FACHHOCHSCHULE **TRIER**
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences

Web-Application Security

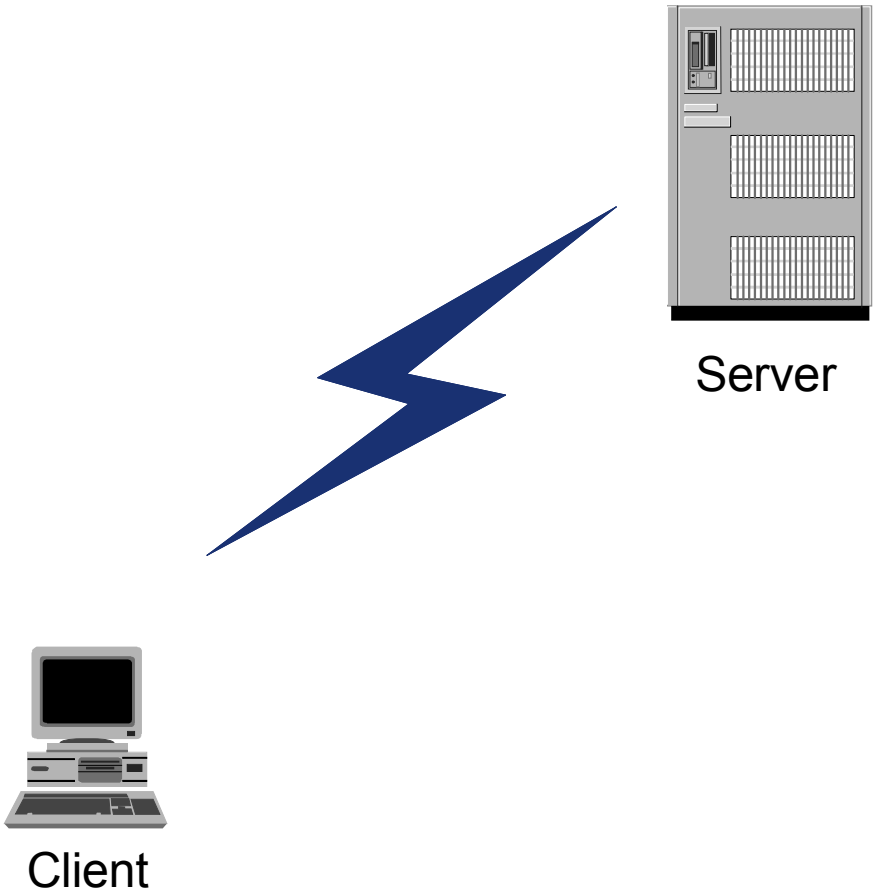
Verbesserung der Sicherheit von Internetanwendungen durch den Einsatz einer Web-Application-Firewall

