TECHNISCHE UNIVERSITÄT DRESDEN

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

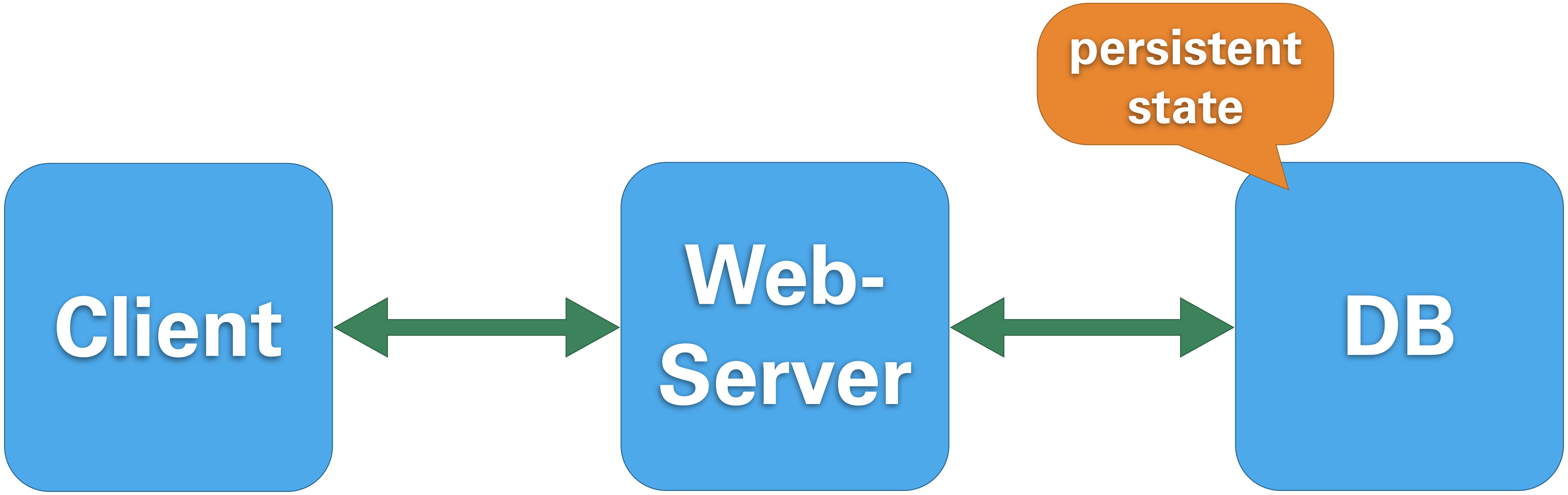
PROBLEMS IN PRACTICE: THE WEB

MICHAEL ROITZSCH

THE WEB AS A DISTRIBUTED SYSTEM

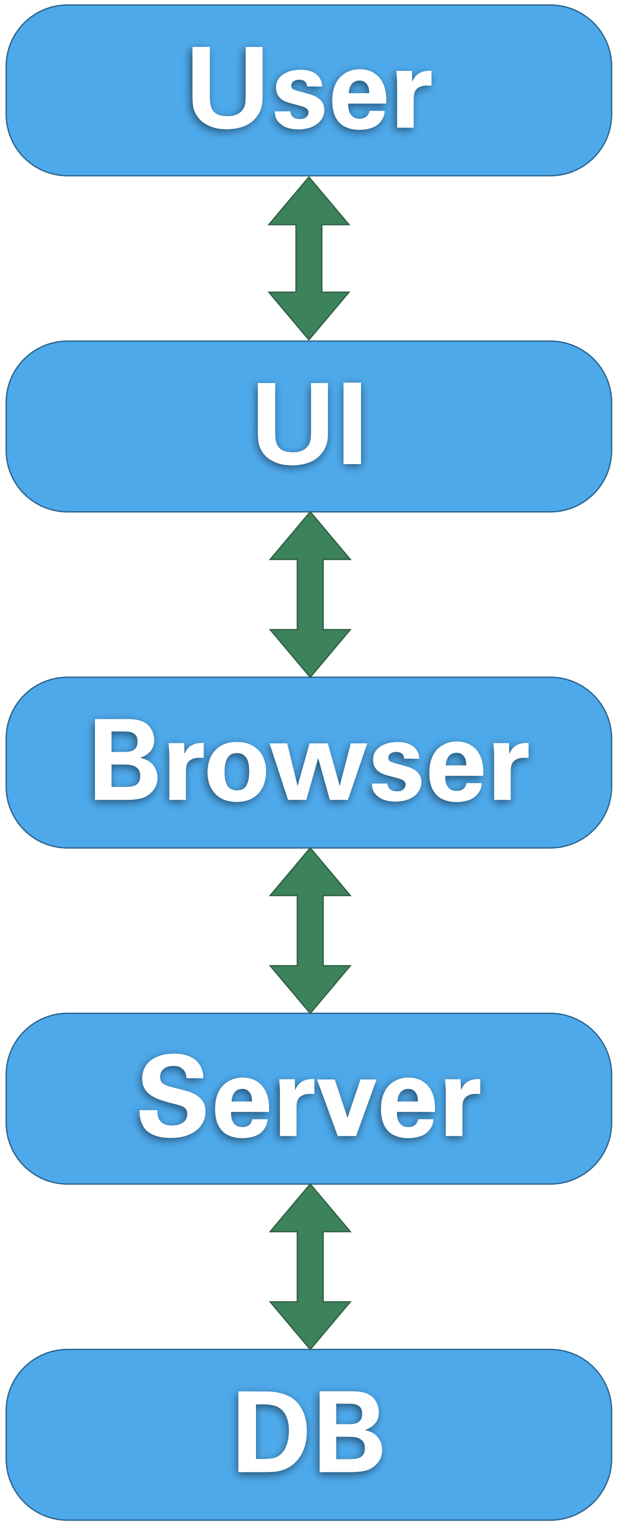
WEB HACKING SESSION

3-TIER



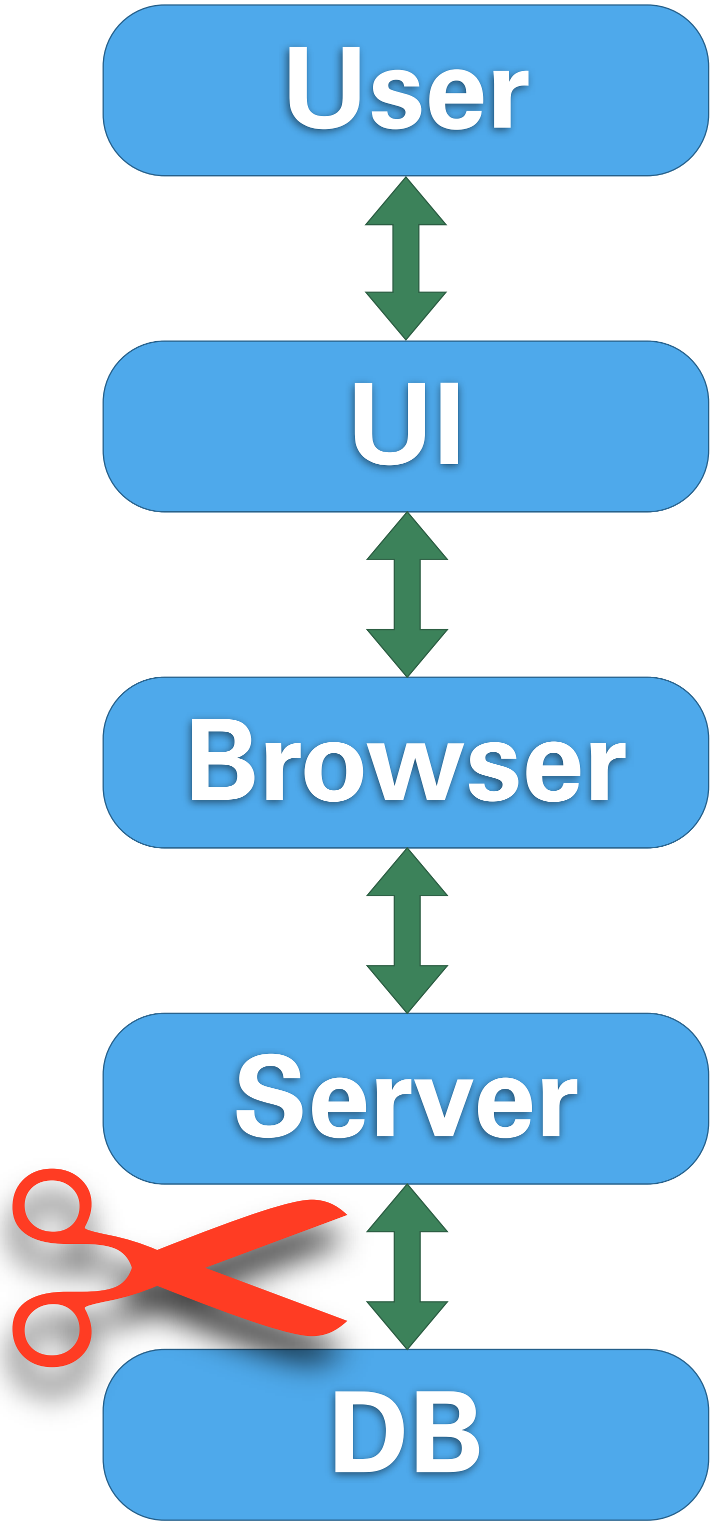
Presentation		Application Logic		Data
HTML JavaScript AJAX	HTTP	PHP EJB WebObjects	SQL	Relations

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

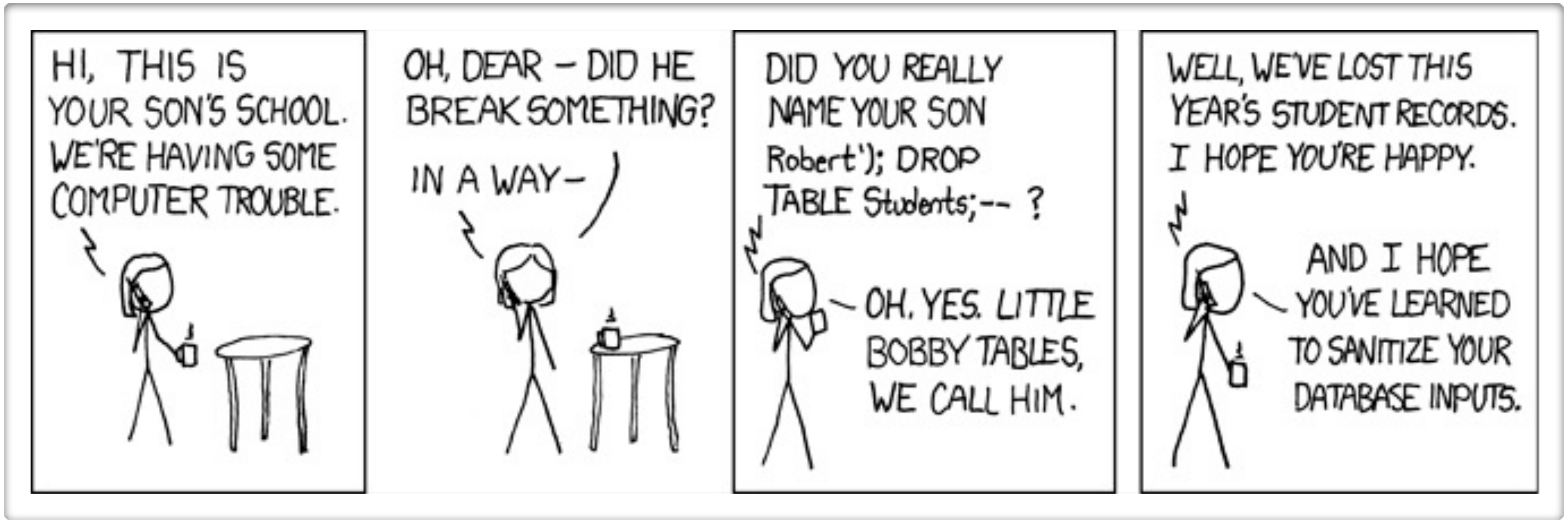
