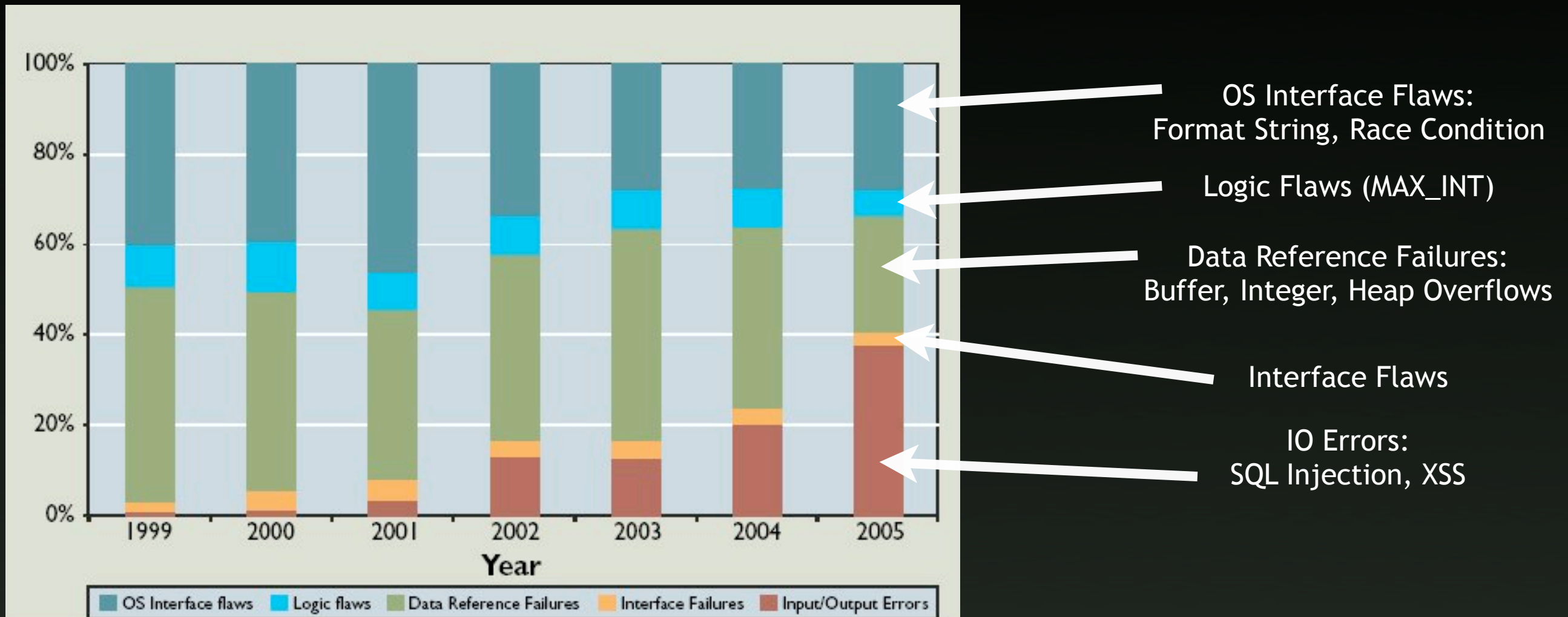


Grundlagen der Web-Sicherheit

- ➡ Das Labor e.V. — 29.05.2008
- © Johannes Dahse, Felix Gröbert
- 📞 johannesdahse@gmx.de, felix@groeibert.org
- ✂ creativecommons.org/licenses/by-nc-nd/2.0/de

pwn pwn pwn ...

