there is a Firefox plugin for that
- 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

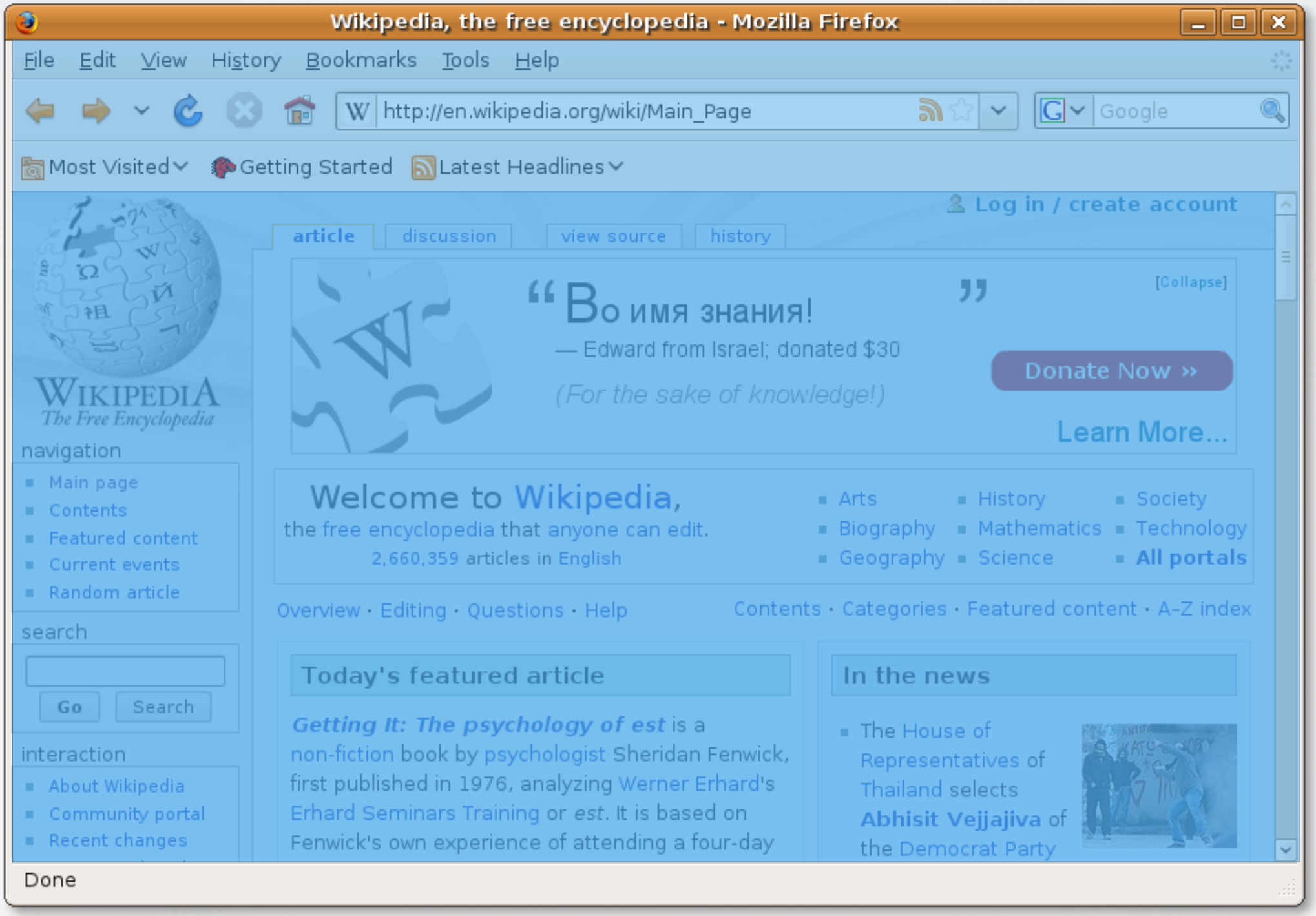
CYRILLIC SMALL LETTER A (U+0430)

LATIN SMALL LETTER A (U+0061)