```
$password = $_POST['password'];

$id = $_POST['id'];

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

Now imagine: `password=';--`

SQL injection

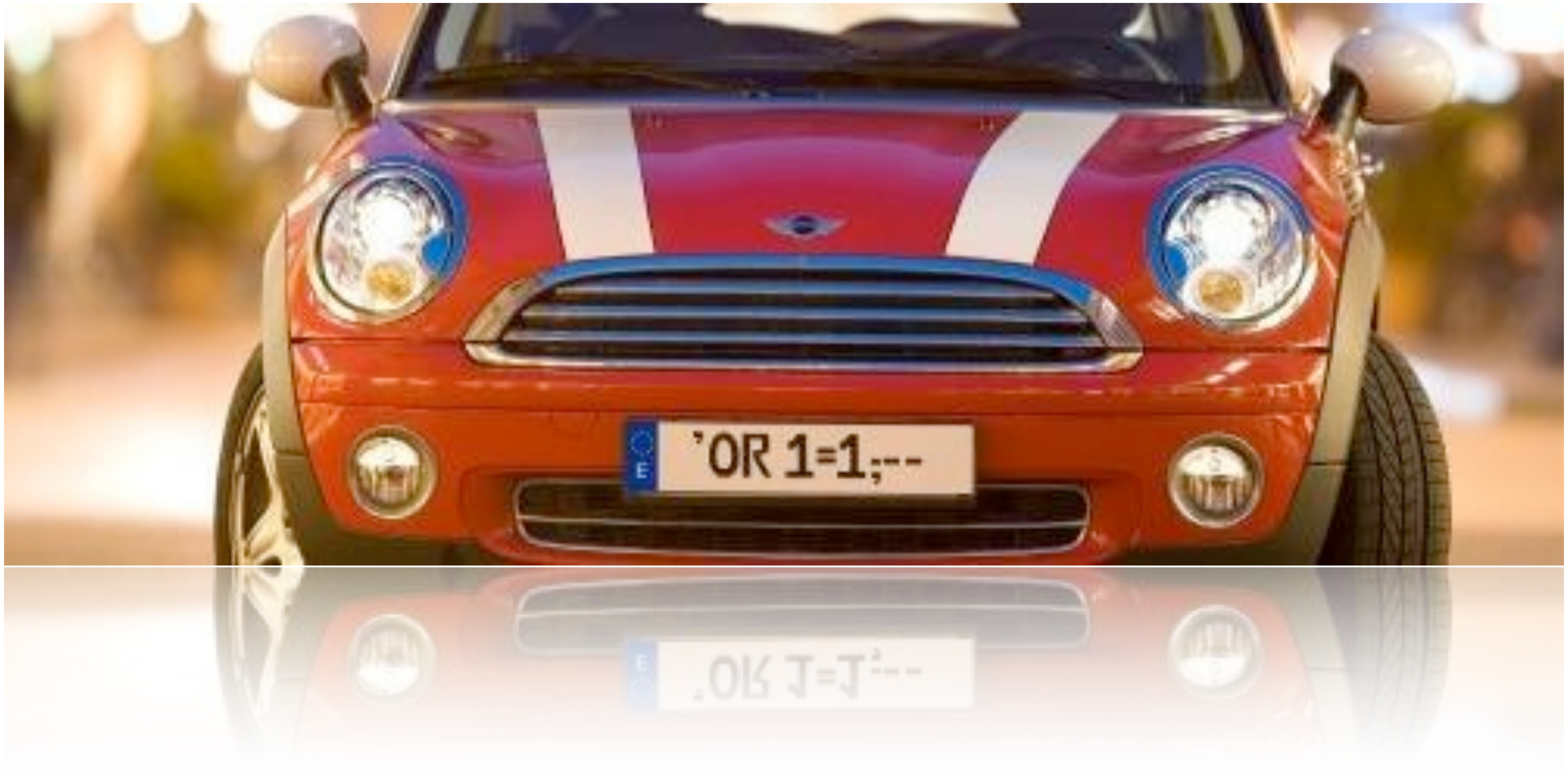
TECHNISCHE UNIVERSITÄT DRESDEN

BOBBY TABLES

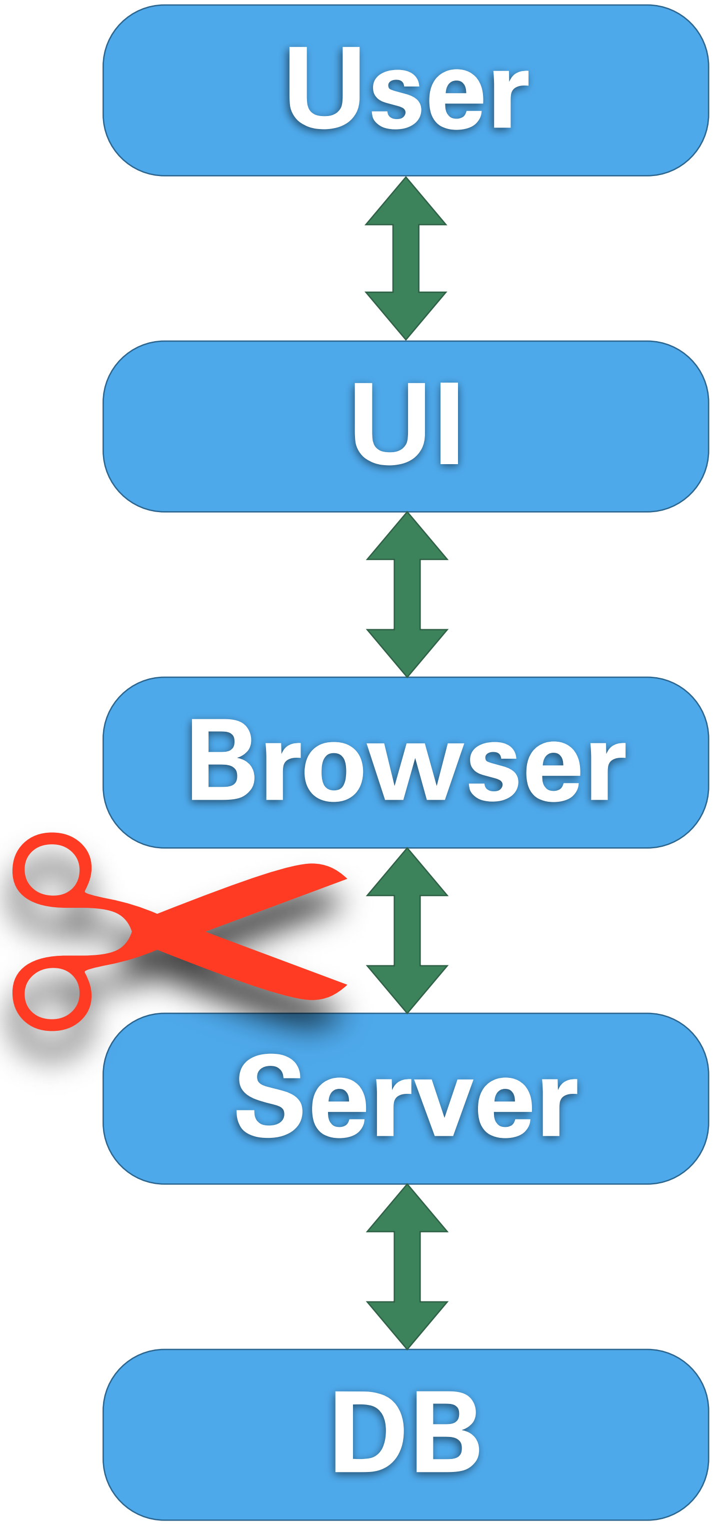

HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Comic by Randall Munroe, xkcd.com

LICENSE PLATE



FRONTEND

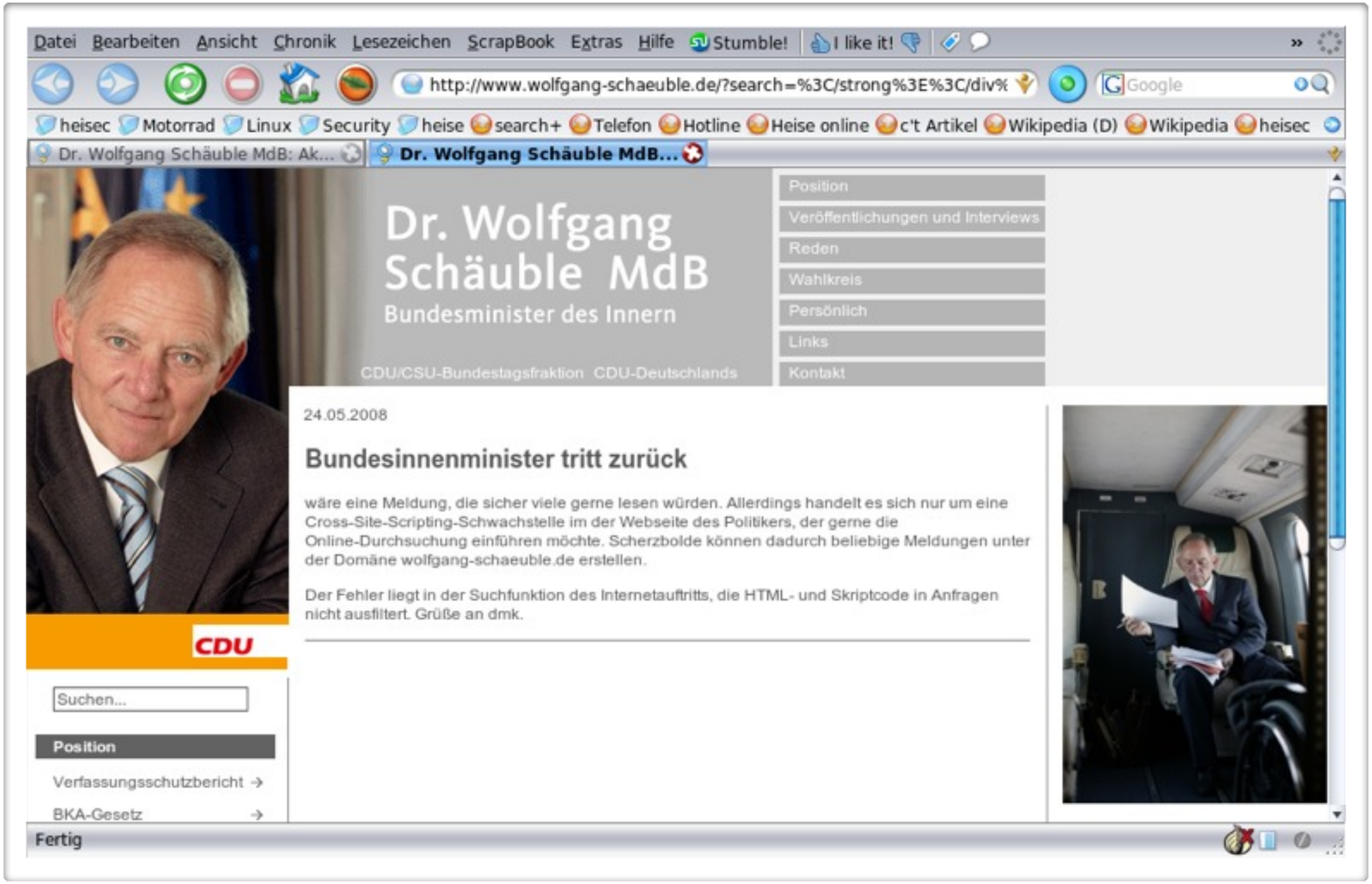


- **goal:** manipulate content delivered to the browser
- infrastructure attacks like DNS cache poisoning
- solution for this:
  make sure you use SSL
- … and check CRLs
- improper input checking can still bite you

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>…`

STEPPING DOWN


Datei Bearbeiten Ansicht Chronik Lesezeichen ScrapBook Extras Hilfe Stumble! I like it!
Google
heisec Motorrad Linux Security heise search+ Telefon Hotline Heise online c't Artikel Wikipedia (D) Wikipedia heisec
Dr. Wolfgang Schäuble MdB: Ak...
