

# Angriffe auf Web Applikationen



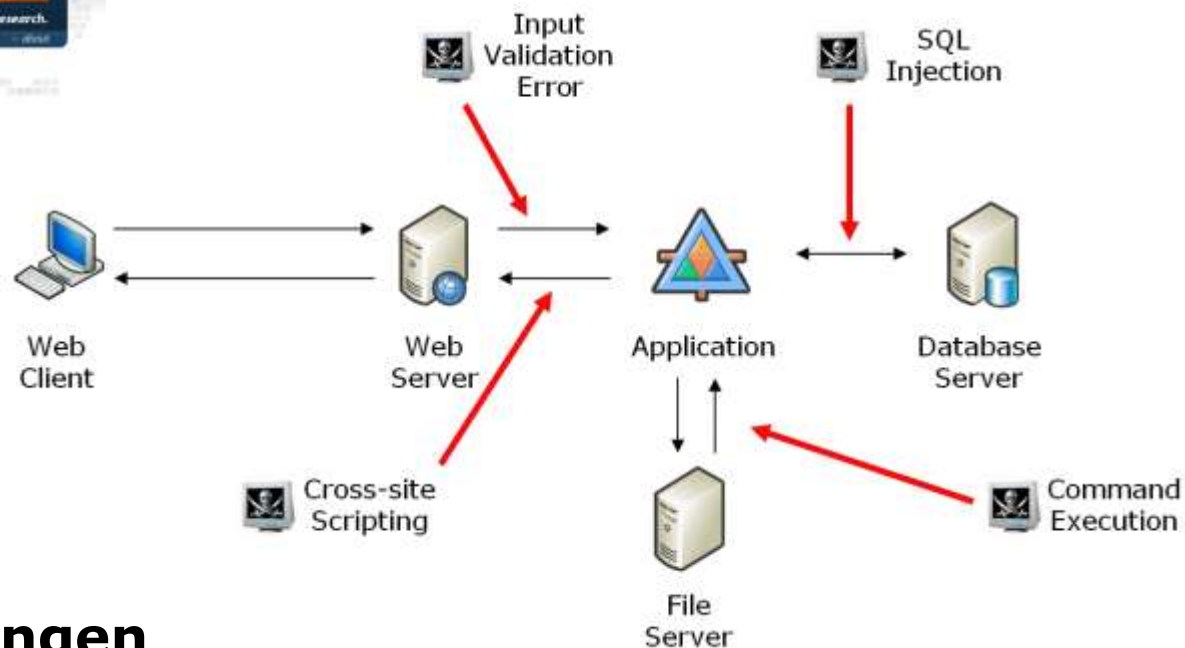
# Bedrohungen



SANS Top-20 2007 Security Risks (2007 Annual Update)

Server-side Vulnerabilities in:

11. Web Applications
12. Webmail Services
13. Unix and Mac OS Services



- **Web-Anwendungen**

sind derzeit das Haupteinfallstor für Angreifer!

- **Neue Gefahren**

können nicht durch alte Technologien geschützt werden!

# Klassifizierung – Angriffsvektoren

- Cross-Site Scripting (XSS)

Eingabevalidierung

Web Applikation

http://www.bekannt.de

The screenshot shows a web profile for Dr. Wolfgang Schäuble MdB, a German politician. The profile includes a navigation menu with items like 'Position', 'Veröffentlichungen und Interviews', 'Reden', 'Wahlkreis', 'Persönlich', 'Links', and 'Kontakt'. A large photo shows Dr. Schäuble holding a handgun. Below the photo is a search bar and a 'Position' section with links to 'Verfassungsschutzbericht', 'BKA-Gesetz', and 'Tarifverhandlungen im öffentlichen Dienst'. The main content area is divided into 'Reden' (Speeches) and 'Interviews'. Under 'Reden', there is a speech from February 18, 2009, at the London School of Economics. Under 'Interviews', there is an interview from February 16, 2009, with the Tagesspiegel. A second 'Reden' section at the bottom features a speech from February 13, 2009, at a symposium in Berlin. On the right side of the page, there are two smaller photos of Dr. Schäuble at a desk and in a close-up, with a 'Weitere Bilder' section and a link to 'Zur Bilderübersicht'.