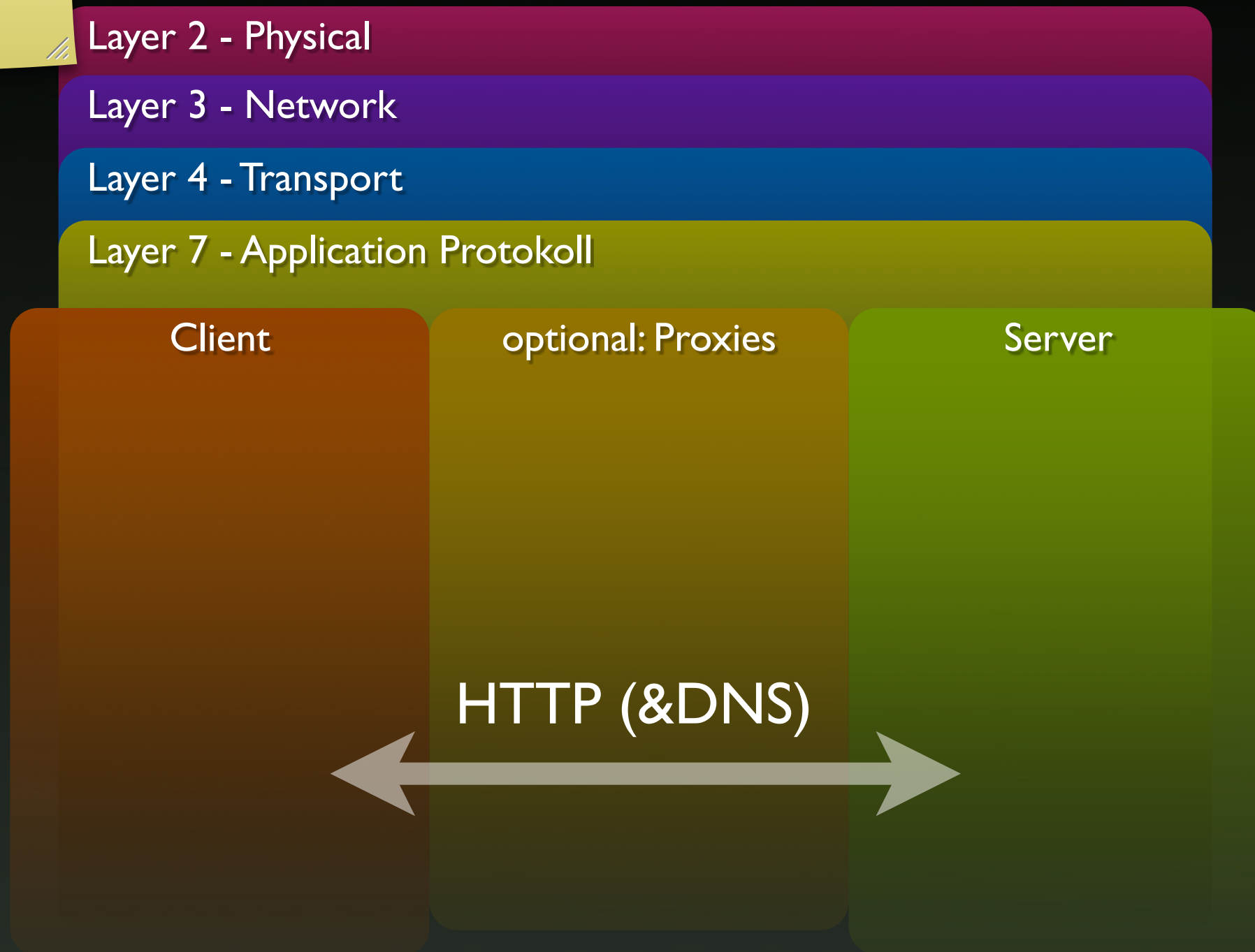


Quelle: "Software Security is Software Reliability", Felix Lindner, CACM 49/6

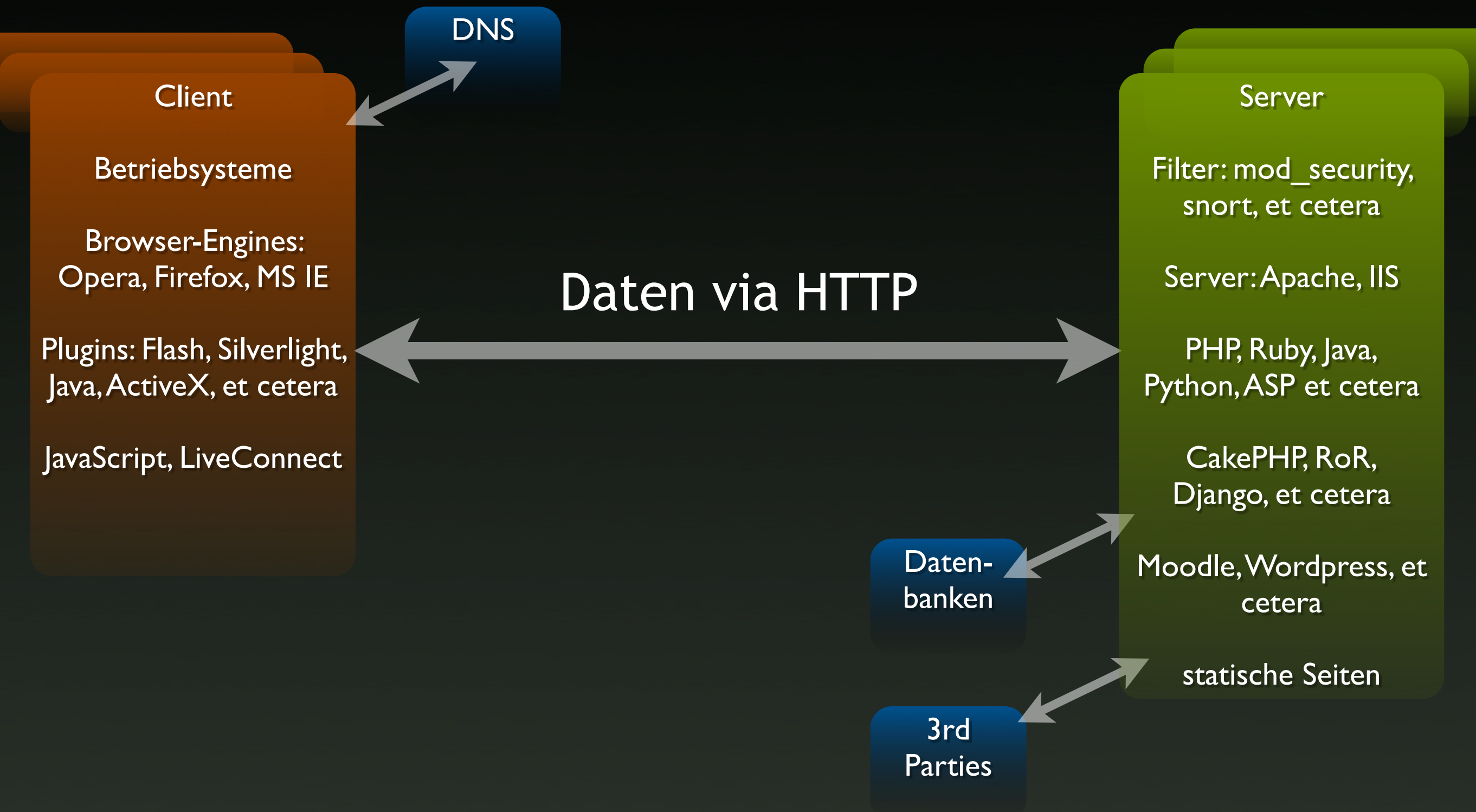
Proxies:

mod_security
snort
SSL
Privoxy

Orientierung



Orientierung



://

iis:
2006 : 1
seh protection
apache:
eben wenig
in komponenten:
mod_rewrite bo
openssl bo

- Hyper Text Transfer Protocol (HTTP)
- 1989 Berners-Lee @ CERN, inkl HTML und URL
- Zustandslos: Anwendung implementiert Session
- HTTPd: IIS 35% Apache 50%* (kaum Security Bugs)

GET /TEXT.html HTTP/1.1
Host: www.example.net
UserAgent: MS IE
Referer: http://seclog.de

HTTP/1.1 200 OK
Server: Apache/1.3.29 (Unix) PHP/4.3.4
Content-Length: (Größe TEXT.html)
Content-Language: de
Content-Type: text/html
Connection: close

(Inhalt TEXT.html)

* Quelle: netcraft

turn it off.

- JavaScript (JS): objektbasierte Sprache für dynamisches HTML
- `<body onload="document.write(document.cookie); window.print()">`
- Same Origin Policy (SOP)
- Local-Zone Scripting
- Ausführen von JS durch Angreifer = volle Kontrolle über Browser im Kontext der SOP

HTTP ist Sitzungslos

lol, schau dir mal den link an...

- Cross Site Scripting (XSS)

- ❖ >20% der Mitre CVE = XSS
- ❖ Jede große Seite betroffen, unter anderem ~40 deutsche Banken
- ❖ Whitehat Security 7/10 Seiten betroffen
- ❖ Effektiv auf SN Sites und in Kombination mit Phishing / Social Engineering
- ❖ Session Fixation / Hijacking




demo: XSS

File Bearbeiten Ansicht Chronik Lesezeichen ScrapBook Extras Hilfe Stumble! I like it!

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

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

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.



CDU

Suchen...