Dr. Wolfgang Schäuble MdB...
Dr. Wolfgang Schäuble MdB
Bundesminister des Innern
CDU/CSU-Bundestagsfraktion CDU-Deutschlands
Position
Veröffentlichungen und Interviews
Reden
Wahlkreis
Persönlich
Links
Kontakt
CDU
Suchen...
Position
Verfassungsschutzbericht →
BKA-Gesetz →
Fertig

http://www.wolfgang-schaeuble.de/?search=%3C/strong%3E%3C/div%

24.05.2008

Bundesinnenminister tritt zurück

wäre eine Meldung, die sicher viele gerne lesen würden. Allerdings handelt es sich nur um eine Cross-Site-Scripting-Schwachstelle im der Webseite des Politikers, der gerne die Online-Durchsuchung einführen möchte. Scherzbolde können dadurch beliebige Meldungen unter der Domäne wolfgang-schaeuble.de erstellen.

Der Fehler liegt in der Suchfunktion des Internetauftritts, die HTML- und Skriptcode in Anfragen nicht ausfiltert. Grüße an dmk.

CREDENTIALS

- Can you steal site credentials with this?
- imagine a bank website allowing injection
- What do we have?
  - there is the standard bank login on the page
  - you can inject a script into the page
  - you want to keep the login form functional
- How do you get 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…

FIX

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

TECHCRUNCH

techcrunch.com

googleadservices.com

facebook.com

snap.com

wordpress.com

topsy.com

doubleclick.net

undertone.com

quantserve.com

crunchboard.com

google-analytics.com

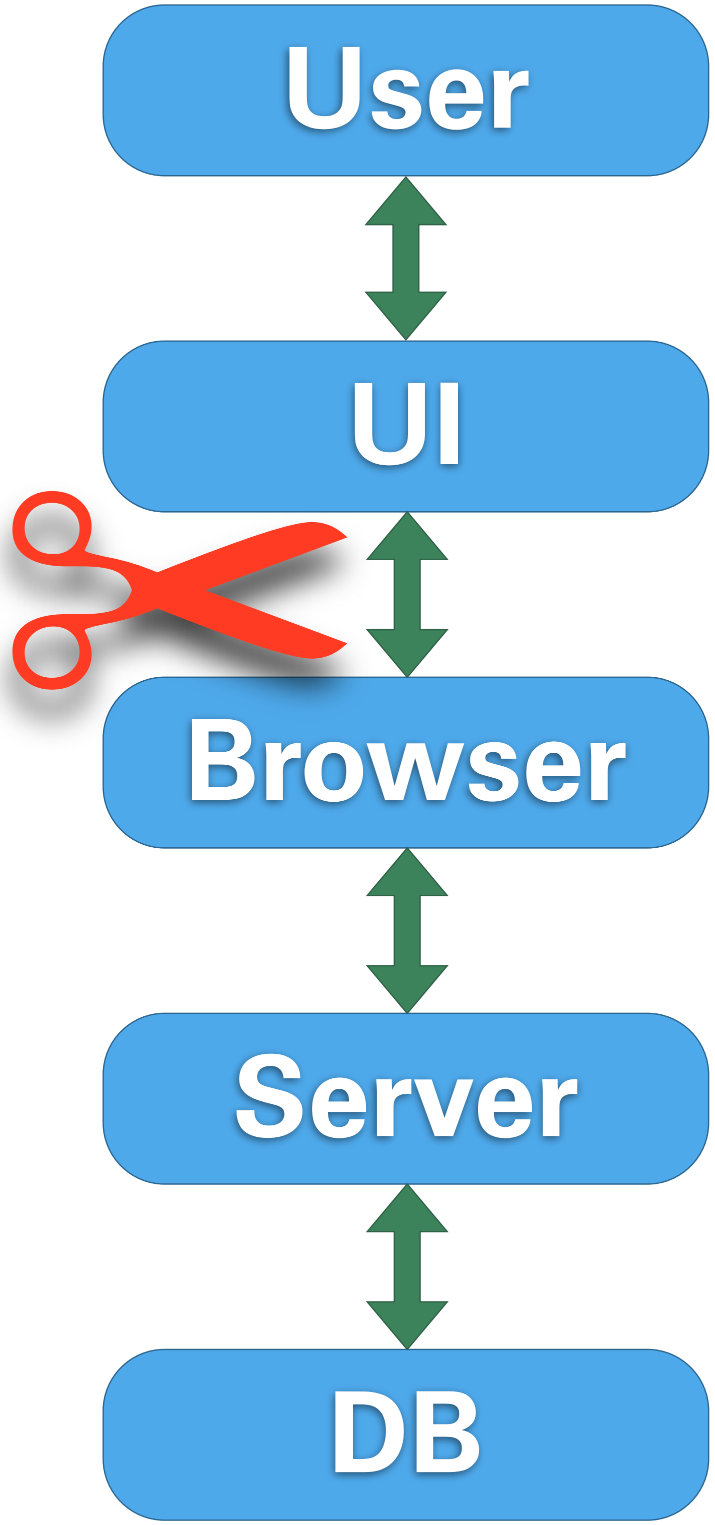
scorecardresearch.com

ixnp.com

fbcdn.net

TECHNISCHE UNIVERSITÄT DRESDEN

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**
- 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>`

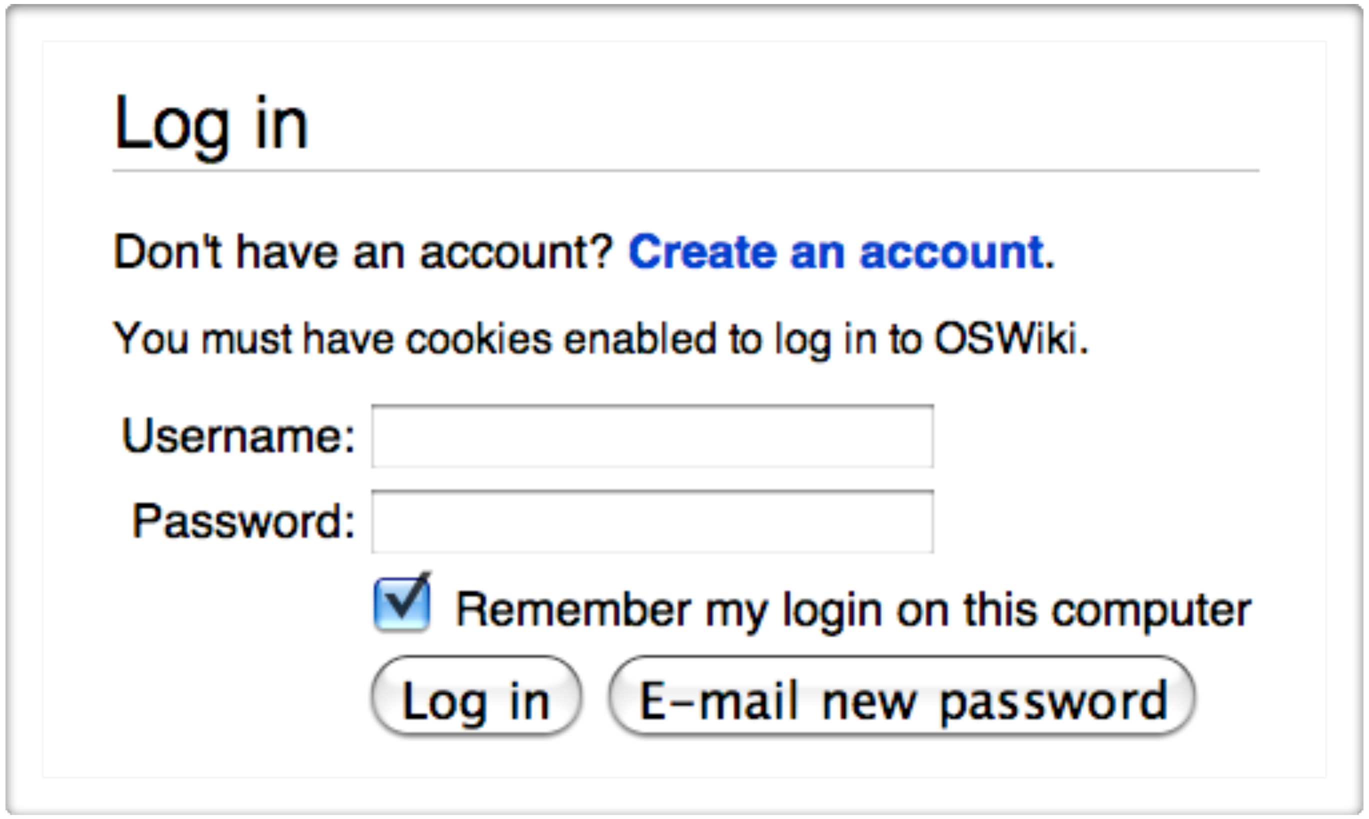
TARGETS

- study in late 2008: high-profile bank websites vulnerable
- 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