innnt.de

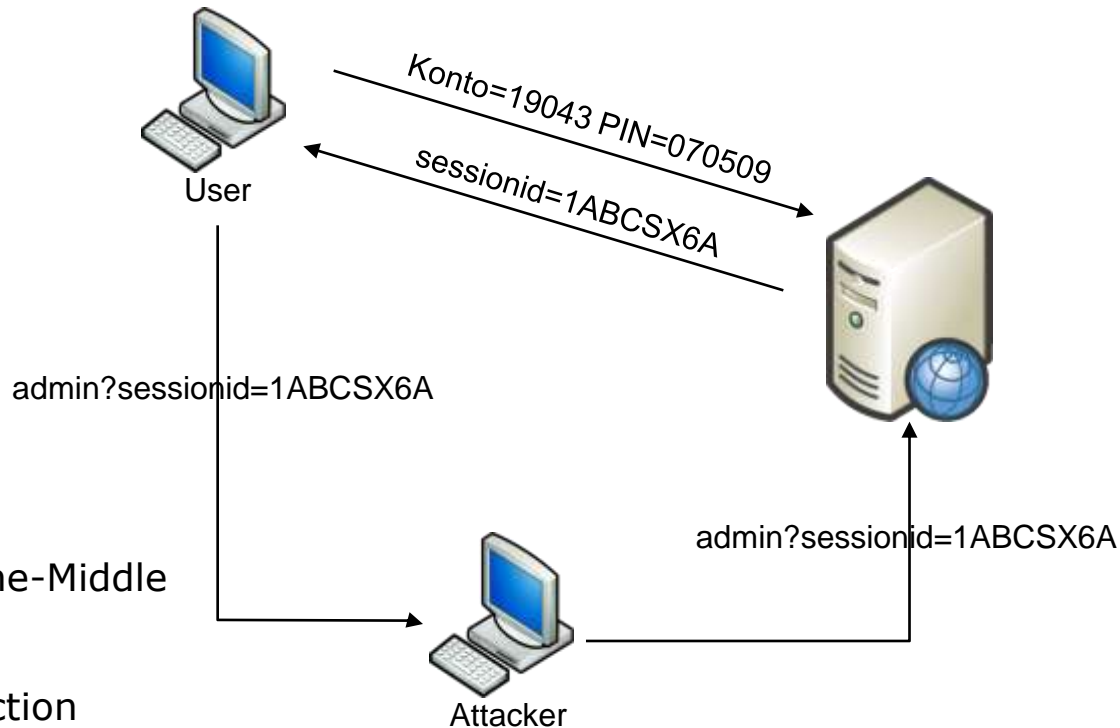
ha.cke.me

# Klassifizierung – Angriffsvektoren

- Session-Hijacking

Sessionmanagement  
MENSCH

Web Applikation



- Man-in-the-Middle
- XSS
- SQL-Injection
- Code-Injection

# Web Application Hacking

# Unternehmensprofil

art OF defence = Web Application Security Softwarehersteller



- Technologiepartnerschaften mit Herstellern  
(u.a. mit Microsoft, GeNUA, Zeus, ...)
- weltweite Kundeninstallationen in Europa, USA und Asien  
(u.a. TOP 10 Webshops, TOP 5 Community-Portale, ...)
- OWASP Member  
(Beteiligung an weltweiten Projekten, German Chapter Co-Leader, ...)