Vortrag zur Masterarbeit
Hans-Jürgen Stemmer
11.01.2006

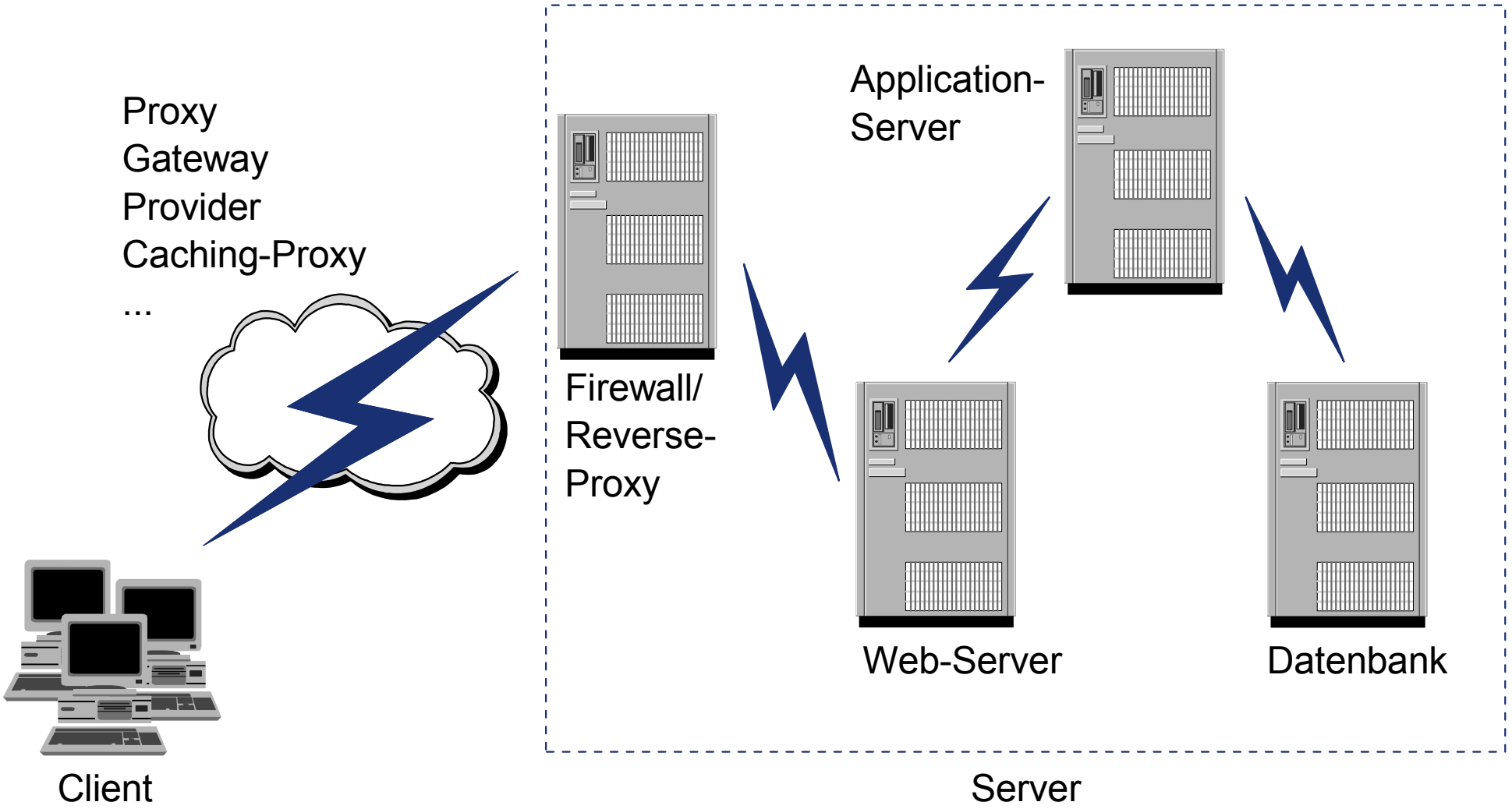
Inhalt

- Internet
- HTML
- HTTP
- Hidden Field Manipulation
- Forceful Browsing
- Web-Application Firewall