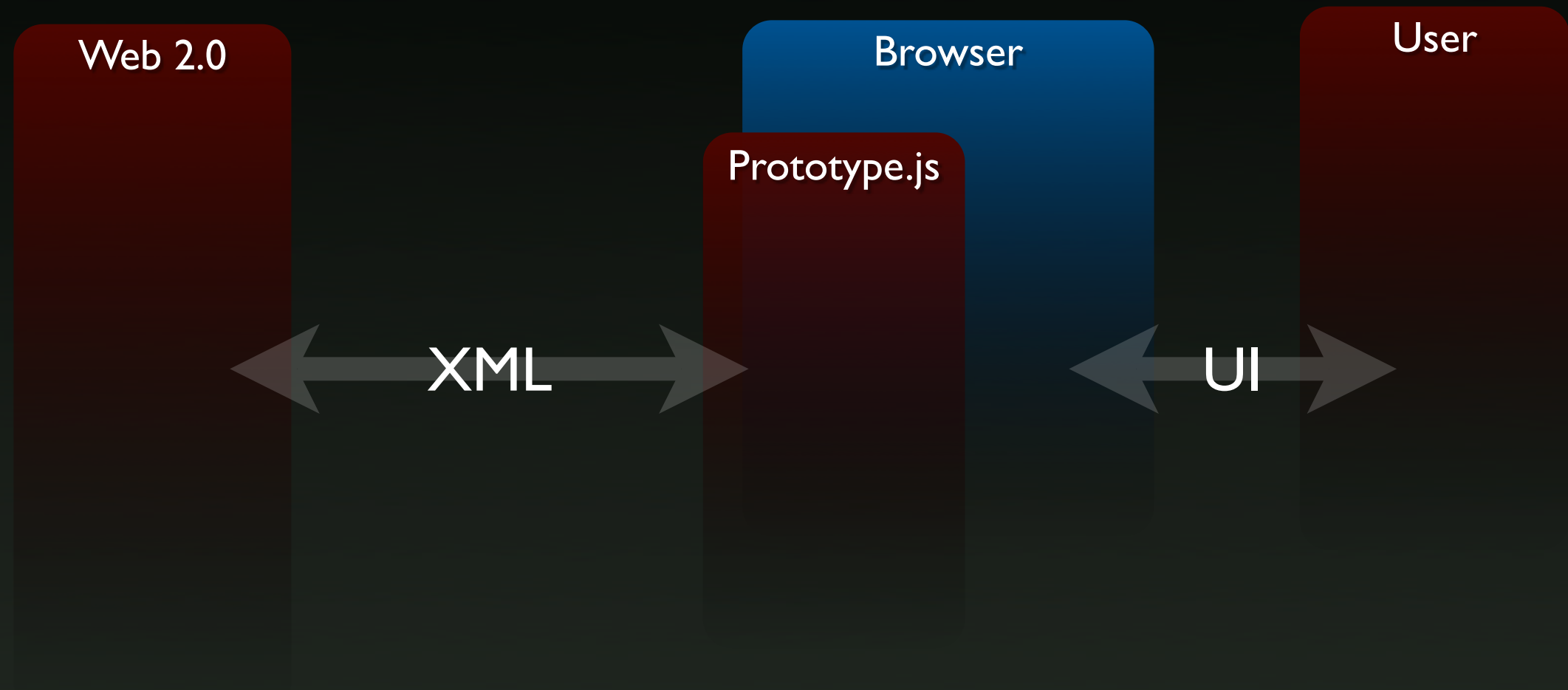
Position

Verfassungsschutzbericht →

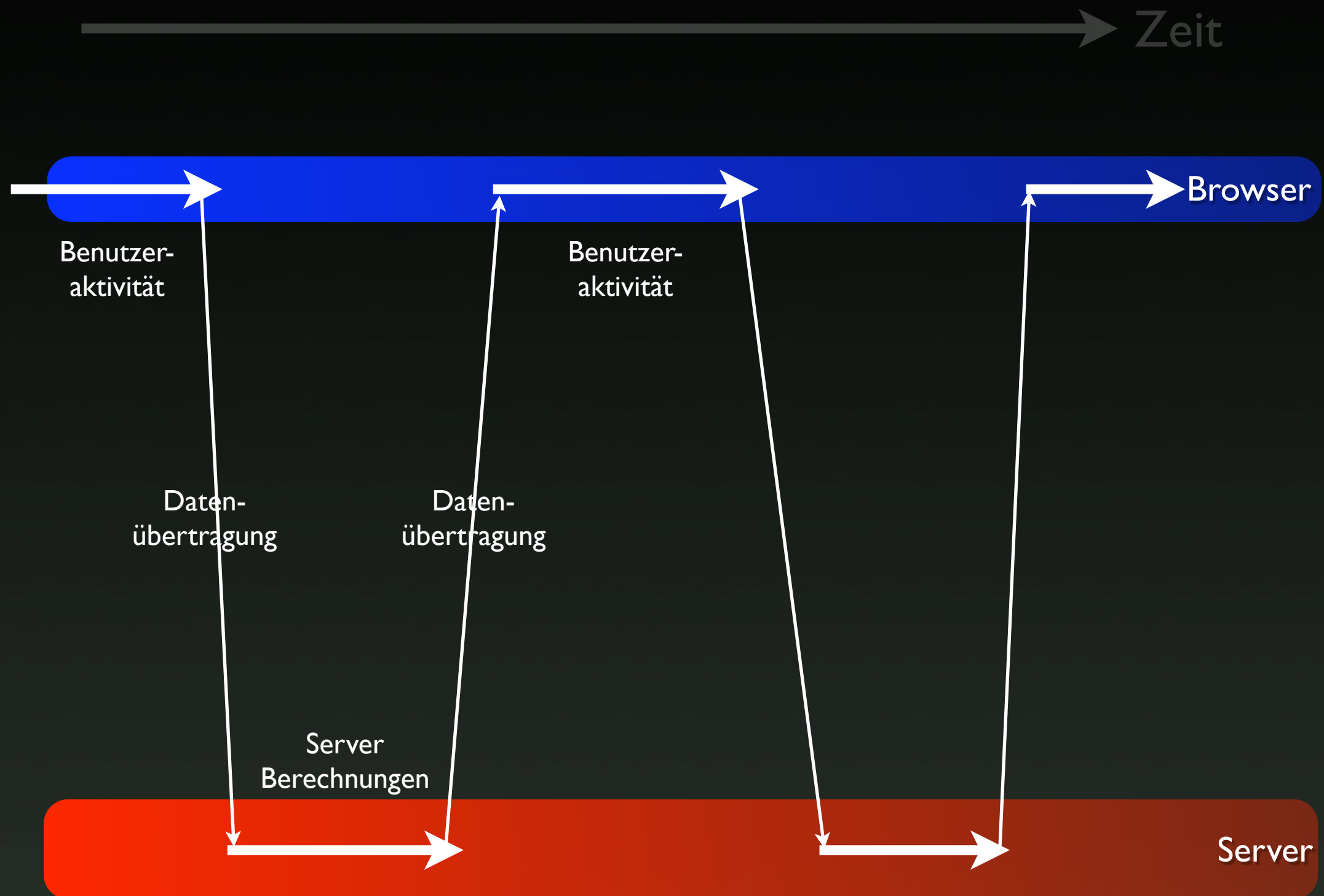
BKA-Gesetz →

Fertig

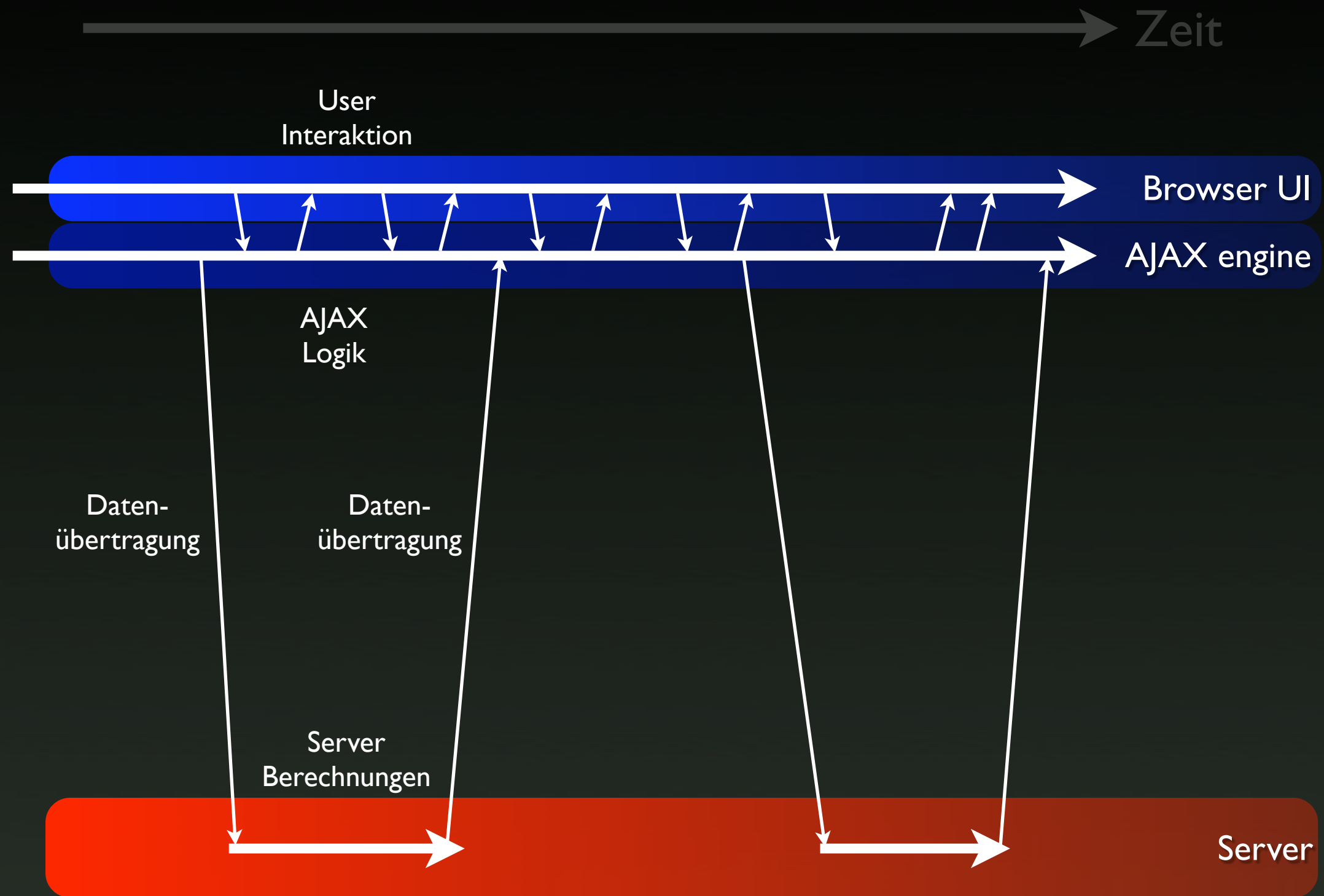
