Web-Applications under attack

Stefan Strobel
CEO cirosec GmbH

cirosec

Agenda

- Introduction
- The threats
- Security testing
- Prevention
- Summary

cirosec

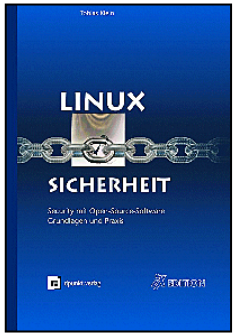
Who is cirosec

- A small company focused on IT Security
  - Founded 2002 by a team that has been working together in IT Security for over 13 years
  - Primarily consulting
    - Audits, penetration tests, risk analysis, training, projects
  - Product resale in niches
    - Innovative topics instead of firewalls
- Our main asset is knowledge and experience
  - Known experts, speakers and authors

cirosec

Books published by cirosec employees

- Klein:
  Buffer Overflows und Format-String-Schwachstellen
  dpunkt Verlag
- Strobel: Firewalls
  dpunkt Verlag
- Klein: Linux Sicherheit
  dpunkt Verlag
- Gundel: Firewalls im Unternehmenseinsatz
  dpunkt Verlag
- Middendorf, Singer:
  Java Programmierhandbuch und Referenz, dpunkt Verlag



Recent publications

- Most frequently iX and ct, but also Computerzeitung, Computerwoche, IT-Sicherheit, Informationweek …
- Past articles in iX e.g.
  - Data Loss Prevention
  - WAFs, application scanners
  - Many conference reviews
  - Security Information Management
  - Measures and metrics in IT security
  - Source code analysis
  - Memory analysis in Incident Response