Internet



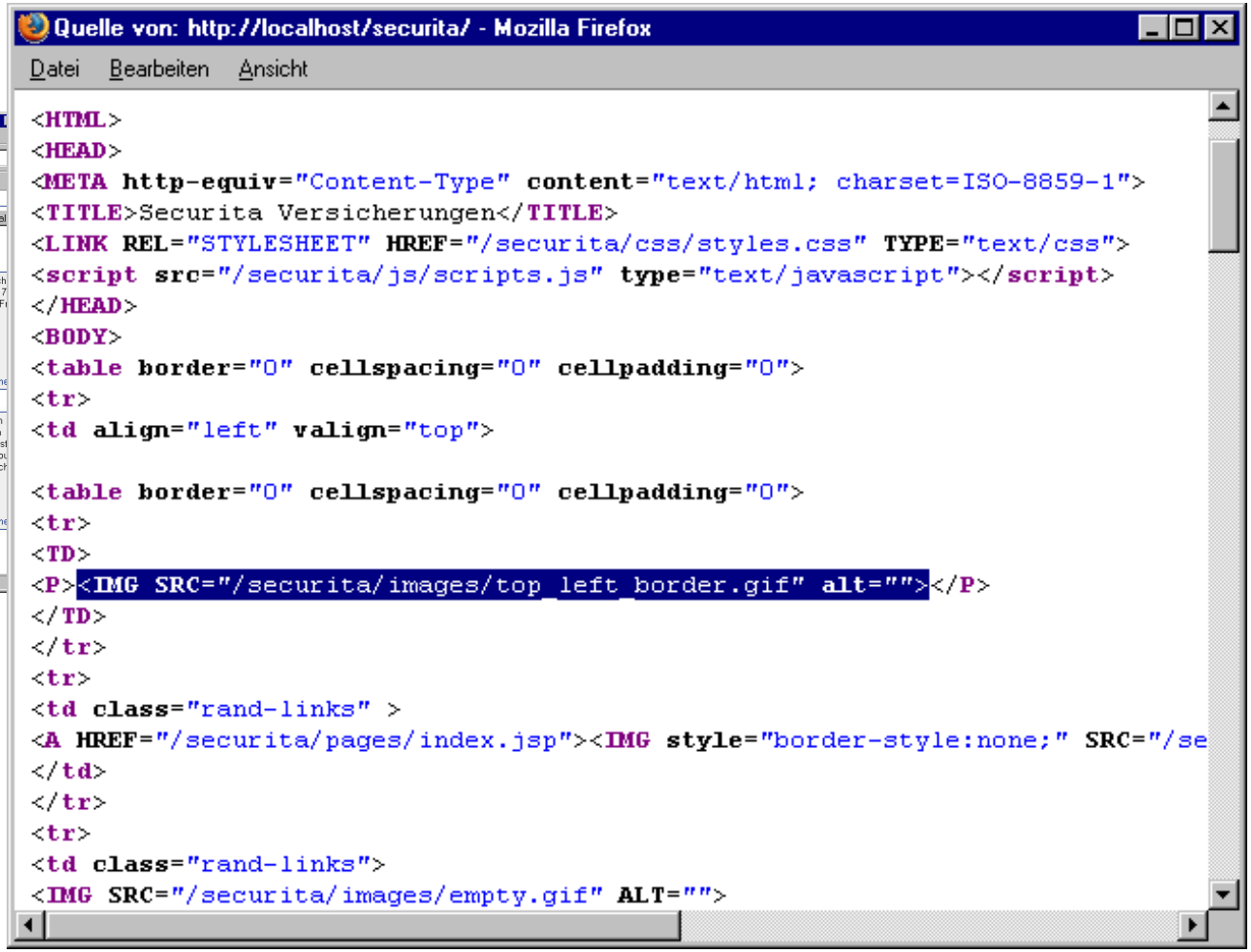
Internet


Proxy
Gateway
Provider
Caching-Proxy
...
Client
Firewall/
Reverse-
Proxy
Application-
Server
Web-Server
Datenbank
Server

HTML

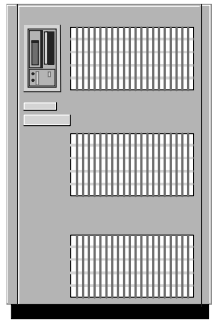
Hyper-Text-Markup-Language

Client



FACHHOCHSCHULE TRIER
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences

Hyper-Text-Transfer-Protocol



Server

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=04F0F5C780AD28; Path=/securita
Content-Type: text/html;charset=ISO-8859-1
X-Transfer-Encoding: chunked
Date: Sat, 07 Jan 2006 14:26:09 GMT
Content-length: 6322