OTHERWISE



Log in

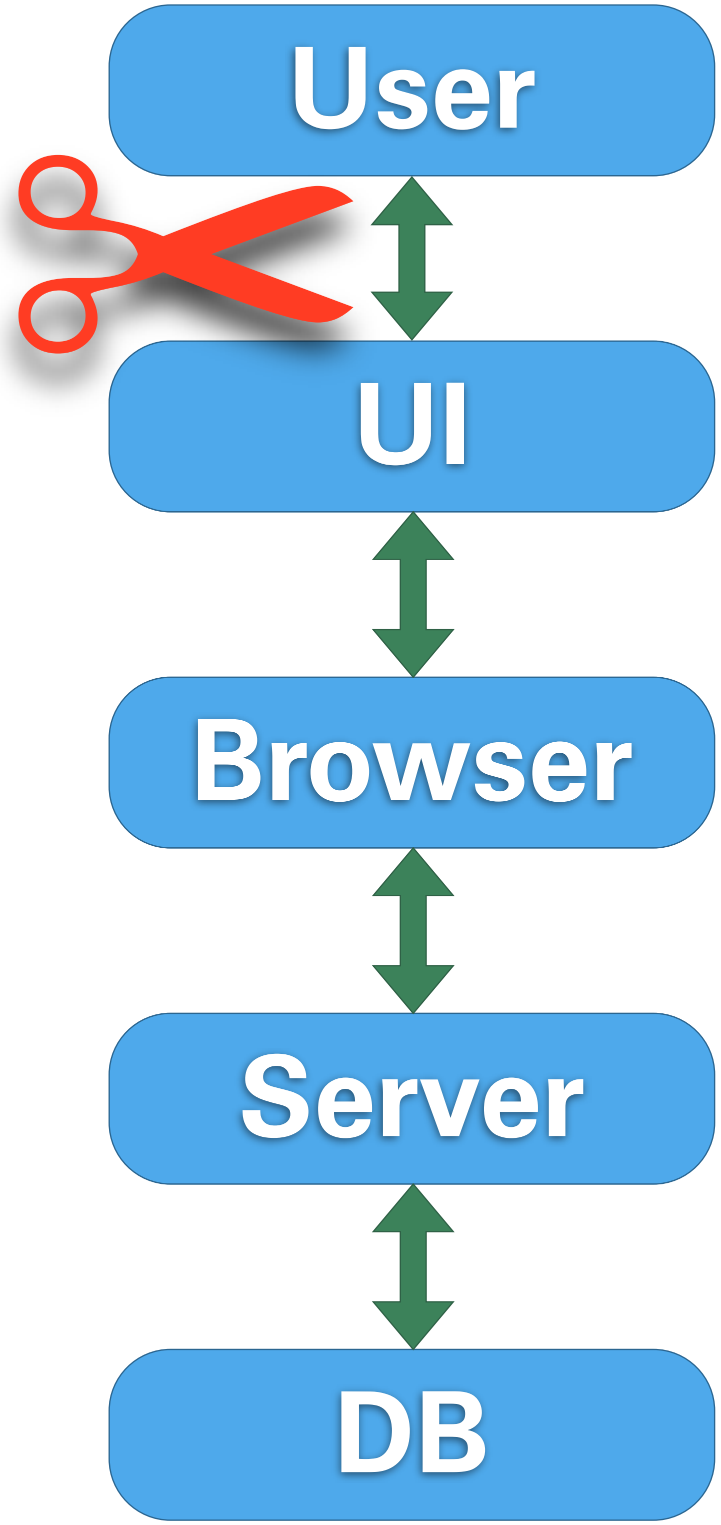
Don't have an account? Create an account.

You must have cookies enabled to log in to OSWiki.

Username:	
Password:	

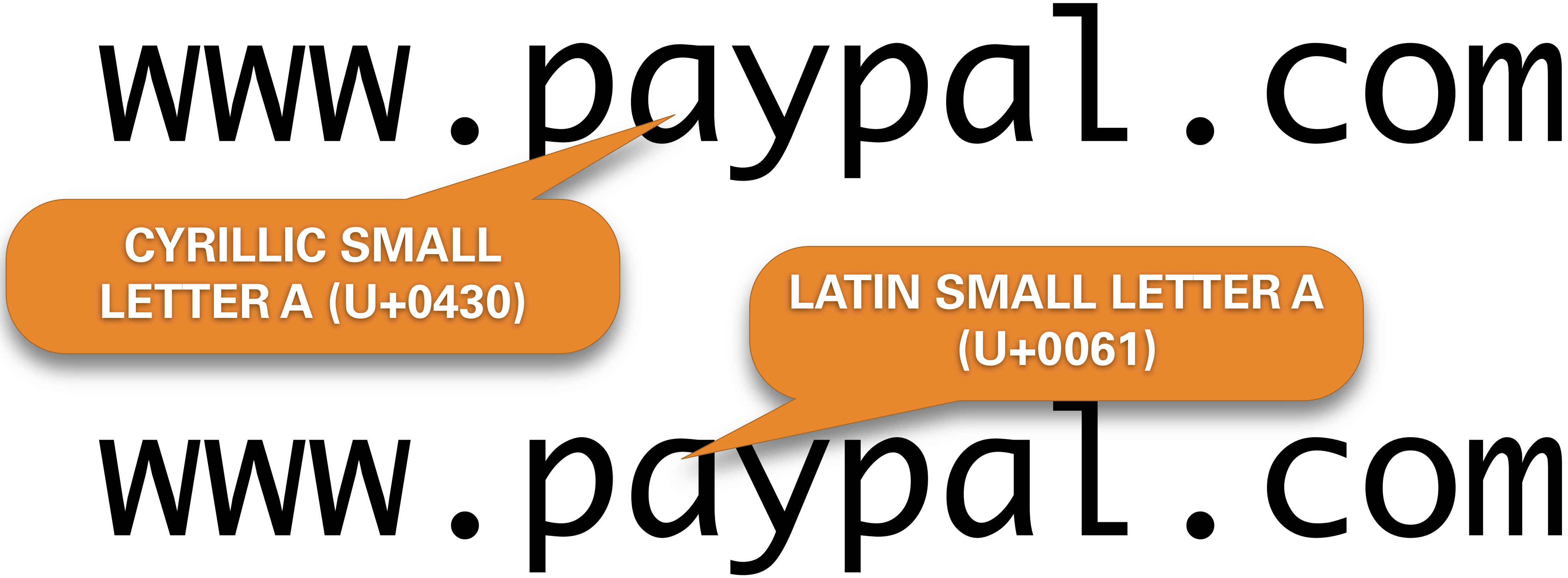
☑ Remember my login on this computer

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.pаypal.com

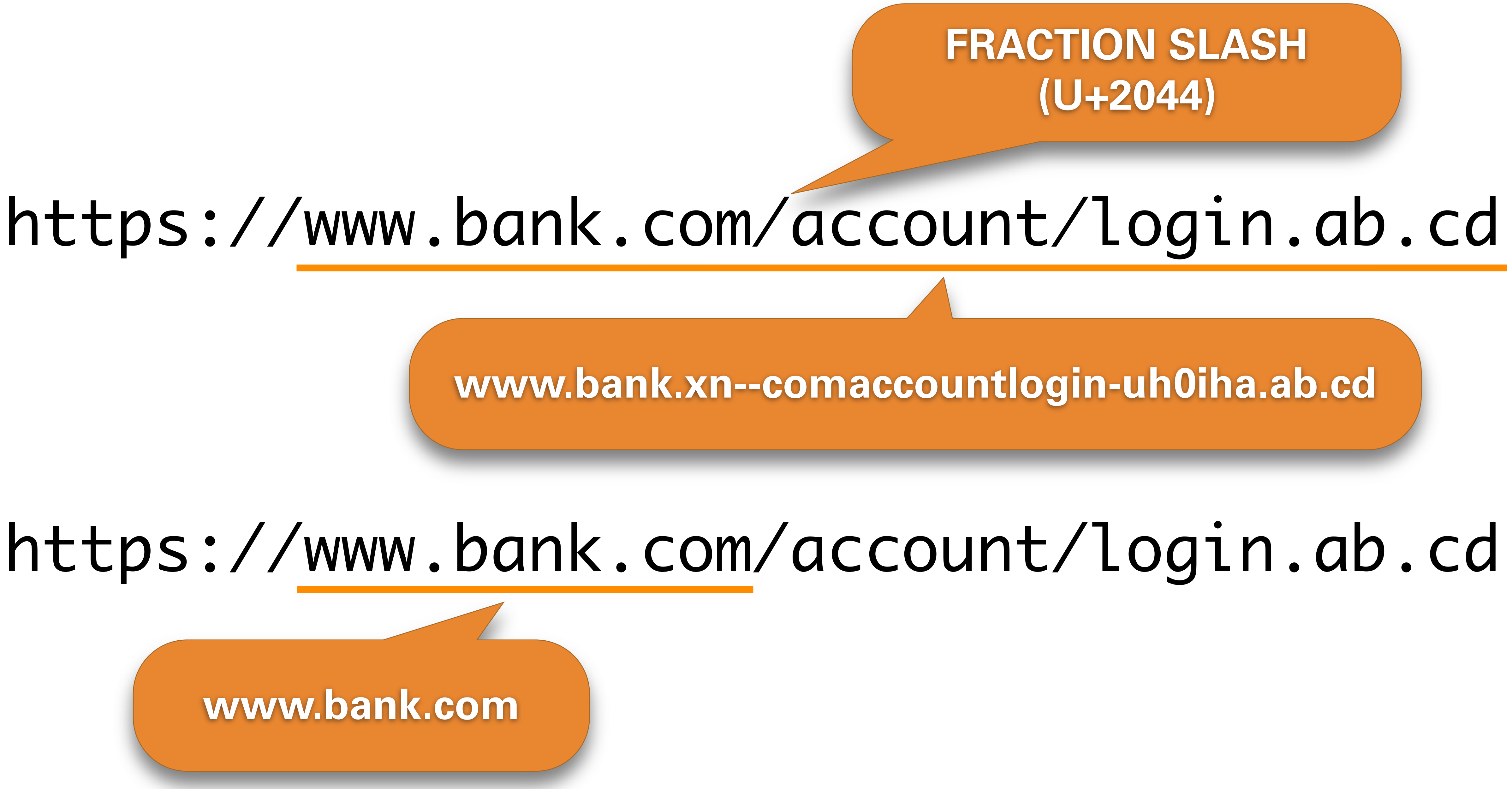
CYRILLIC SMALL LETTER A (U+0430)

LATIN SMALL LETTER A (U+0061)

www.paypal.com

homograph attack

GENERALIZE



FRACTION SLASH (U+2044)

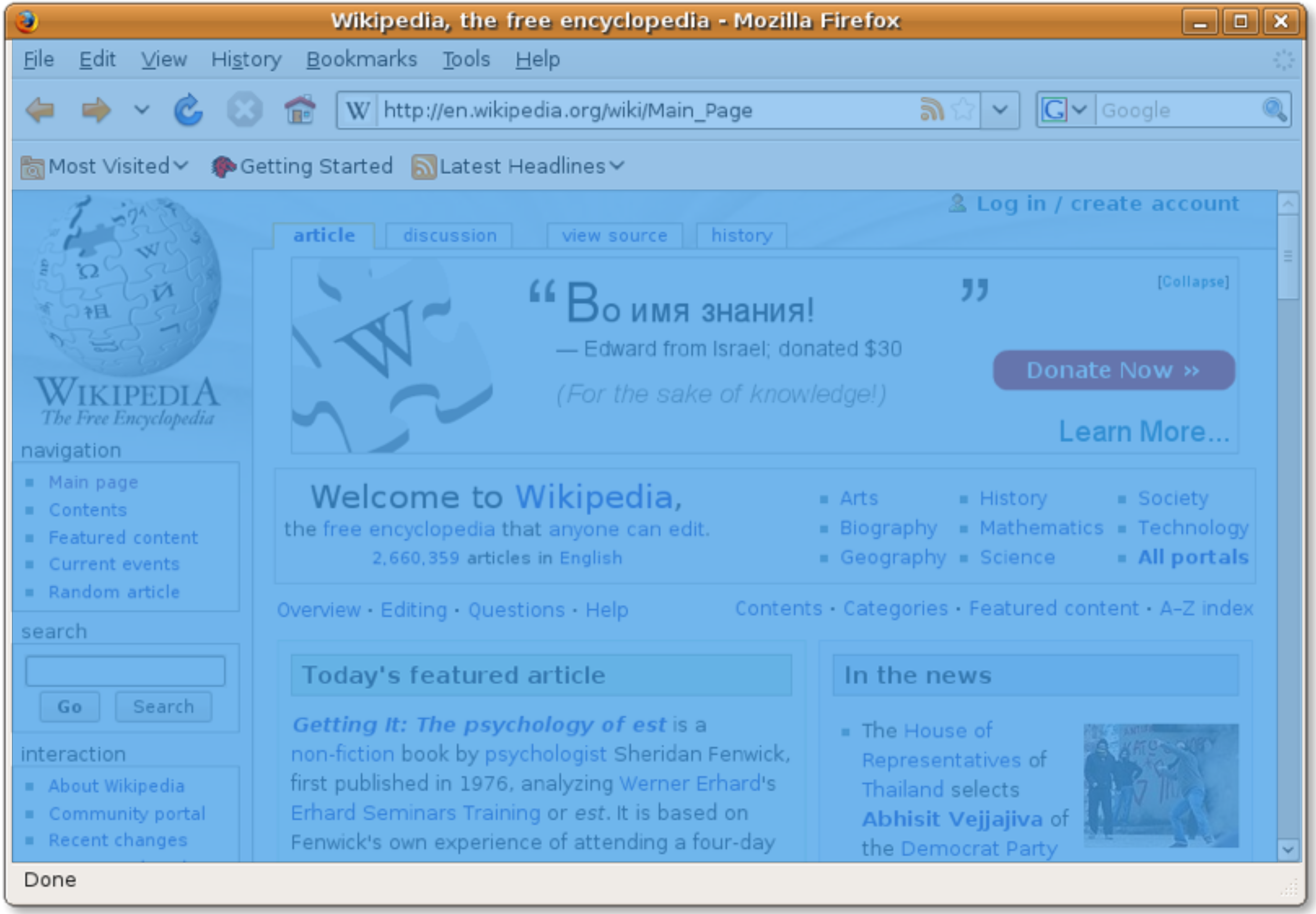
https://www.bank.com⁄account⁄login.ab.cd

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

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

www.bank.com

CONTENT



“ Bo имя знания! ”

— Edward from Israel; donated $30

(For the sake of knowledge!)

Welcome to Wikipedia,

the free encyclopedia that anyone can edit.