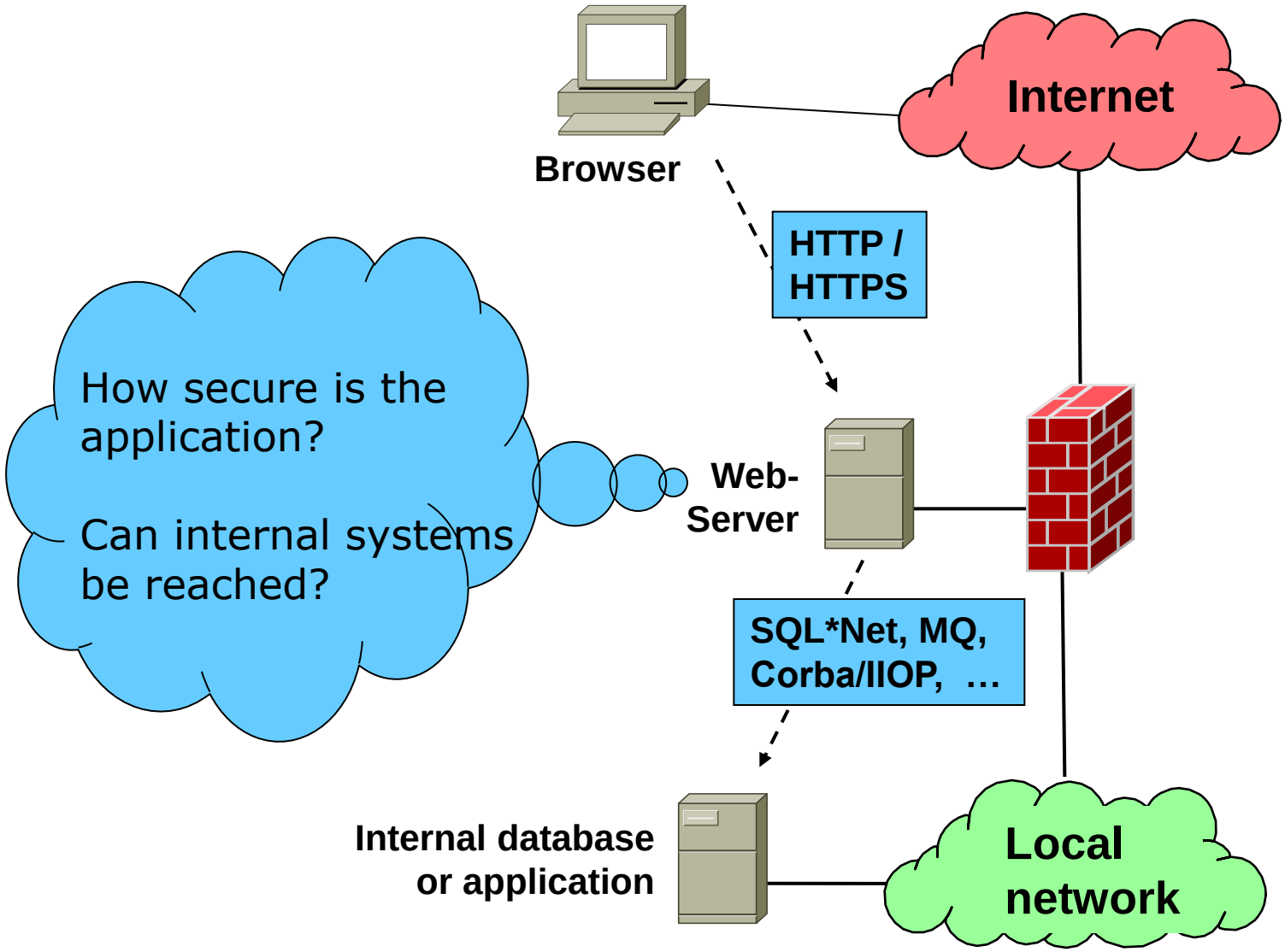
cirosec

speaking engagements

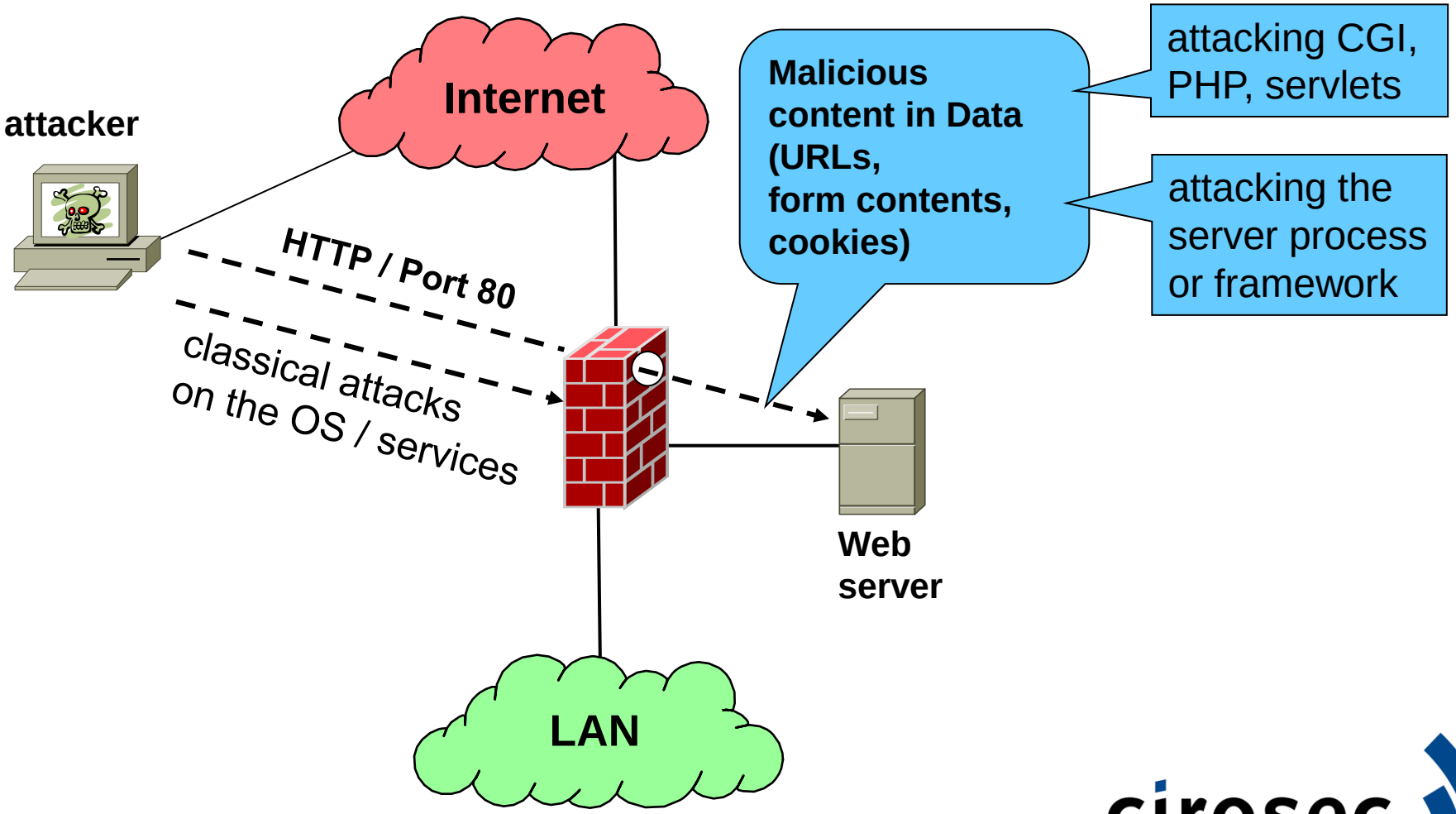
- At more than 20 conferences / events in the last 12 months
  - currently at HITB
- Lecturers at different universities in our area
- cirosec's own conference "IT-Defense"