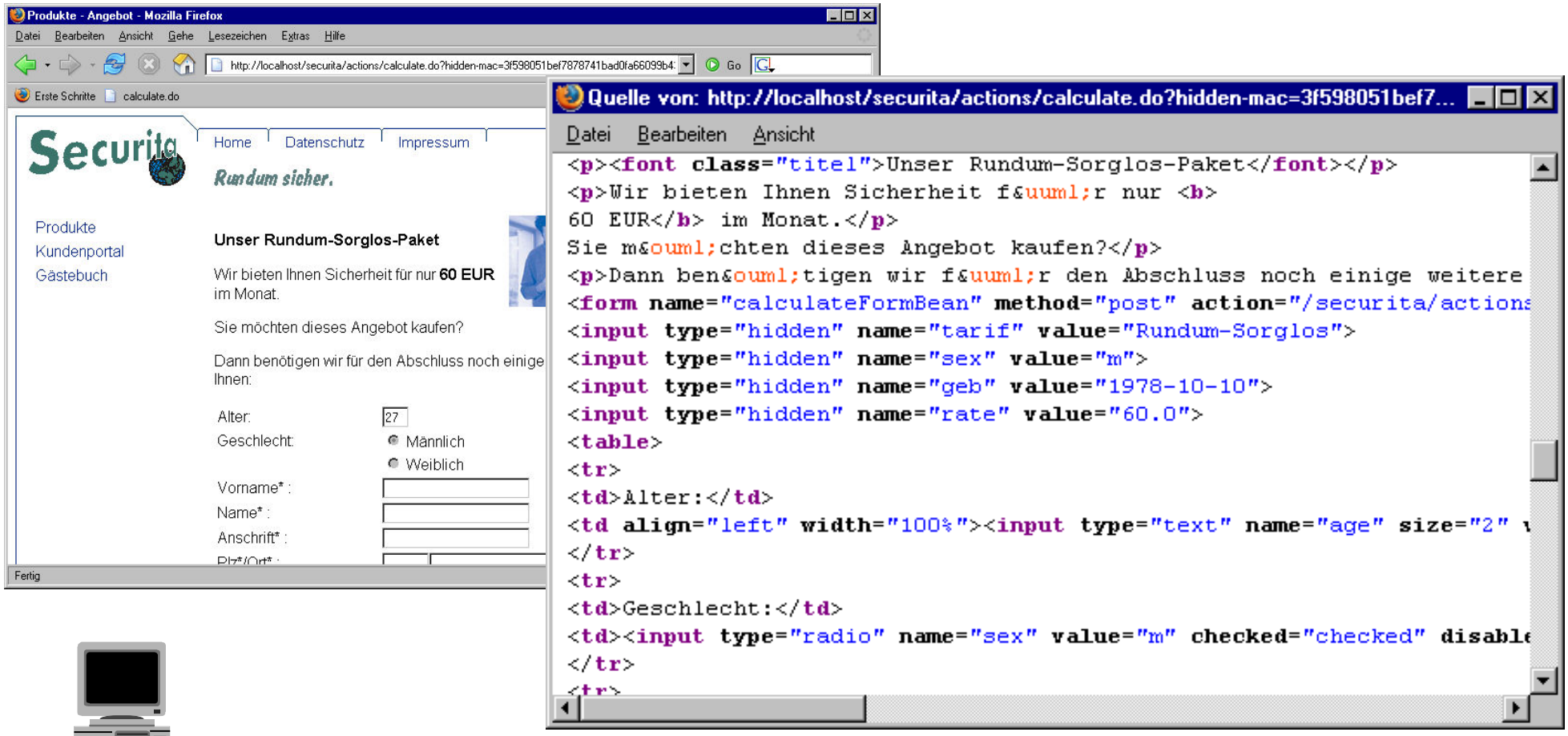
<HTML> ...