AJAX



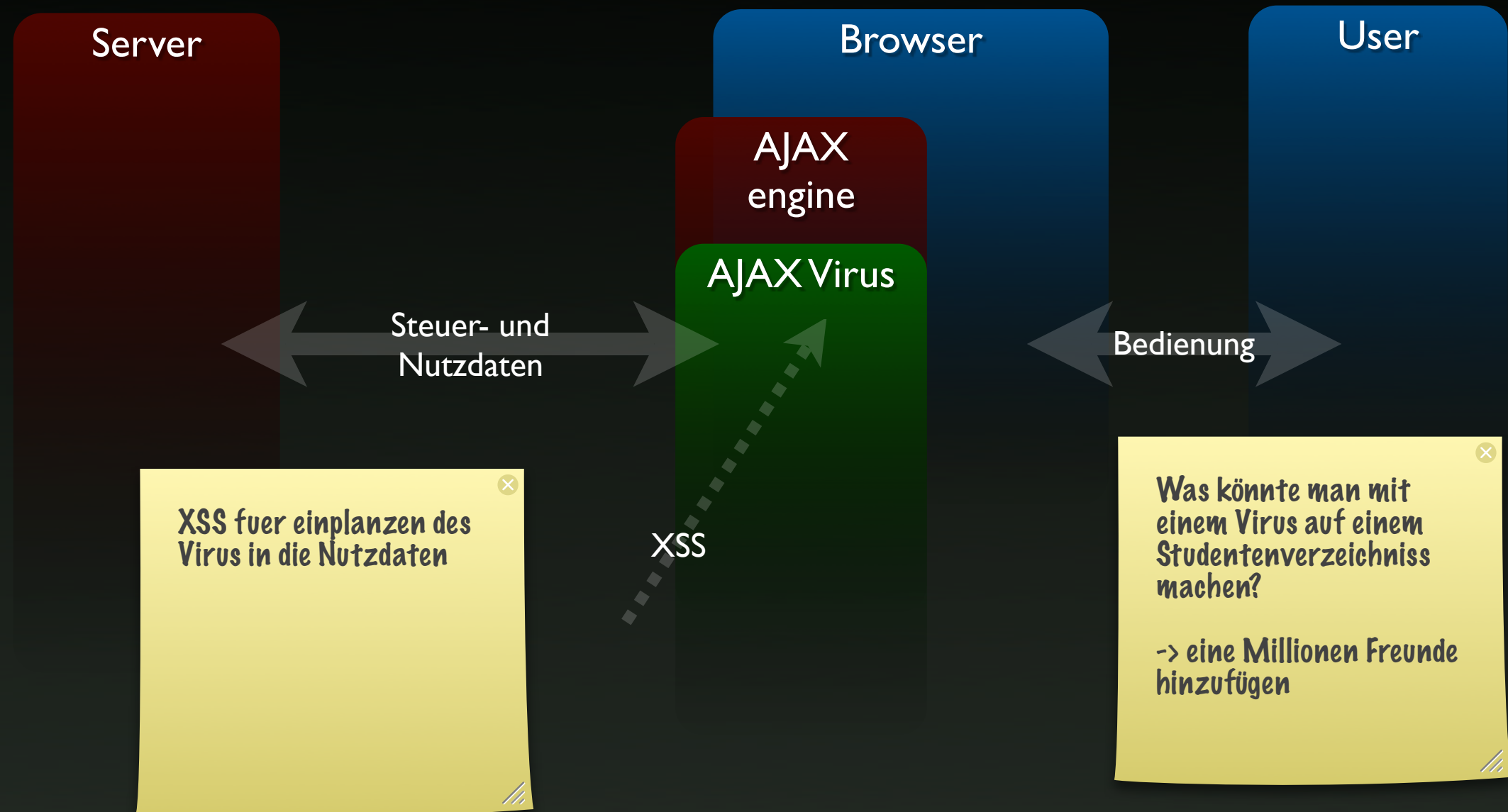
Web 1.0



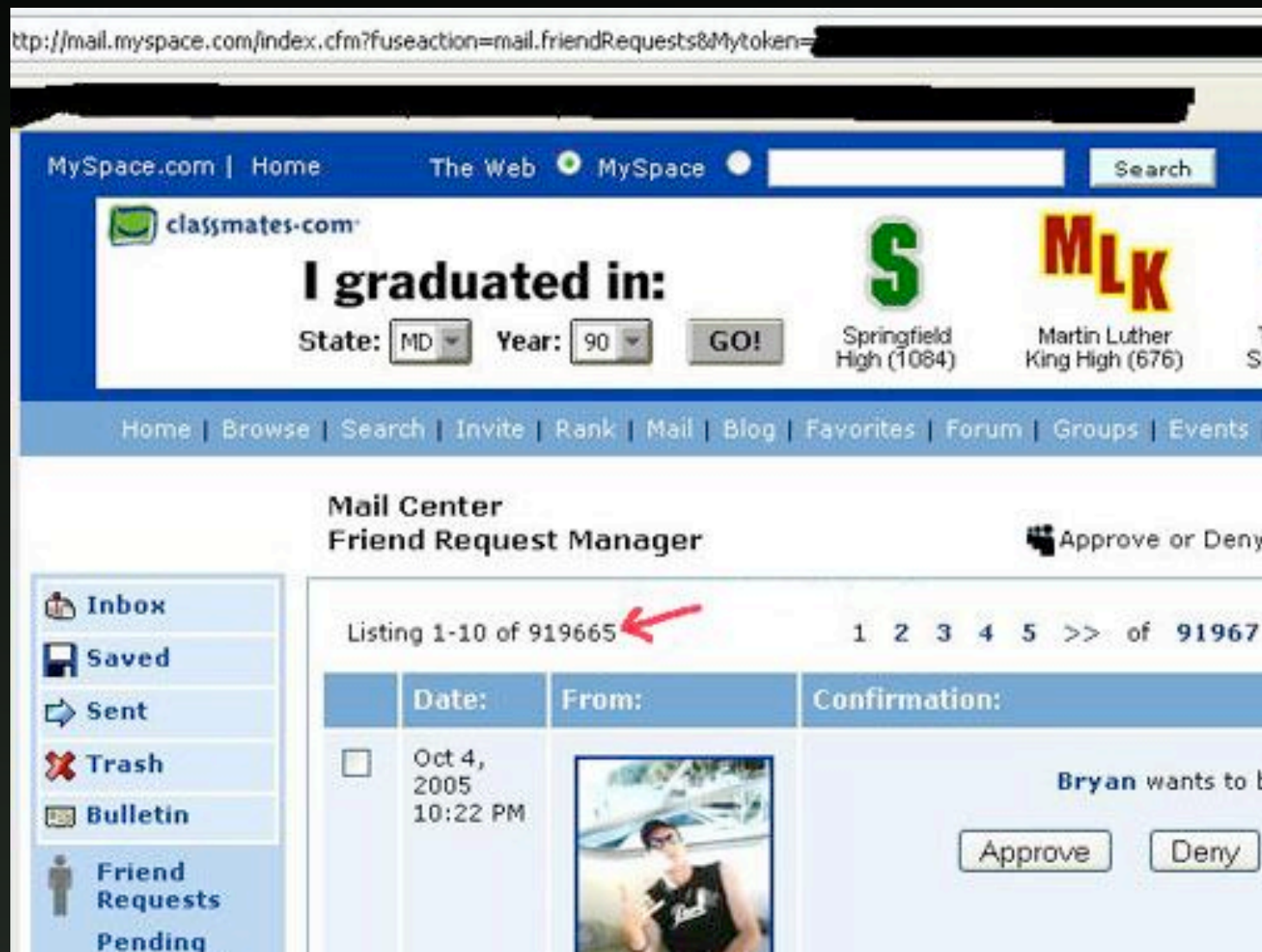
Web 2.0



AJAX VX



i want to be your friend



Virus erzeugte 1
Millionen Freunde in 24h

damit ist Samy der
schnellst verbreitende
Virus der Geschichte

MySpace.com

wer routet so spät durch Nacht und Wind?