cirosec

Abstract structure of the problem

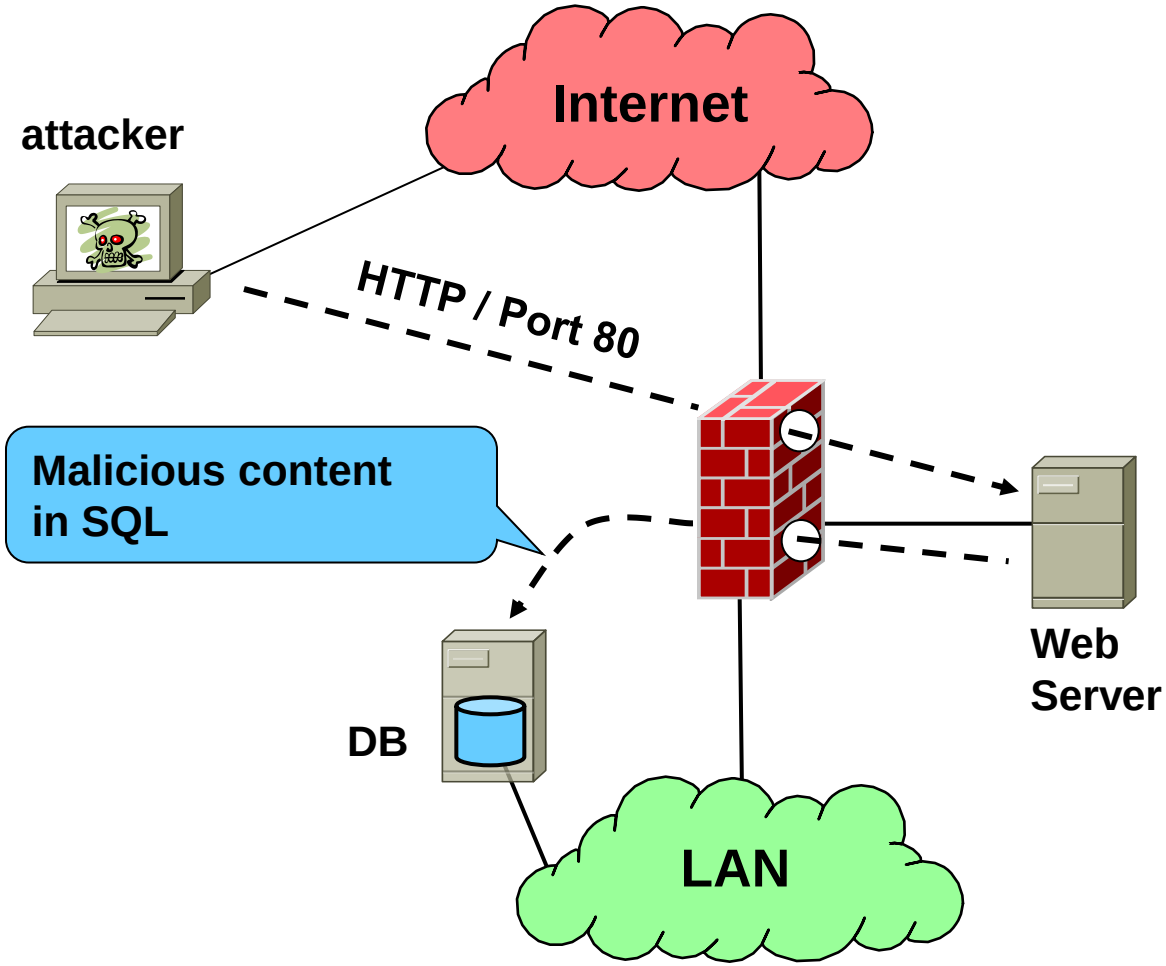


Attacking the web server



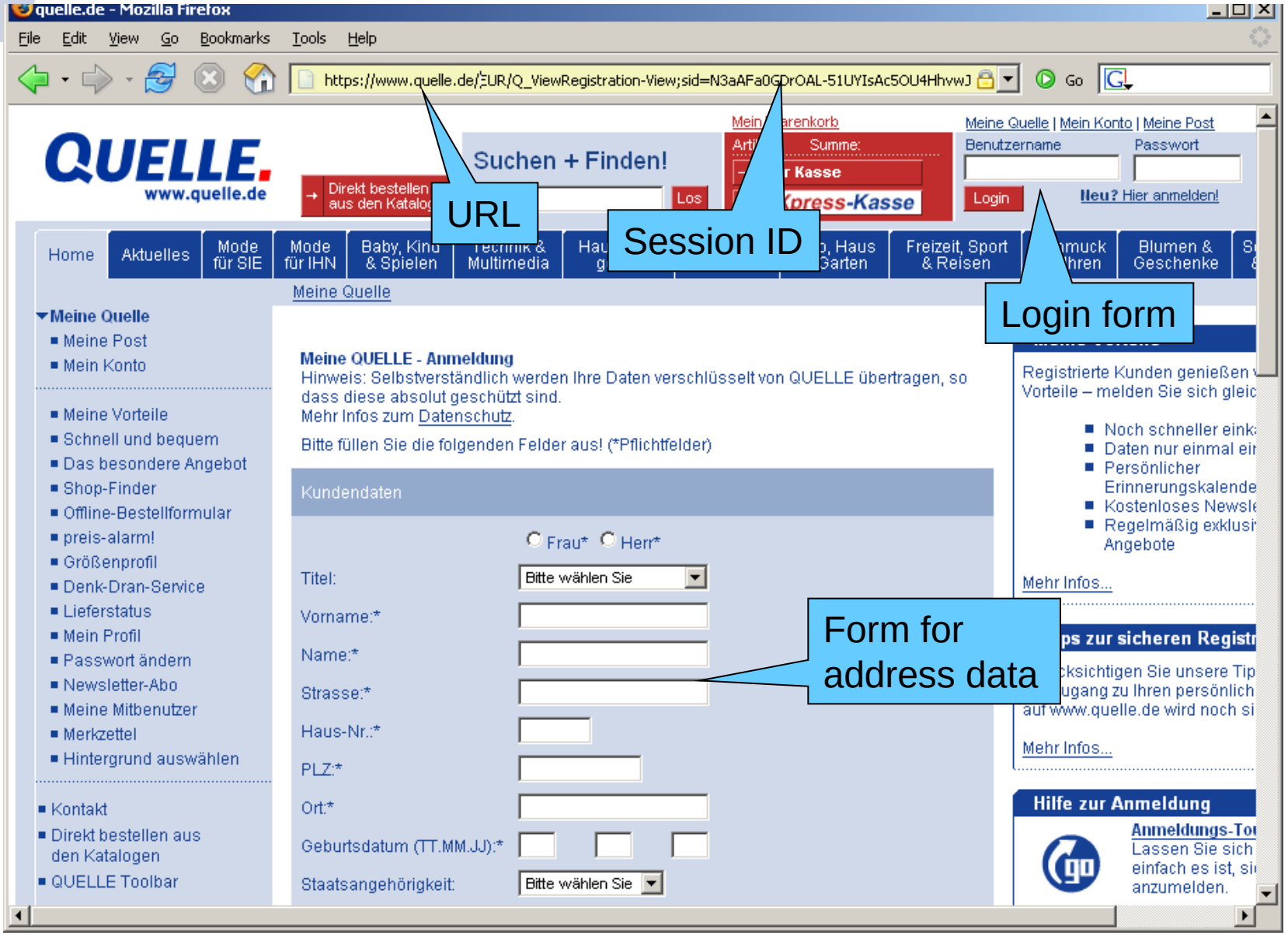
cirosec

Attacking databases

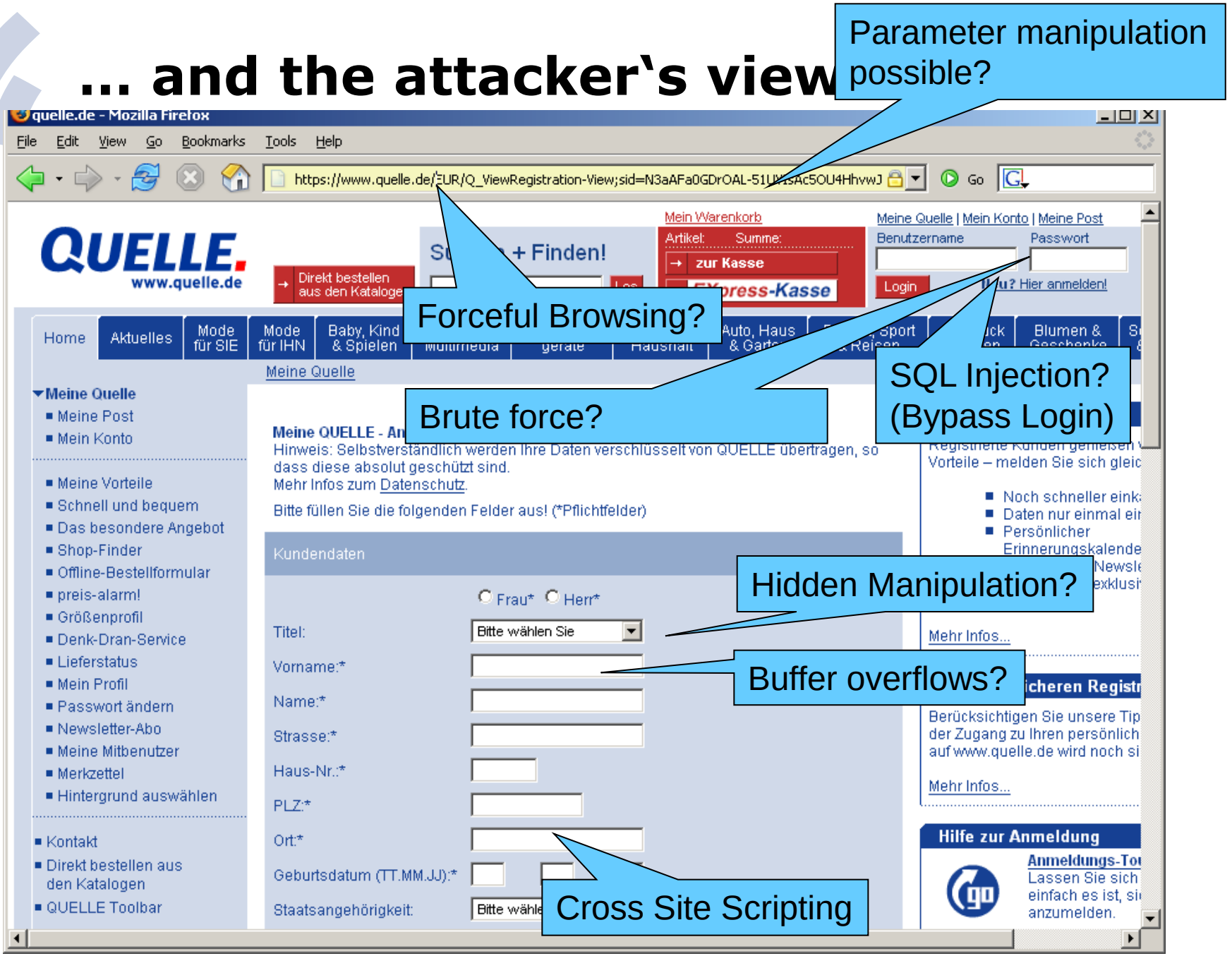


cirosec

Your view


quelle.de - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://www.quelle.de/EUR/Q_ViewRegistration-View;sid=N3aAFa0GDrOAL-51UYIsAc5OU4HhvwJ
Go
QUELLE.
www.quelle.de
Suchen + Finden!
Los
Meine Quelle | Mein Konto | Meine Post
Benutzername
Passwort
Login
Neu? Hier anmelden!
Home
Aktuelles
Mode für SIE
Mode für IHN
Baby, Kind & Spielen
Technik & Multimedia
Freizeit, Sport & Reisen
Blumen & Geschenke
Meine Quelle
Meine Quelle
Meine Post
Mein Konto
Meine Vorteile
Schnell und bequem
Das besondere Angebot
Shop-Finder
Offline-Bestellformular
preis-alarm!
Größenprofil
Denk-Dran-Service
Lieferstatus
Mein Profil
Passwort ändern
Newsletter-Abo
Meine Mitbenutzer
Merkzettel
Hintergrund auswählen
Kontakt
Direkt bestellen aus den Katalogen
QUELLE Toolbar
Meine QUELLE - Anmeldung
Hinweis: Selbstverständlich werden Ihre Daten verschlüsselt von QUELLE übertragen, so dass diese absolut geschützt sind.
Mehr Infos zum Datenschutz.
Bitte füllen Sie die folgenden Felder aus! (*Pflichtfelder)
Kundendaten
Frau* Herr*
Titel:
Bitte wählen Sie
Vorname:*
Name:*
Strasse:*
Haus-Nr.:*
PLZ:*
Ort:*
Geburtsdatum (TT.MM.JJ):*
Staatsangehörigkeit:
Bitte wählen Sie
Registrierte Kunden genießen
Vorteile – melden Sie sich gleic
Noch schneller eink
Daten nur einmal ei
Persönlicher Erinnerungskalende
Kostenloses Newsl
Regelmäßig exklusi Angebote
Mehr Infos...
Hilfe zur Anmeldung
Lassen Sie sich einfach es ist, si anzumelden.
URL
Session ID
Login form
Form for address data