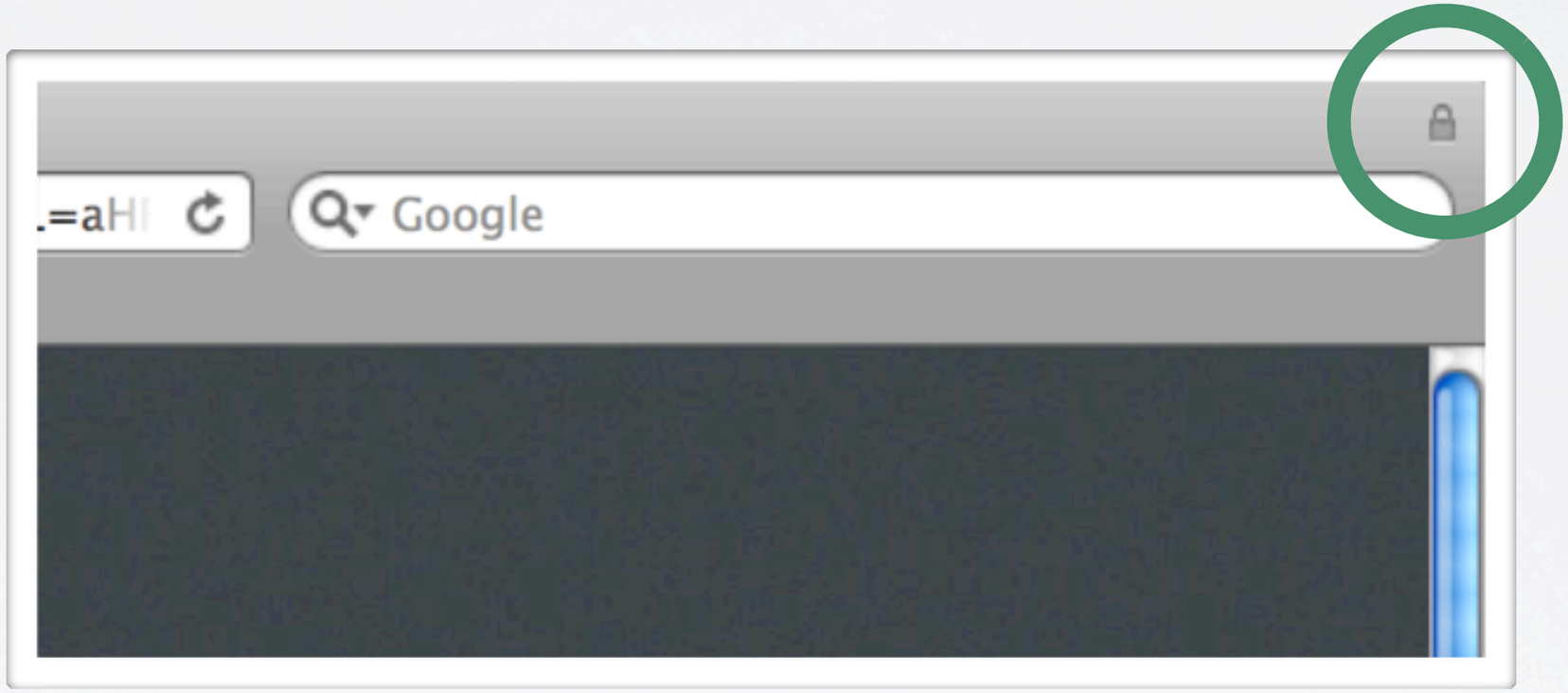
www.paypal.com

homograph attack

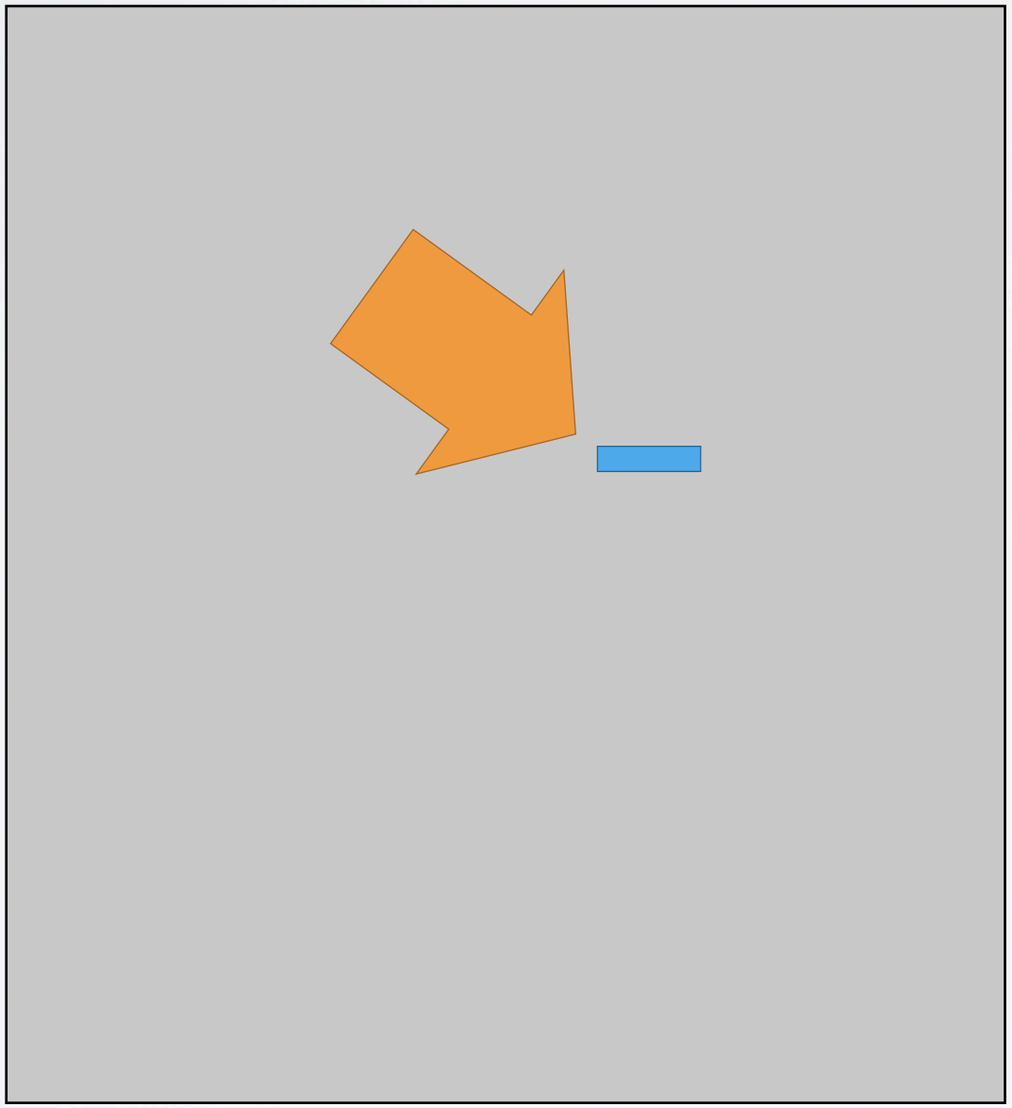
CONTENT

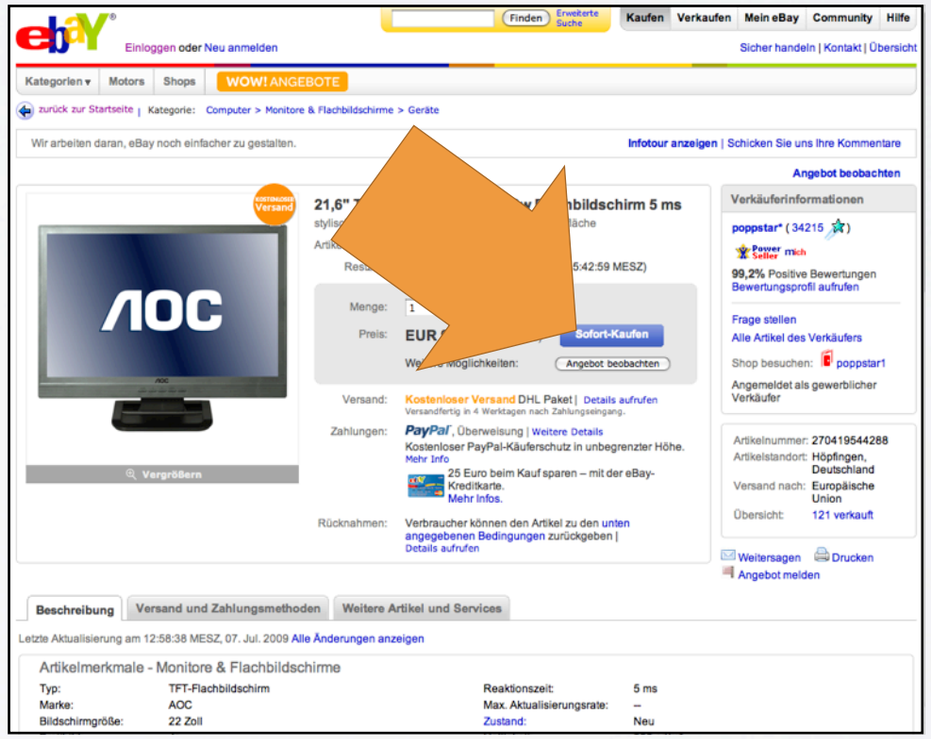

Wikipedia, the free encyclopedia - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://en.wikipedia.org/wiki/Main_Page
Google
Most Visited
Getting Started
Latest Headlines
Log in / create account
article
discussion
view source
history
WIKIPEDIA
The Free Encyclopedia
"Во имя знания!"
— 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