2,660,359 articles in English

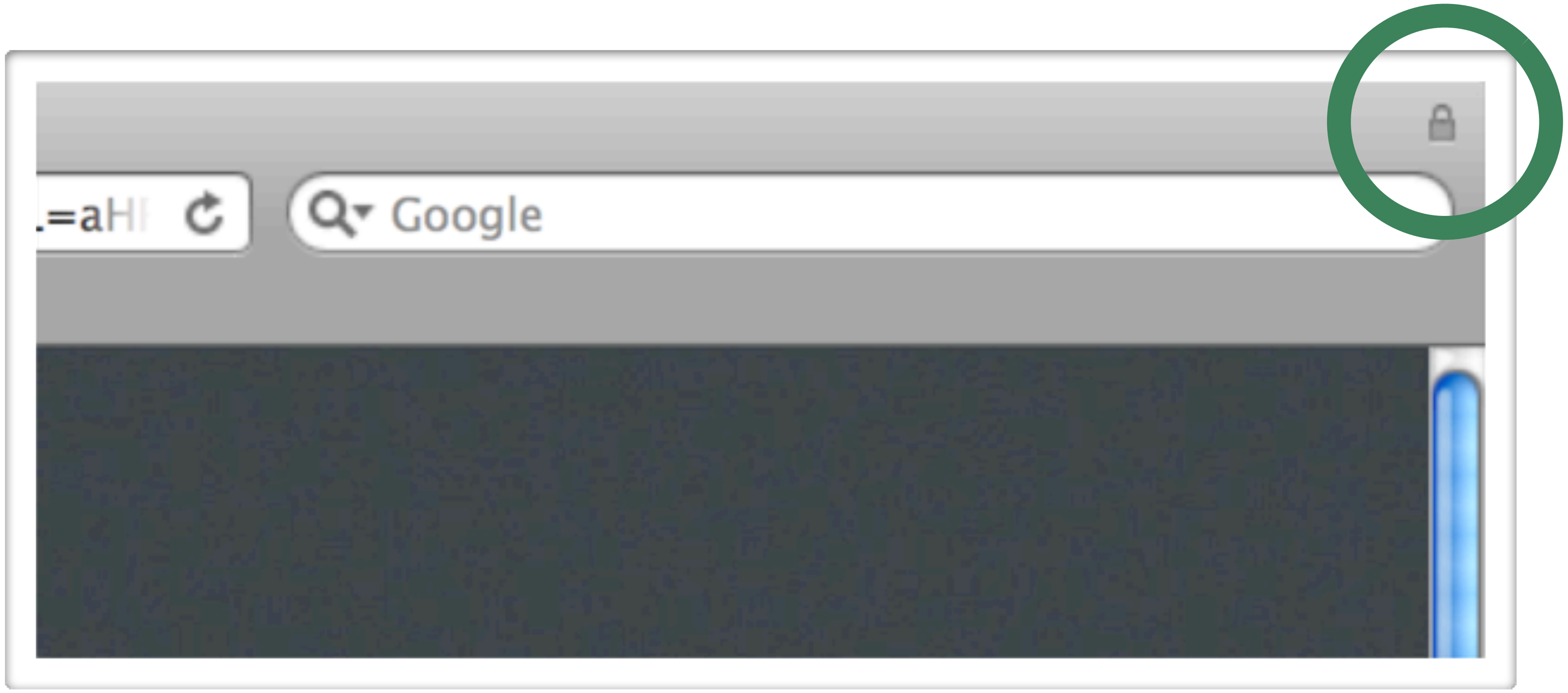
Today's featured article

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

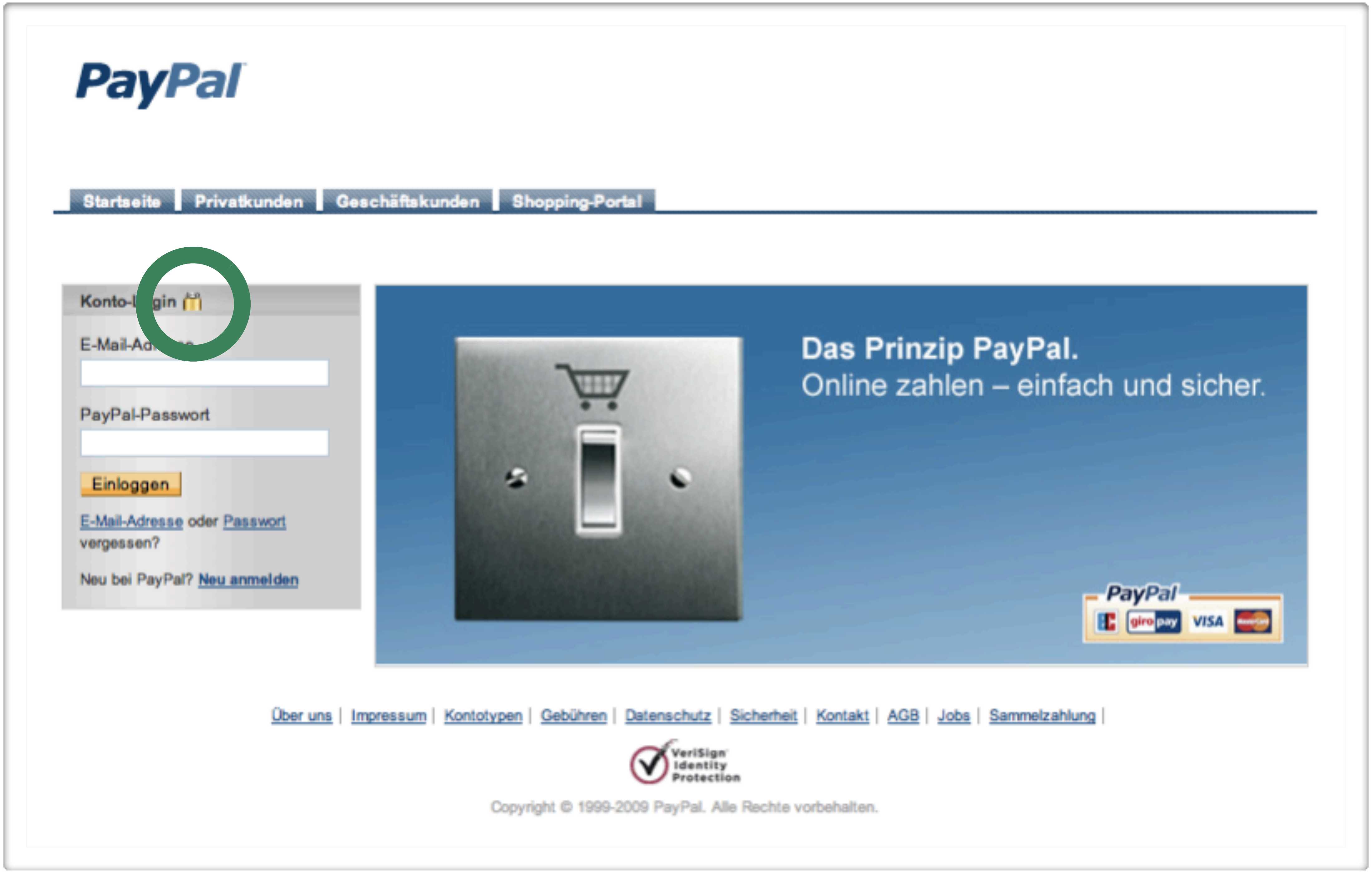
In the news

- The House of Representatives of Thailand selects **Abhisit Vejjajiva** of the Democrat Party

BETTER



PADLOCKS



PayPal

Startseite | Privatkunden | Geschäftskunden | Shopping-Portal

Konto-Login

E-Mail-Adresse

PayPal-Passwort

Einloggen

E-Mail-Adresse oder Passwort vergessen?