… and the attacker's view



example: SQL Injection

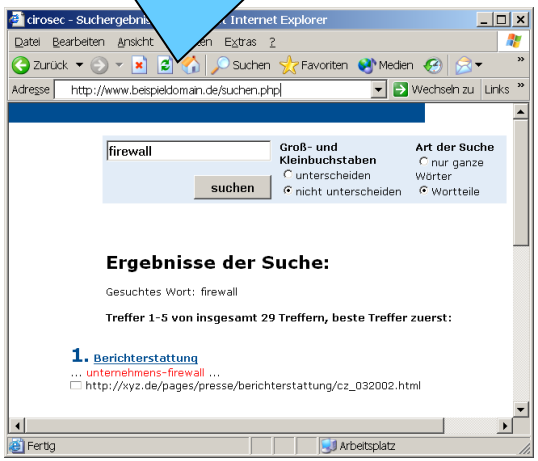
select info from products where id = 1; update set price = 1 = 1 where artikel like %notebook

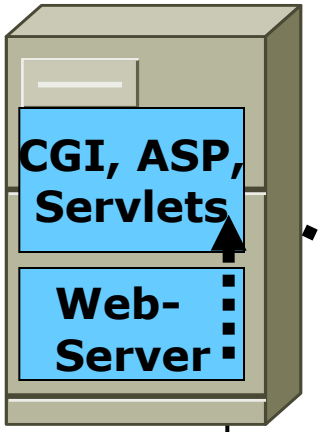
1; update set price = 1 where artikel like %notebook

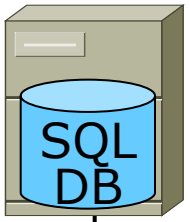
Shopping application

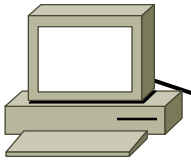
Prices beeing changed

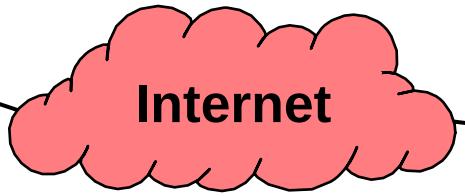
Internal database

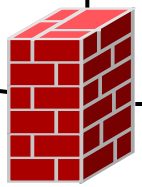


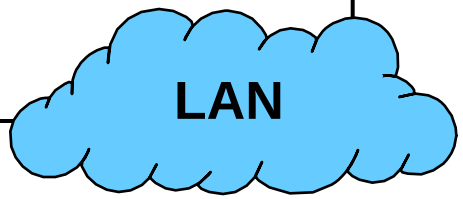












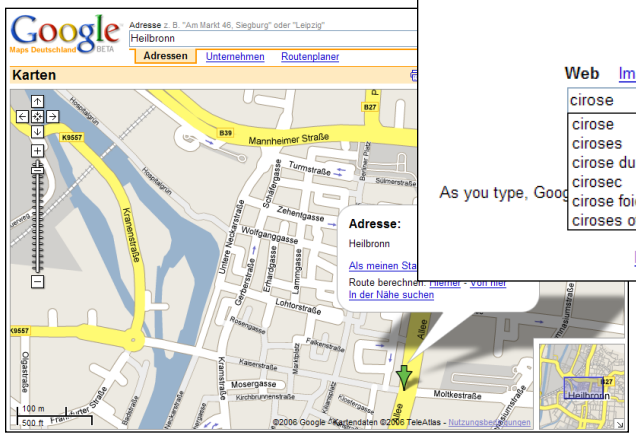
cirosec

Some more examples

- CSRF
  - Start illegal transactions
- Weaknesses in the session management
  - Manipulation of session IDs
  - Session Fixation
  - Privilege escalation, access to other people's data
- Logical bugs in the application
  - Download of arbitrary files
  - Negative money transfers
- New challenges because of AJAX
- And many more

What is AJAX?

- **A**synchronous **J**avaScript **a**nd **X**ML
- HTTP-requests within HTML-pages without page reload
- Since 2005, similar technology existing since 1998 (Outlook Web Access/IE4)
- Used in many well known web sites:
  - Google Suggest
  - Google Maps
  - Flickr
  - Del.icio.us
  - …