Client

GET http://localhost/securita/ HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows; U; WinNT4.0;...
Accept: text/xml,application/xml,text/html;...
Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive

Hidden Field Manipulation

FACHHOCHSCHULE **TRIER**
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences



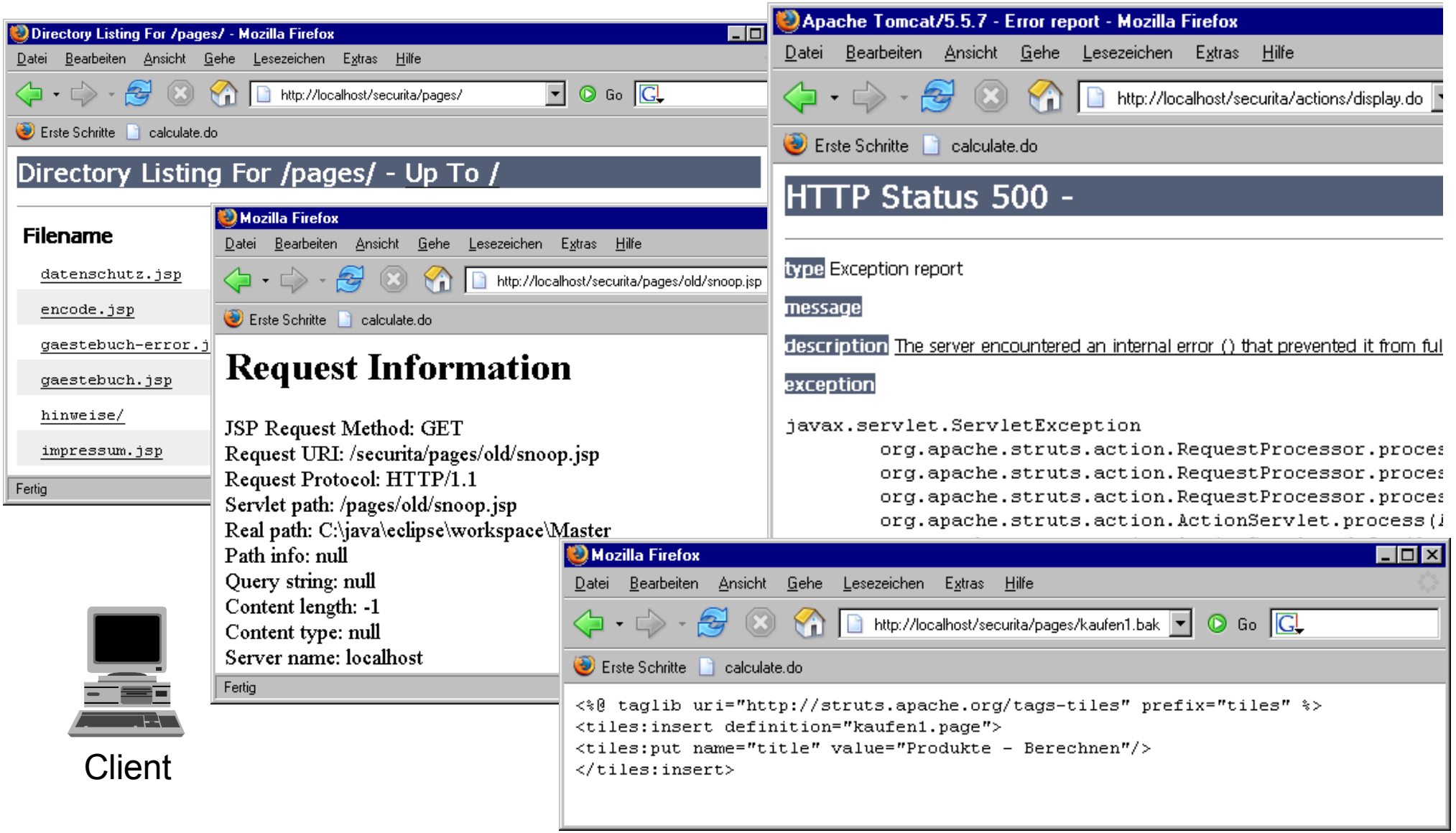
Client

POST http://localhost/securita/actions/abschluss.do HTTP/1.1

tarif=Rundum-Sorglos&sex=m&geb=1978-10-10&rate=60.0&...