# Web Application Security Software

## Web Source Code Analyzer



hyper SOURCE

- PHP, Java und ASP.NET Code Analyse (z.B. Basis für manuellen Code Review)
- Signaturen für den hyperscan
- Regelgenerierung für hyperguard

## Web Vulnerability Scan Server



hyper scan

- Web Application Security Scanner (z.B. Basis für manuellen PenTest)
- Regelgenerierung für hyperguard

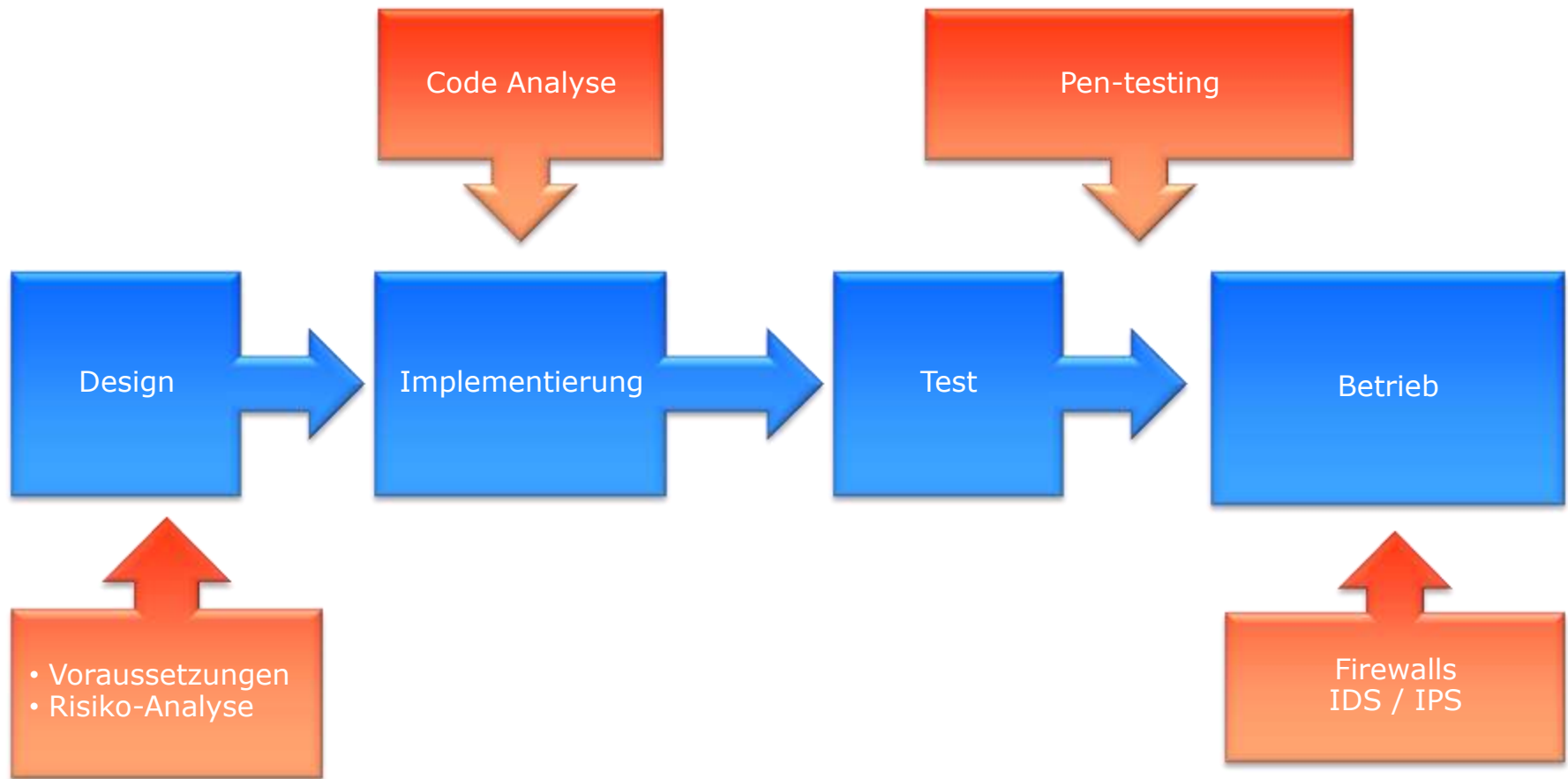
## Web Application Attack Detection



hyper guard

- zentrales Management
- Monitoring, Reporting und Alerting
- Clustertechnologie
- Protection:**
  - frei programmierbare API
  - URL-Encryption
  - ICAP-Client

# Web Application Live Cycle



Vielen Dank!