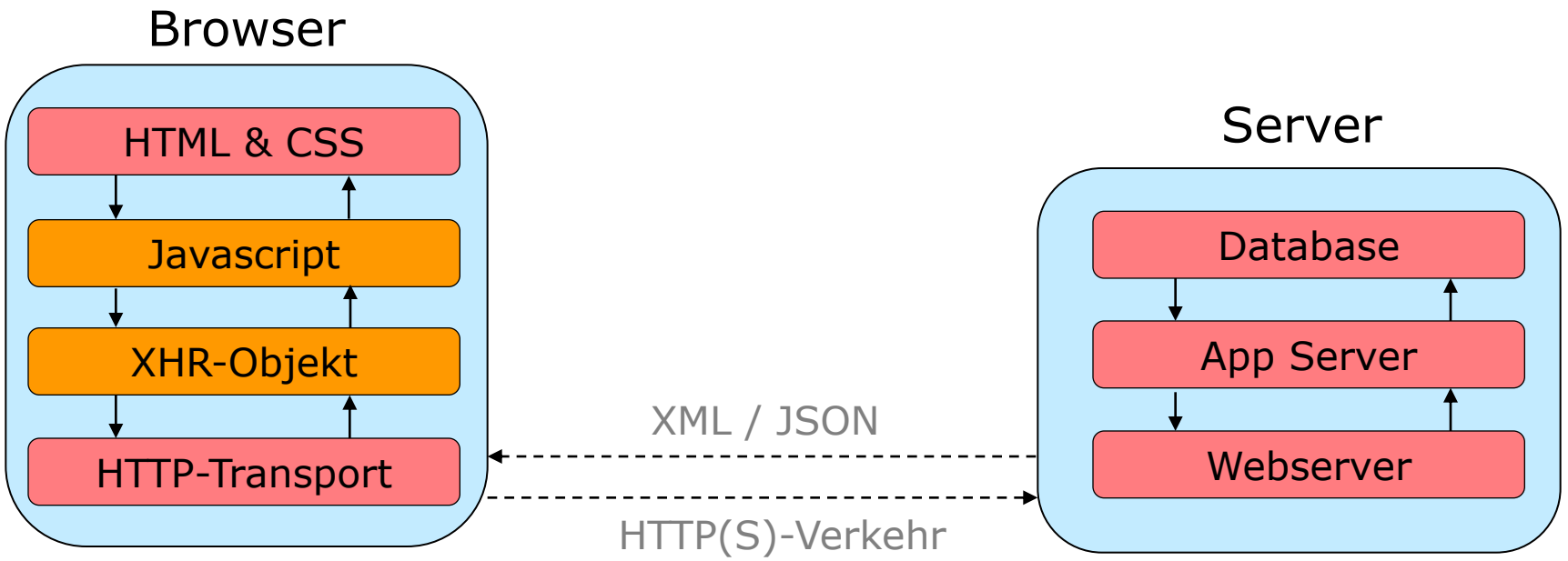


cirosec

Classic model of web applications

cirosec

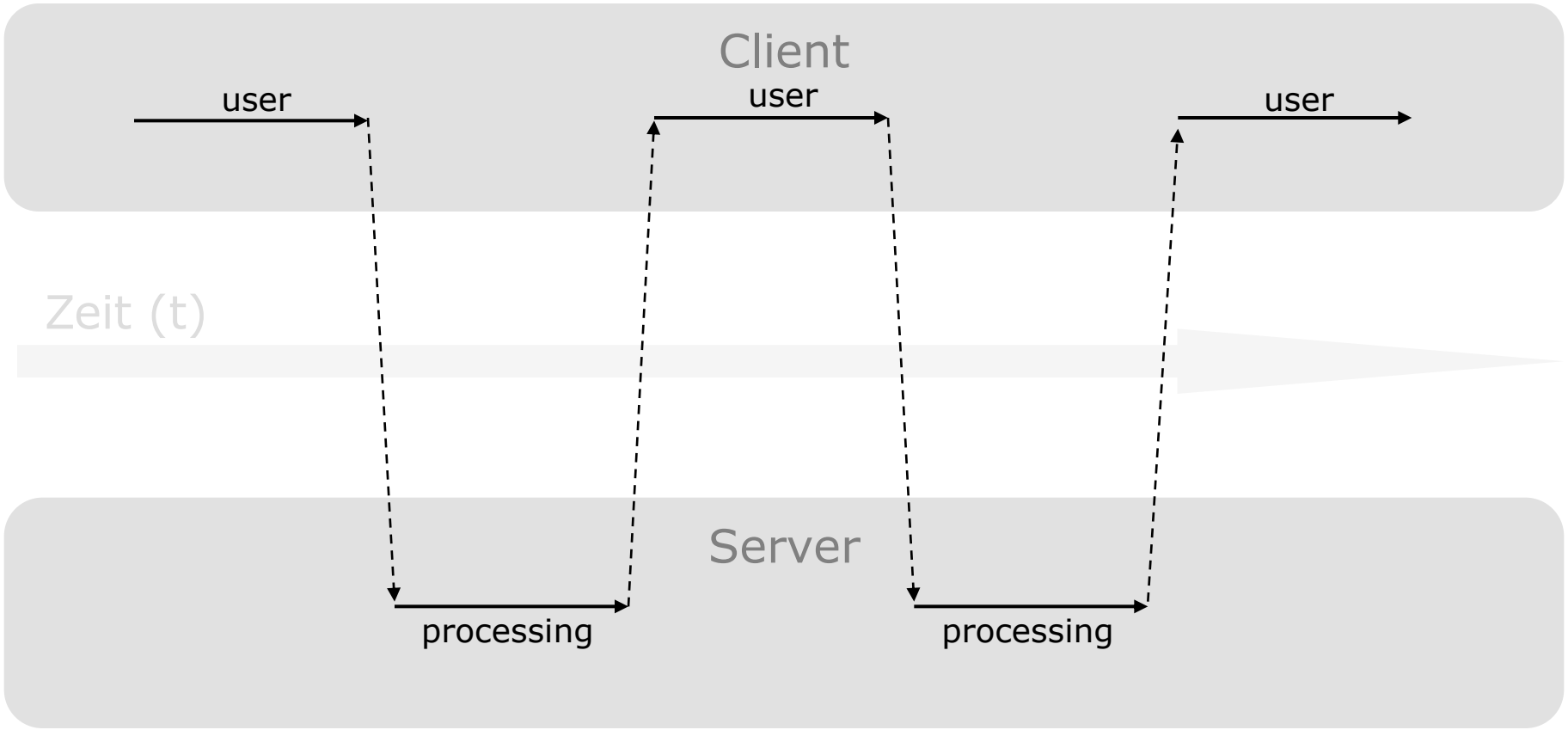
AJAX model



- Transfer of logic to the client side

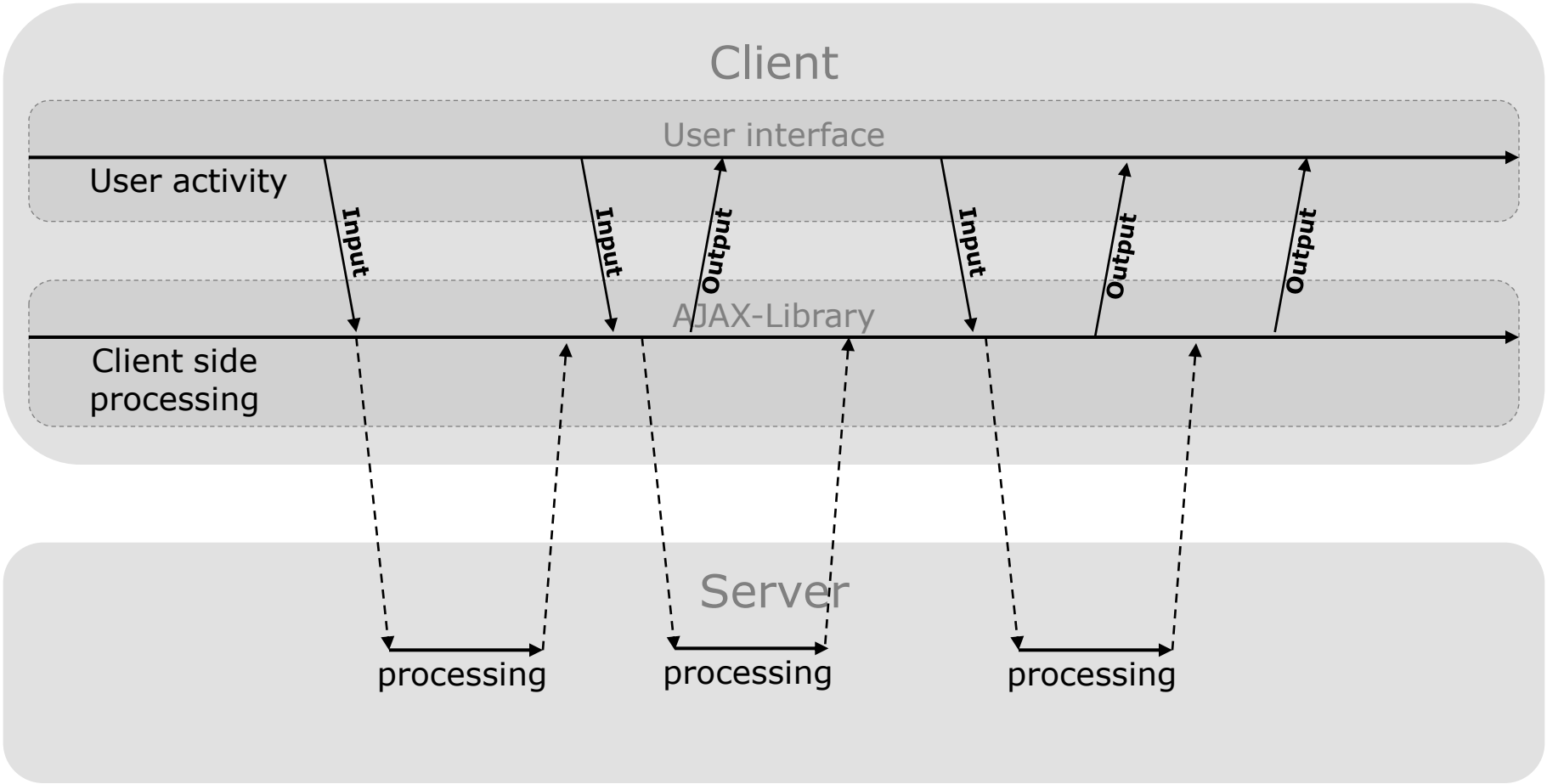
cirosec

Classical web process flow



cirosec

AJAX process flow



cirosec

Old threats

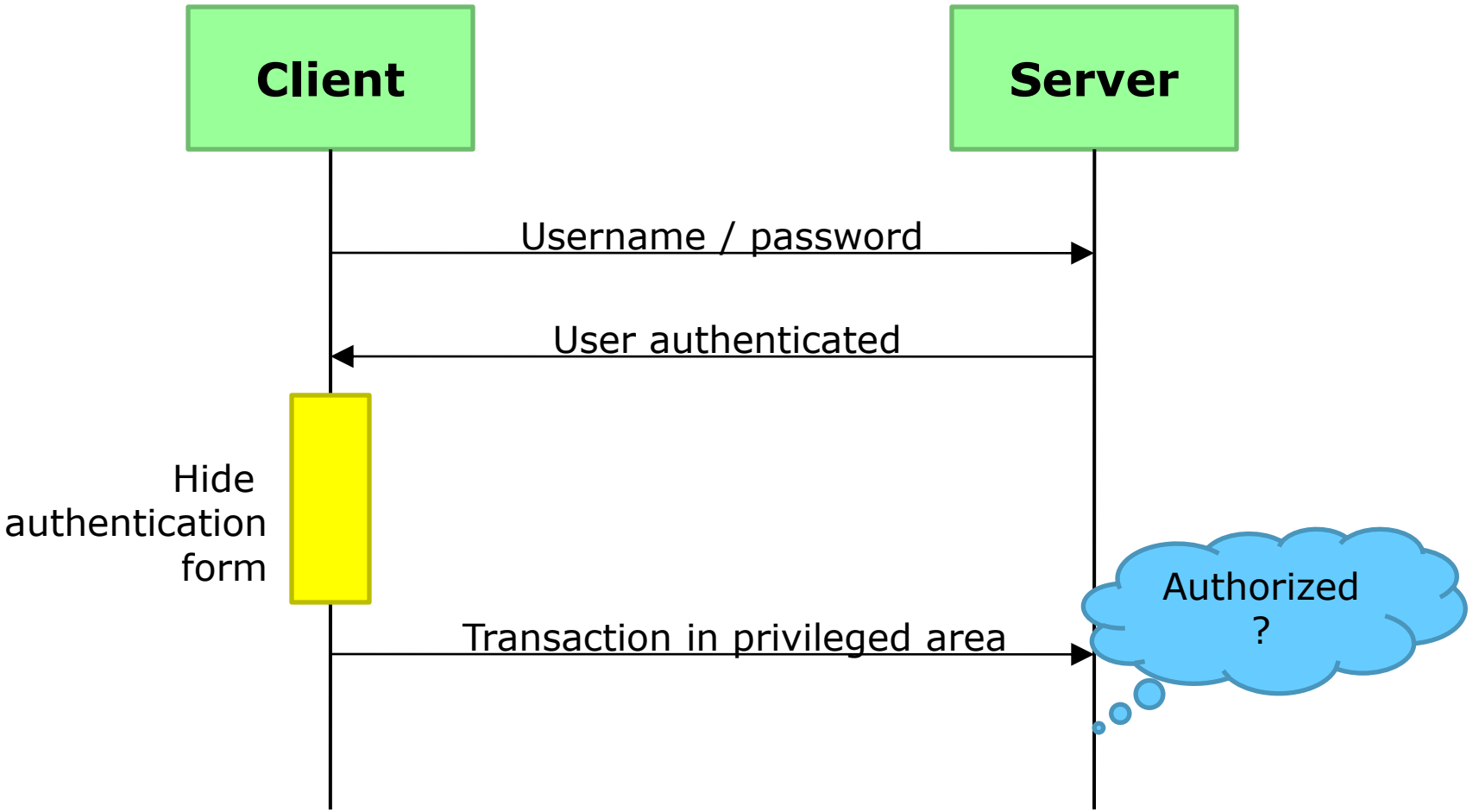
- ...remain the same
- AJAX requests are normal HTTP requests
- Known attacks like SQL-Injection, XSS or File-Inclusion are still relevant

New threats because of AJAX

- Server side
  - Attack surface increased because of more parameters
    - Input validation?
  - Unauthorized / unauthenticated use of AJAX functions
- Client side
  - More logic on the client side
    - Vulnerabilities in client side code