Forceful Browsing

FACHHOCHSCHULE **TRIER**
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences

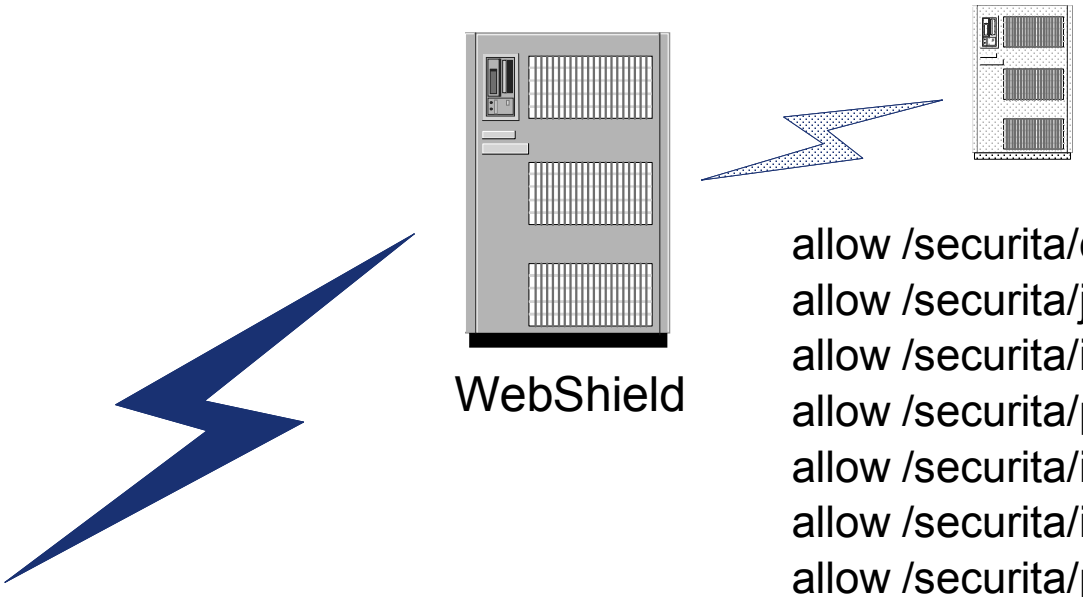


Web-Application Firewall

FACHHOCHSCHULE **TRIER**
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences

WebShield

tarif+sex+geb+rate /securita/actions/abschluss.do for hidden-mac
-> hidden-mac=fa74138cc61bd5b4df6d51bbce3a97fcf5136469&...



allow /securita/css/styles.css
allow /securita/js/scripts.js
allow /securita/images/top_left_border.gif
allow /securita/pages/index.jsp
allow /securita/images/Securita.gif
allow /securita/images/head_nav_spacer2.gif
allow /securita/pages/datenschutz.jsp
allow /securita/pages/impressum.jsp
allow /securita/images/Rundum_sicher.gif
allow /securita/actions/invalidate.do
allow /securita/pages/kaufen1.jsp
allow /securita/pages/kundenportal/index.jsp
allow /securita/actions/gaestebuch.do
allow /securita/images/blue199/02.jpg