- Mexico XSRF Router DNS Poison Incident
- `http://home/xslt?PAGE=J38_SET&THISPAGE=J38&NEXTPAGE=J38_SET&NAME=www.prueba.hkm&ADDR=216.163.137.3`
- “It does not validate POST, or Referer or Anything...” -- hkm (at) hakim (dot) ws

demo: XSRF

A or A

- Logic Flaws
 - ❖ `unister.de/einladung_12345.html`
 - ↳ Einladung für User mit E-Mail und Namen
 - ❖ asmallworld Social Network (SN)
 - ↳ Iteration über Namen wie oben
 - ❖ `<input name=price value="299.99 EUR" type=hidden>`

Interface Flaws

- `example.com/?user=foo&pass=bar`
→ error: unknown user
aber:
`example.com/?user=felix&pass=123456`
→ error: wrong password

demo: rfi

it's a feature, not a bug

- remote file inclusion (rfi) / local file inclusion (lfi):
 - ❖ allow_url_fopen = 0 (rfi)
 - ❖ nullbyte nur mgl. mit magic_quotes_gpc = 0
- example.com/?file=../../../../../../../../var/db/locatedb
- Mass Exploits via Google Dorking

Hello DB! Hello Mr DROPTABLE!

- IO Error: SQL Injection (SQLi)
 - ❖ Benutzereingaben werden ungeprüft an SQL Datenbank weiter gereicht
 - ❖ Benutzereingaben enthalten SQL Befehle
→ Kompromittierung des Servers
 - ❖ Problem des In-Band-Signalling (à la 2600 Hz)
→ Trennung Kontroll-Befehle und Daten

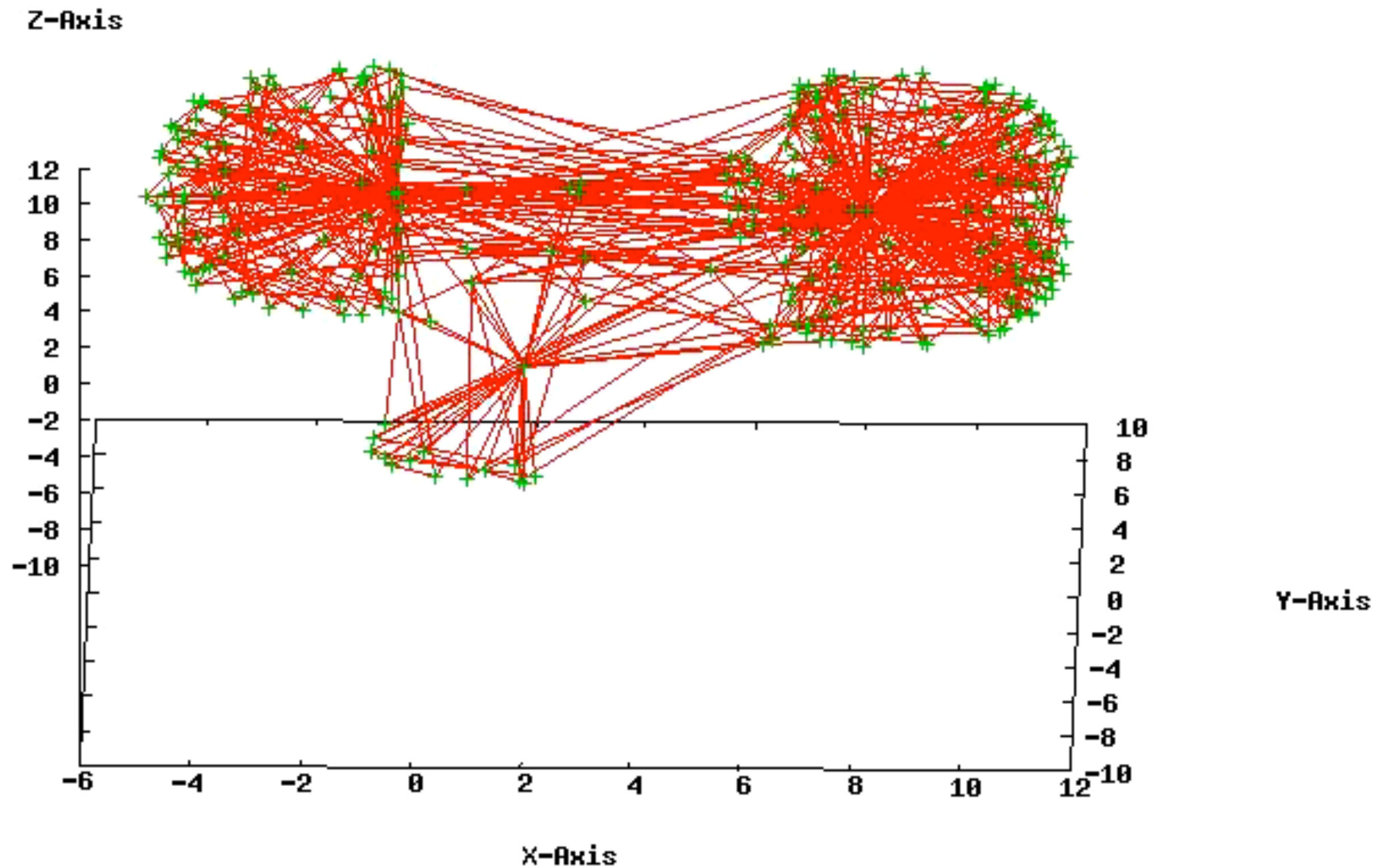
demo: SQLi

Ausblick

- HTTP Response Splitting
- Web Exploit Toolkits
- DNS Rebinding
- XSRF Worms
- Client & Server Worms (auto-SQLi-iframe)