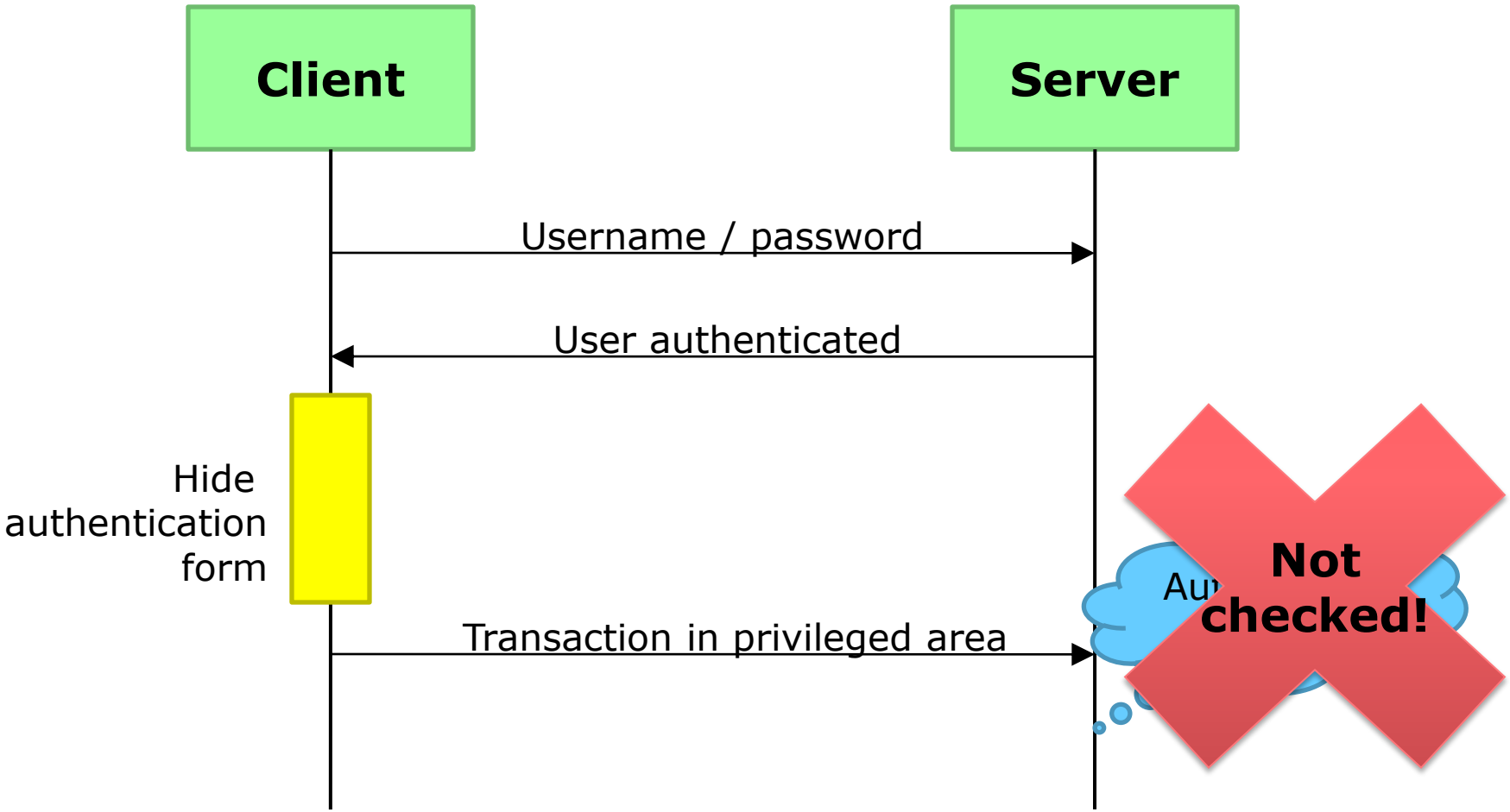
cirosec

Vulnerable authentication



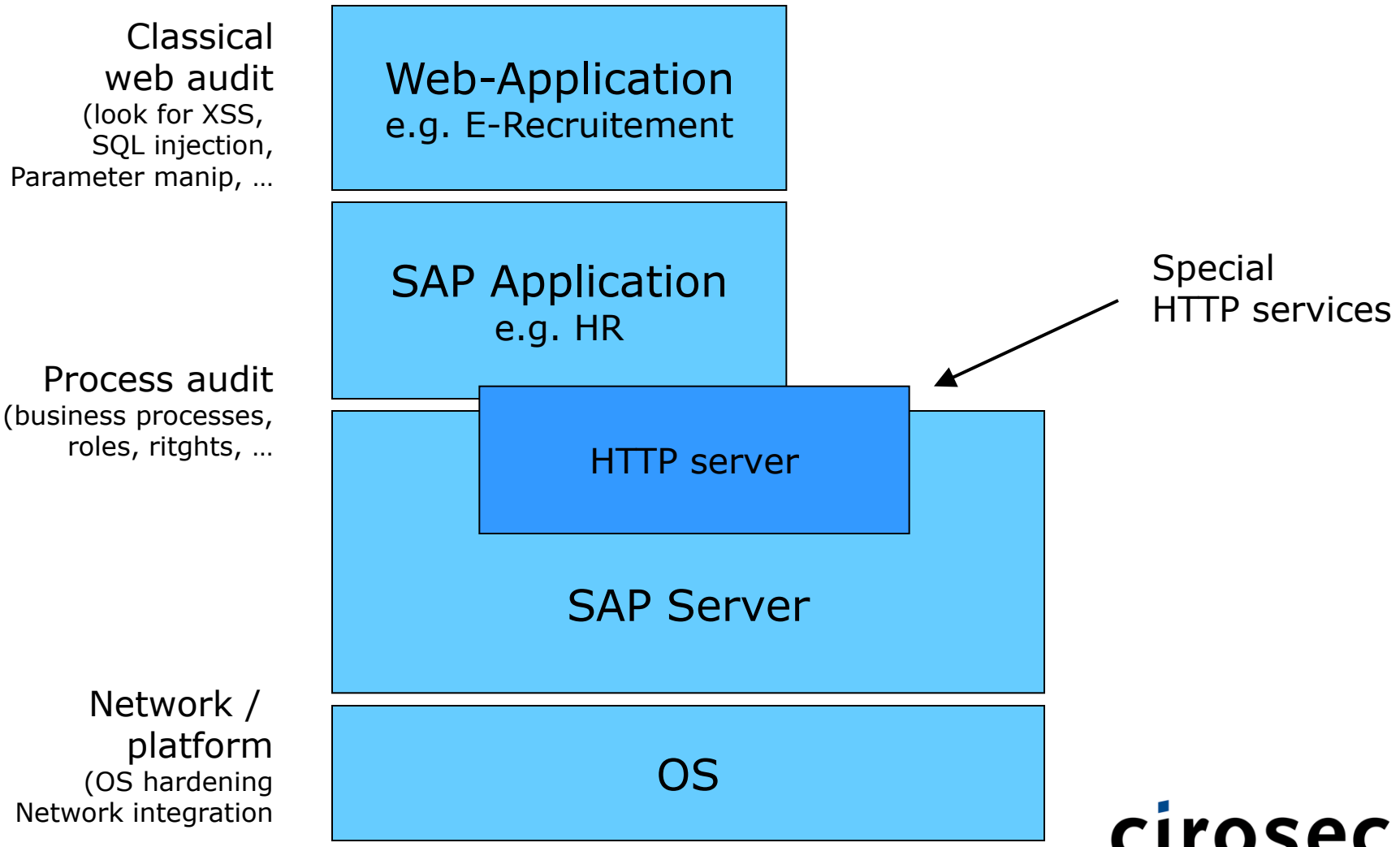
cirosec

Vulnerable authentication



cirosec

SAP based web applications



cirosec

SAP HTTP Services

- More than 150 services in a raw server
  - Web GUI, SOAP, etc.
- Enumeration and audit with Webinspect
  - Custom policy created by cirosec

cirosec

example: SAP-Info over HTTP

http://172.16.0.106:8001/sap/public/info?icm=1

```
- <RFCSI>
    <RFCPROTO>011</RFCPROTO>
    <RFCCHARTYP>4103</RFCCHARTYP>
    <RFCINTTYP>LIT</RFCINTTYP>
    <RFCFLOTYP>IE3</RFCFLOTYP>
    <RFCDEST>sapn4s_N4S_01</RFCDEST>
    <RFCHOST>sapn4s</RFCHOST>
    <RFCSYSID>N4S</RFCSYSID>
    <RFCDATABS>N4S</RFCDATABS>
    <RFCDBHOST>sapn4s</RFCDBHOST>
    <RFCDBSYS>ADABAS D</RFCDBSYS>
    <RFCSAPRL>700</RFCSAPRL>
    <RFCMACH>390</RFCMACH>
    <RFCOPSYS>Linux</RFCOPSYS>
    <RFCTZONE>3600</RFCTZONE>
    <RFCDAYST />
    <RFCIPADDR>172.16.0.106</RFCIPADDR>
    <RFCKERNRL>700</RFCKERNRL>
    <RFCHOST2>sapn4s</RFCHOST2>
    <RFCSI_RESV />
    <RFCIPV6ADDR>172.16.0.106</RFCIPV6ADDR>
```