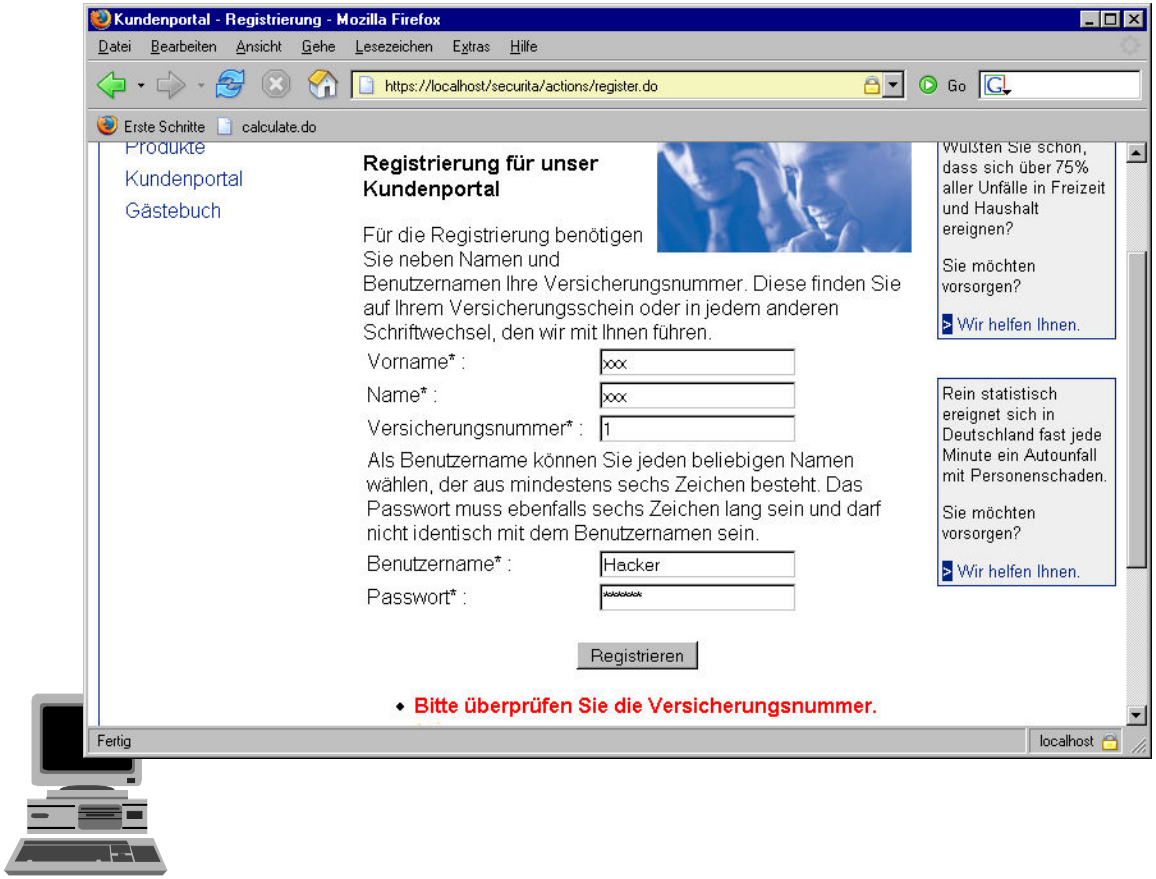
Fragen

??????????????

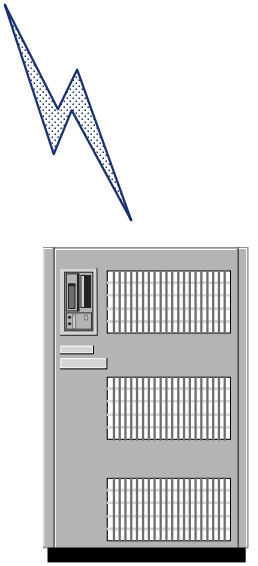
Injection Flaw

FACHHOCHSCHULE TRIER
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences

POST https://localhost/securita/actions/register.do HTTP/1.1
vorname=xxx&name=xxx&versnr=1&j_username=Hacker&j_password=123456