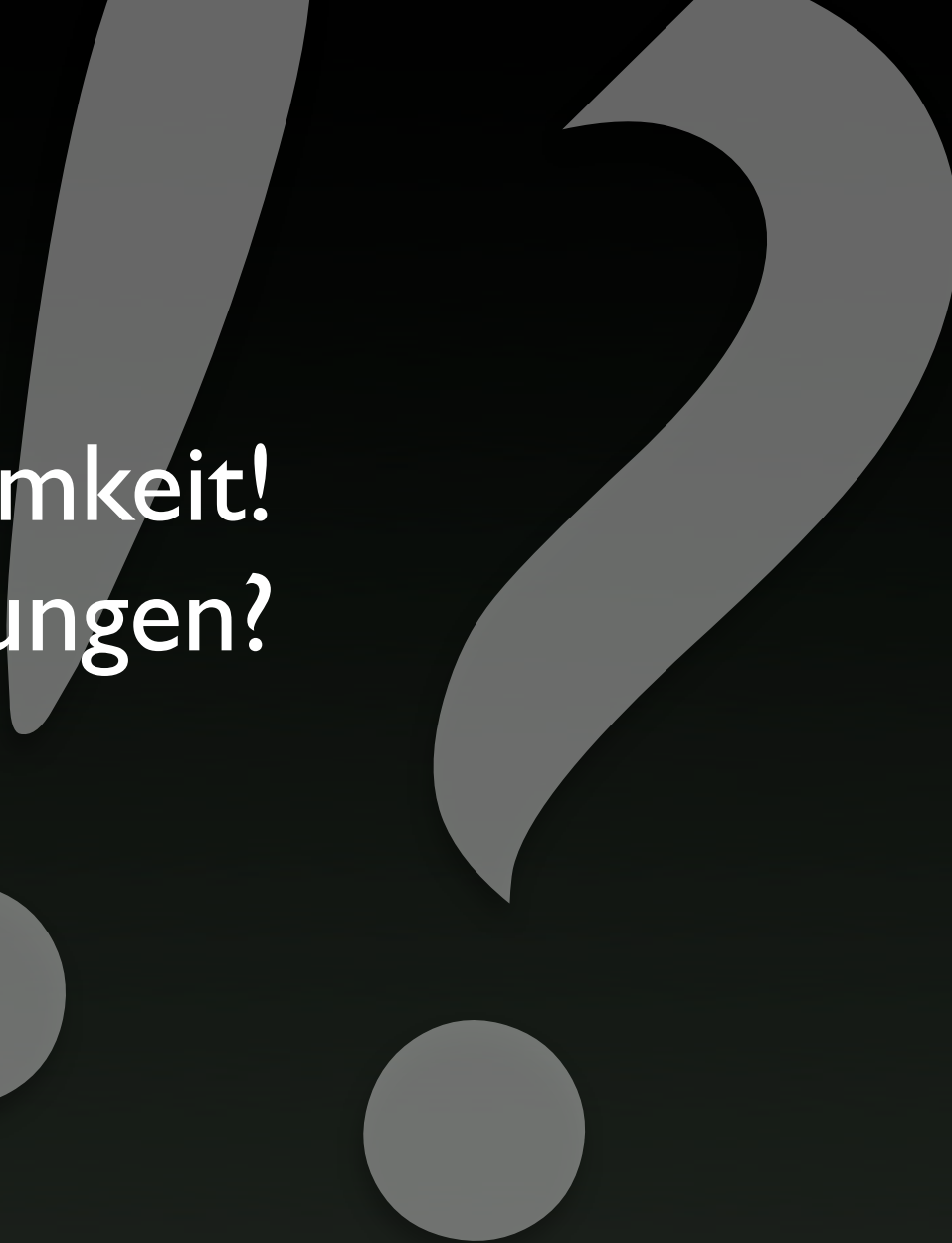
cycle 1=3

Graphenbeispiel



Fazit

- Sichere Programmierung & Frameworks
- Web 2.0 Hebel
- Datamining: Datenschutz und Nutzer-Sensibilisierung wichtig wie nie zuvor
- PHP-ids.org / OWASP.org



Vielen Dank für Eure Aufmerksamkeit!
Fragen oder Anmerkungen?

- ➡ Das Labor e.V. — 29.05.2008
- © Johannes Dahse, Felix Gröbert
- ☎ johannesdahse@gmx.de, felix@groeibert.org
- ✂ creativecommons.org/licenses/by-nc-nd/2.0/de

Werbung!

- CIPHER IV, 01.08.2008
- <http://www.cipher-ctf.org>
- RUB-CTF@gmx.de