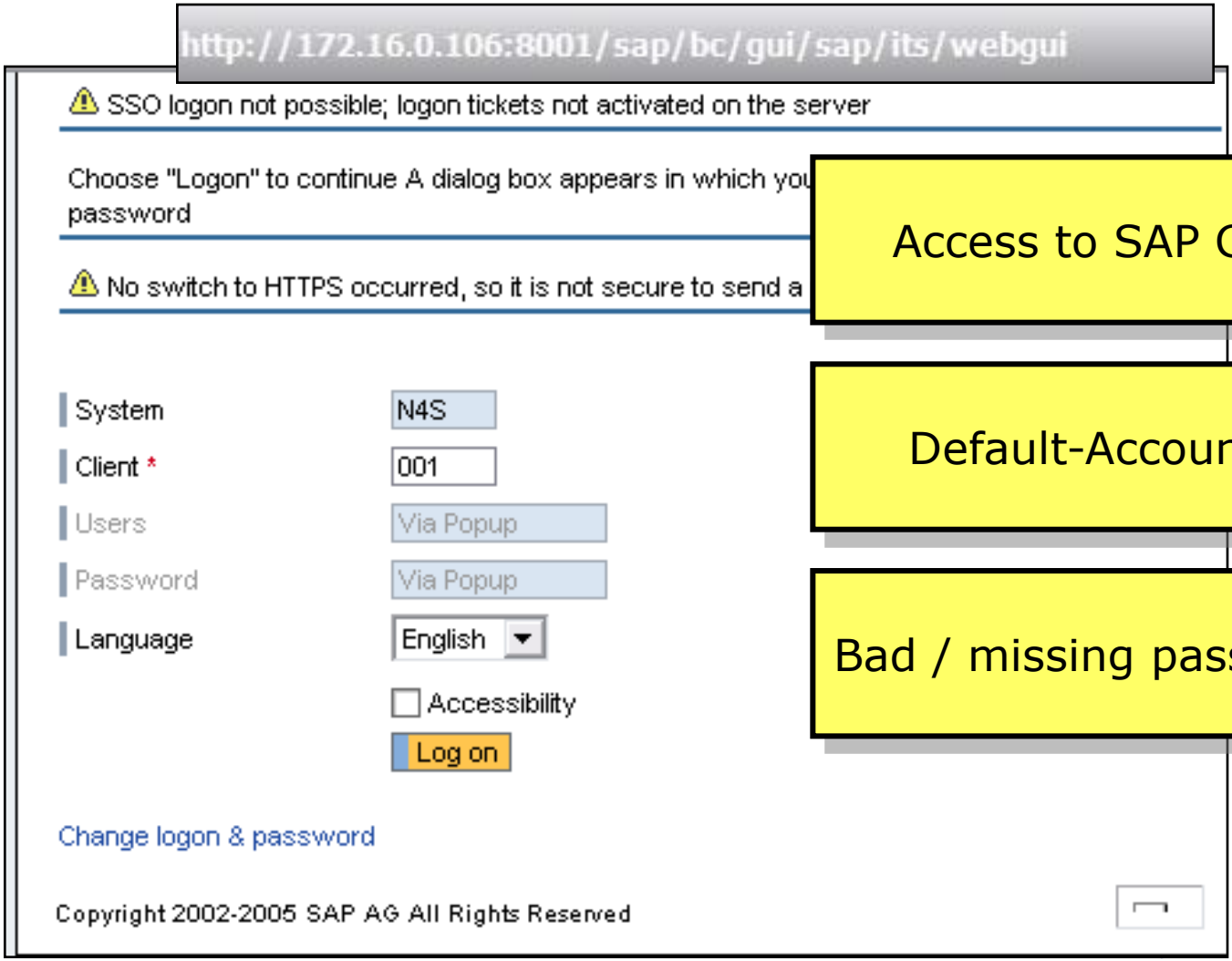
Database (SAP Max DB)

SAP Version

OS Version

Internal IP-Address

WebInspect SAP Policy



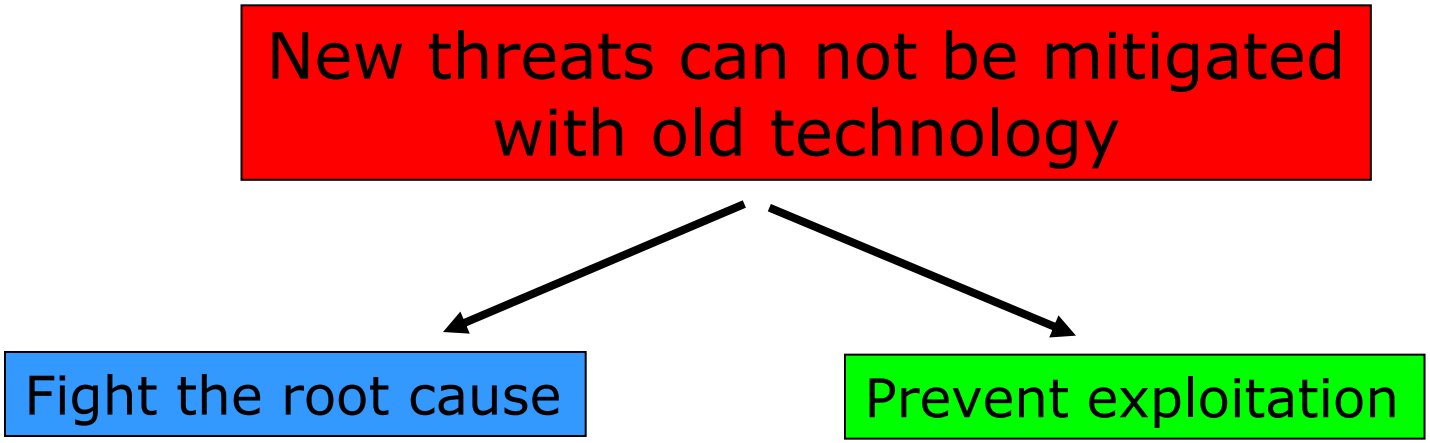
Access to SAP GUI

Default-Accounts

Bad / missing password

cirosec

Security for web applications



- secure programming
- secure architecture
- regular security testing

- new technologies and products

cirosec

1. Fight the root cause

cirosec

Coding guidelines for secure development

- Need awareness and support
  - Hacker trainings have proven to be successful here
- Should be developed together with the developers

- Source code analysis tools can help to constantly remind people of the guidelines

Secure coding is not a full solution

- Limited influence due to foreign code
  - Libraries, platforms, frameworks, backends
- People make mistakes
  - Doing input validation right is not as simple as it seems

2. Testing security

cirosec

Application audits / pentests

- During development
  - Security testing tools integrated in the development environment
- During QA
  - Security as part of quality
  - Security testing while testing anyway
- Before going into production
  - By security experts

- The earlier the cheaper

cirosec

Different approaches

- From the outside
  - With tools like Webinspect and manual work
- Looking inside the code
  - Source code analysis tools and manual work
- Combination of both

- Tools are important even if more time is spent doing manual checks

cirosec

Automated black box tests

- Checking for the existence of
  - Standard (sub) directories
  - Backup or config files
- Checking the reaction to input
  - <script> being output
  - Error messages to special character input
    - Internal server error
    - ODBC Error
- And much more

cirosec

3. Prevent exploitation

cirosec

WAFs

- Gateways in front of the web server farm
- can validate input where applications do not
- Can track session state
- And much more

cirosec

Summary

- Web application security is and remains an important issue
- Security testing needs to be done earlier in the lifecycle
- The right tools make things easier
- Awareness and trainings must not be left out

cirosec