BETTER

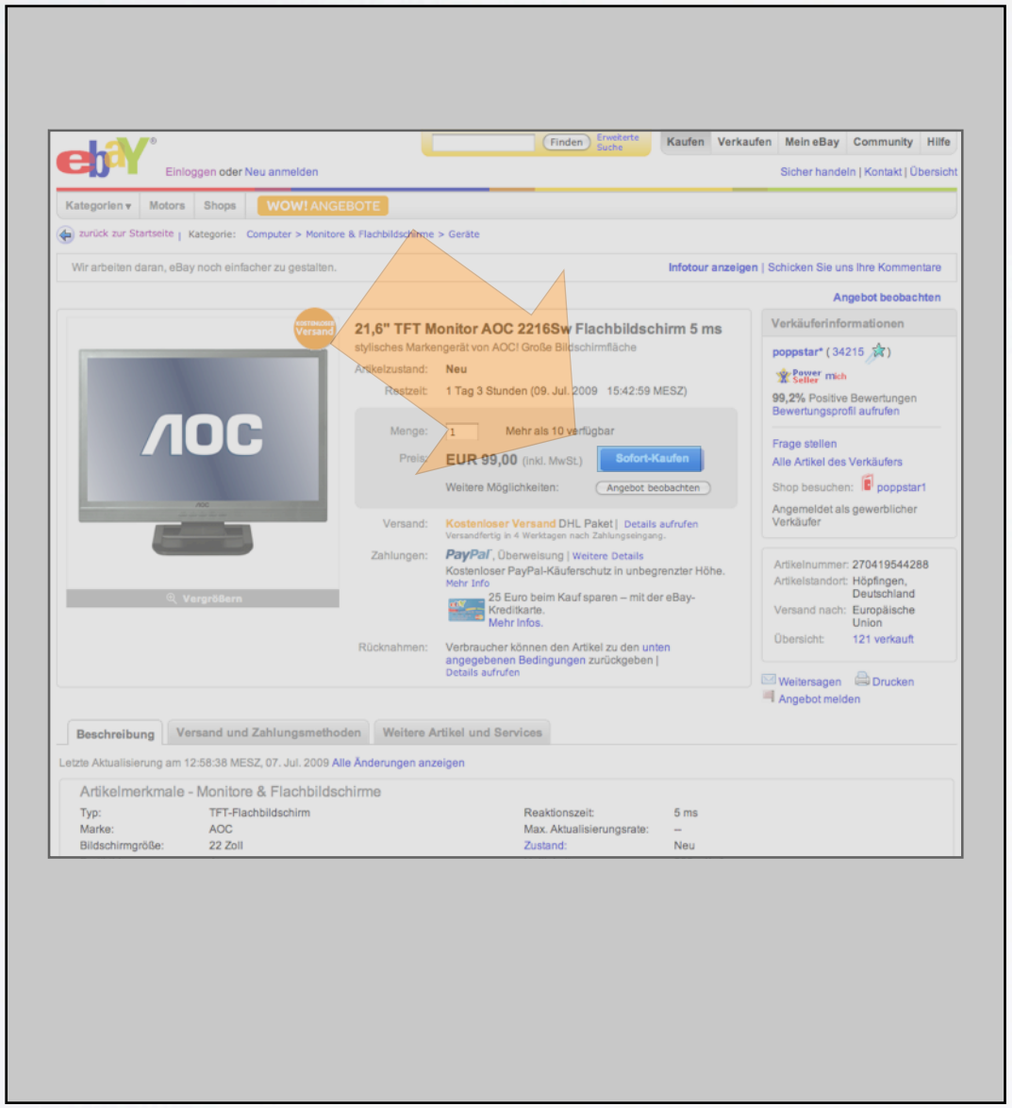


CLICKJACKING





CLICKJACKING



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

SUMMARY

Is everything lost?

Yes