Client

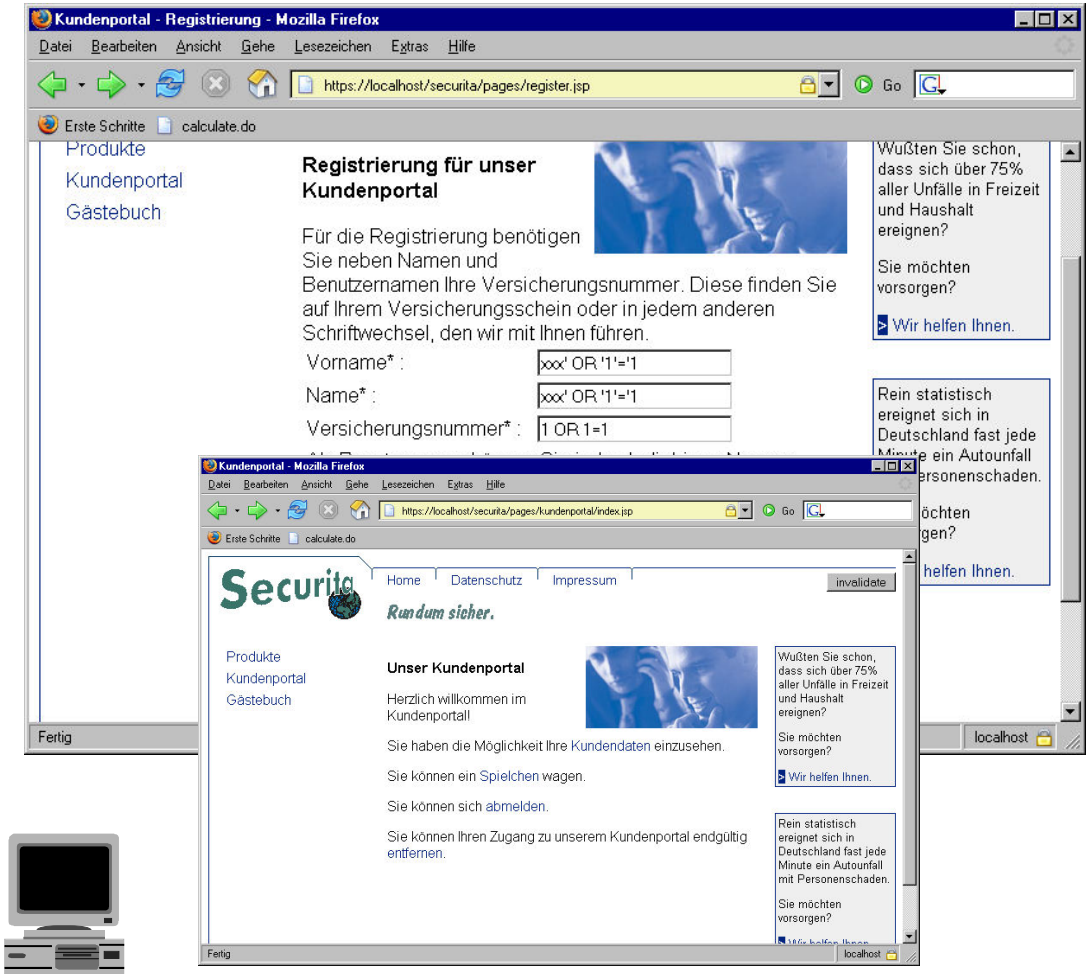


Datenbank

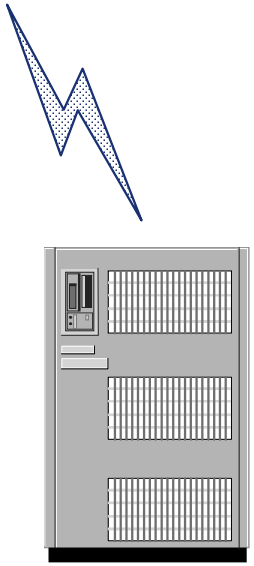
select * from vertrag where versnr=1

Injection Flaw

FACHHOCHSCHULE TRIER
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences



Client



Datenbank

select * from vertrag where versnr=1 OR 1=1

select 1 from vn t1, person t2 where t1.persid=t2.persid and t1.id =1 and t2.vorname='xxx' OR '1'='1' and t2.name='xxx' OR '1'='1'