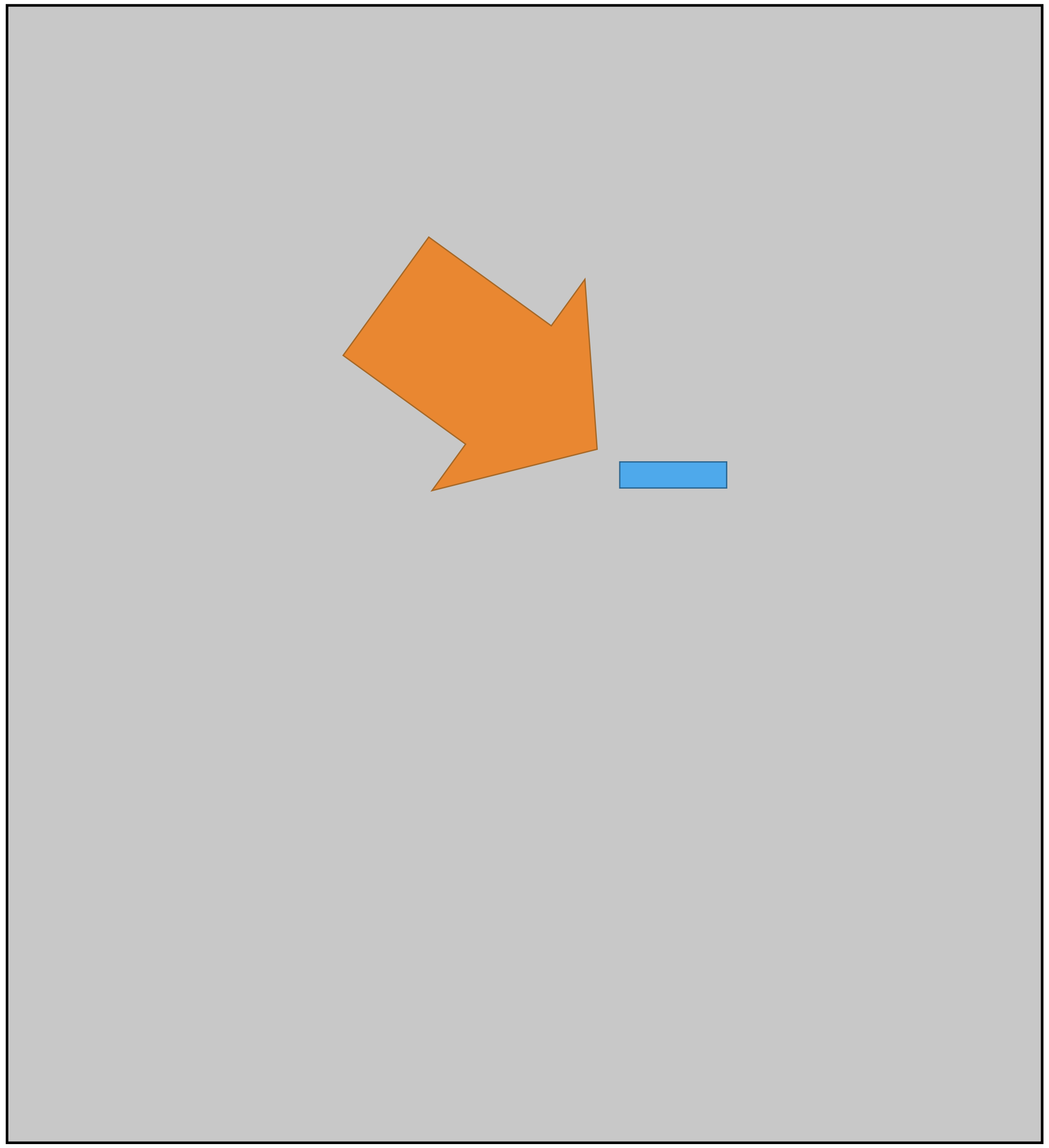
Neu bei PayPal? Neu anmelden

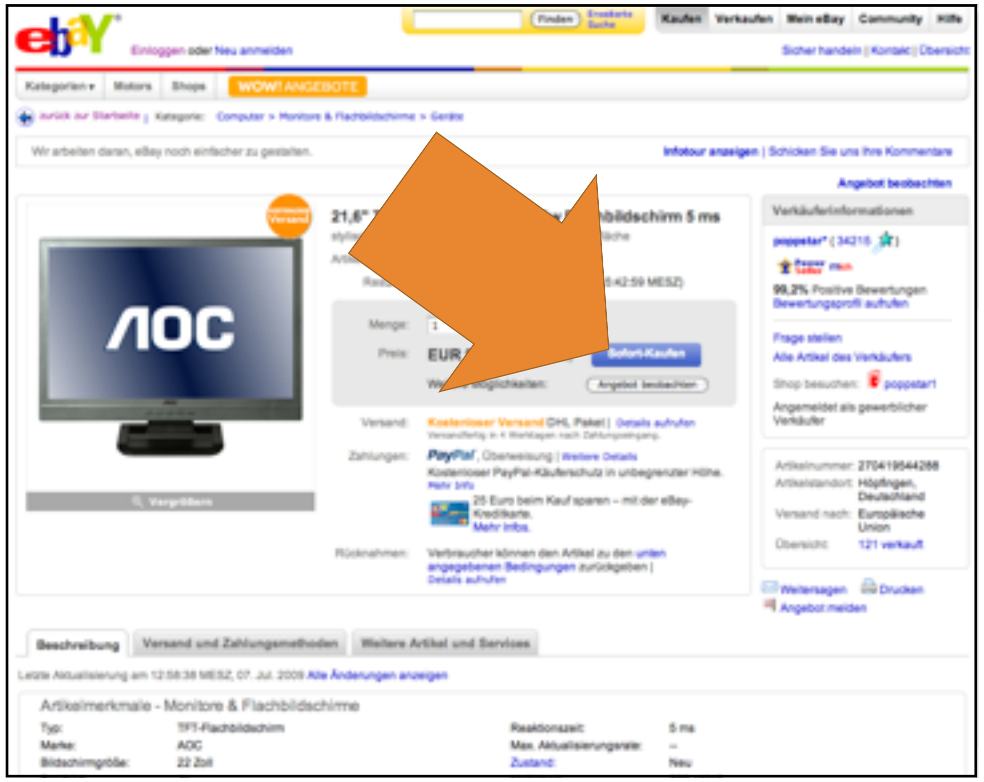
Das Prinzip PayPal.
Online zahlen – einfach und sicher.

Über uns | Impressum | Kontotypen | Gebühren | Datenschutz | Sicherheit | Kontakt | AGB | Jobs | Sammelzahlung |

Copyright © 1999-2009 PayPal. Alle Rechte vorbehalten.

CLICKJACKING




Einloggen oder Neu anmelden
Finden
Erweiterte Suche
Kaufen
Verkaufen
Mein eBay
Community
Hilfe
Sicher handeln | Kontakt | Übersicht
Kategorien ▾
Motors
Shops
WOW! ANGEBOTE
zurück zur Startseite
Kategorie: Computer > Monitore & Flachbildschirme > Geräte
Infotour anzeigen | Schicken Sie uns Ihre Kommentare
Angebot beobachten
Sofort-Kaufen
Angebot beobachten
Vergrößern
Beschreibung
Versand und Zahlungsmethoden
Weitere Artikel und Services
Weitersagen
Drucken
Angebot melden

Wir arbeiten daran, eBay noch einfacher zu gestalten.

21,6" T… …bildschirm 5 ms

…5:42:59 MESZ)

Menge: 1

Preis: EUR …

Versand: Kostenloser Versand DHL Paket | Details aufrufen
Versandfertig in 4 Werktagen nach Zahlungseingang.

Zahlungen: PayPal, Überweisung | Weitere Details
Kostenloser PayPal-Käuferschutz in unbegrenzter Höhe.
Mehr Info
25 Euro beim Kauf sparen – mit der eBay-Kreditkarte.
Mehr Infos.

Rücknahmen: Verbraucher können den Artikel zu den unten angegebenen Bedingungen zurückgeben | Details aufrufen

Verkäuferinformationen
poppstar* (34215)
99,2% Positive Bewertungen
Bewertungsprofil aufrufen
Frage stellen
Alle Artikel des Verkäufers
Shop besuchen: poppstar1
Angemeldet als gewerblicher Verkäufer

Artikelnummer:	270419544288
Artikelstandort:	Höpfingen, Deutschland
Versand nach:	Europäische Union
Übersicht:	121 verkauft

Letzte Aktualisierung am 12:58:38 MESZ, 07. Jul. 2009 Alle Änderungen anzeigen

Artikelmerkmale - Monitore & Flachbildschirme

Typ:	TFT-Flachbildschirm	Reaktionszeit:	5 ms
Marke:	AOC	Max. Aktualisierungsrate:	--
Bildschirmgröße:	22 Zoll	Zustand:	Neu

FIX

- 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

SUMMARY

Is everything lost?

Yes