

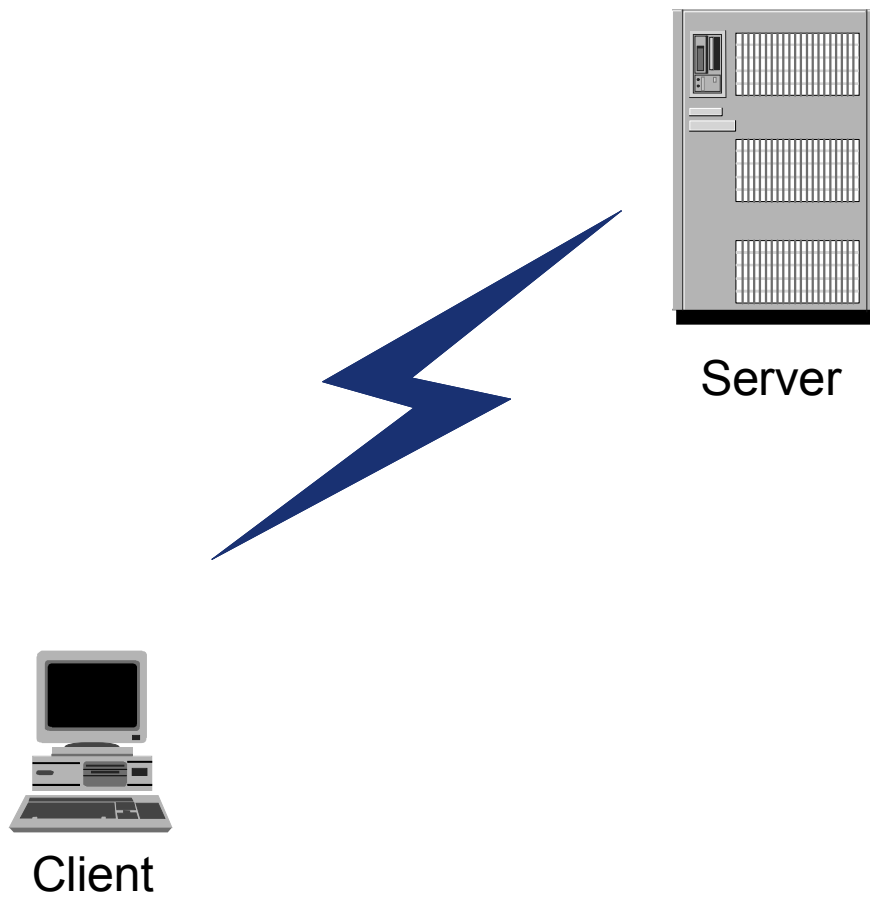
Web-Application Security

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

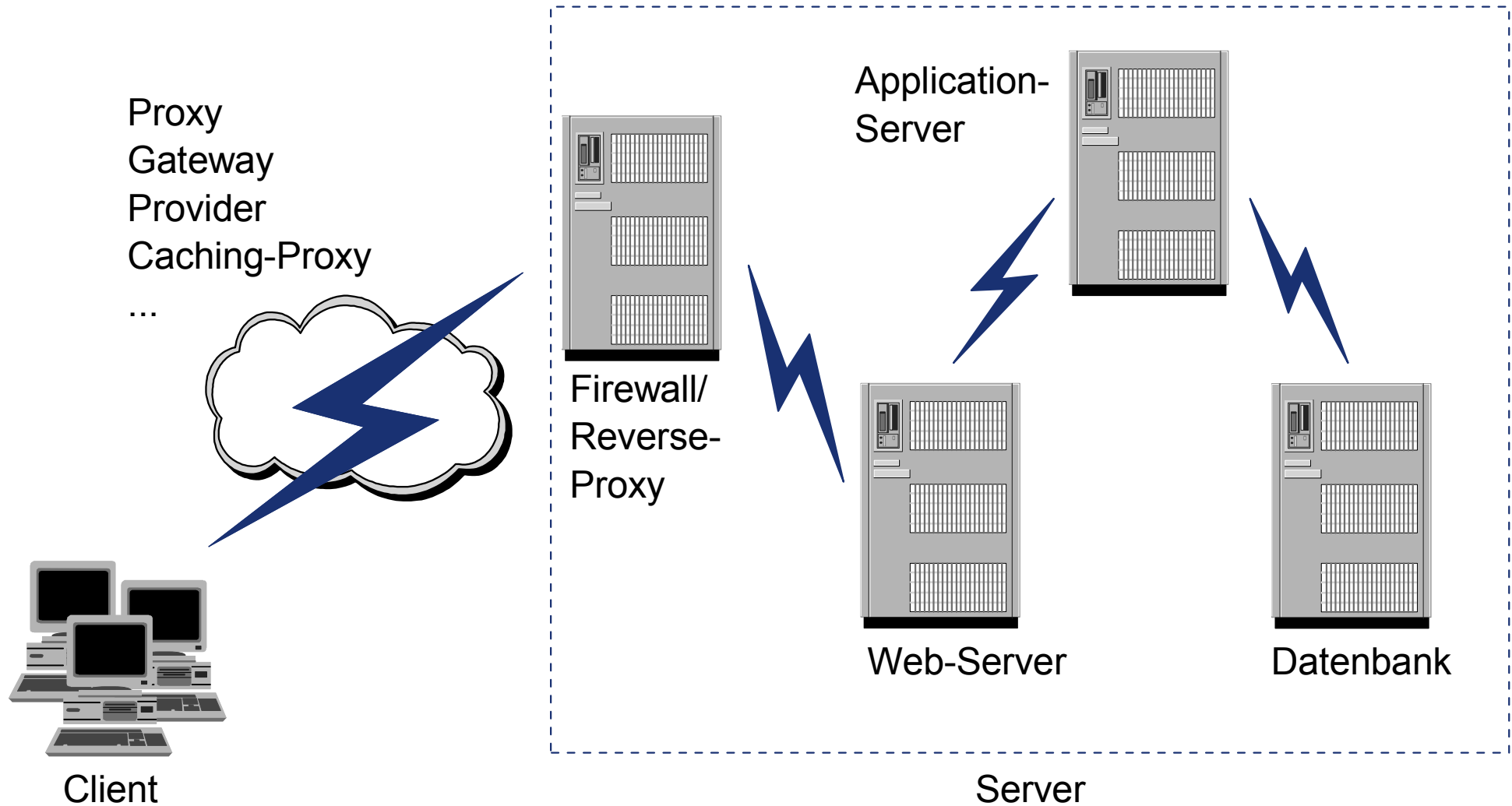
Vortrag zur Masterarbeit
Hans-Jürgen Stemmer
11.01.2006

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

Internet



Internet



Hyper-Text-Markup-Language



Client

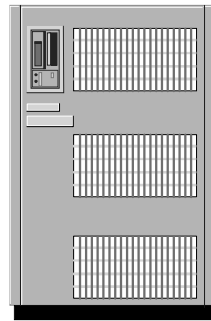
```
Quelle von: http://localhost/securita/ - Mozilla Firefox
Datei Bearbeiten Ansicht

<HTML>
<HEAD>
<META http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<TITLE>Securita Versicherungen</TITLE>
<LINK REL="STYLESHEET" HREF="/securita/css/styles.css" TYPE="text/css">
<script src="/securita/js/scripts.js" type="text/javascript"></script>
</HEAD>
<BODY>
<table border="0" cellspacing="0" cellpadding="0">
<tr>
<td align="left" valign="top">

<table border="0" cellspacing="0" cellpadding="0">
<tr>
<TD>
<P><IMG SRC="/securita/images/top_left_border.gif" alt=""></P>
</TD>
</tr>
<tr>
<td class="rand-links" >
<A HREF="/securita/pages/index.jsp"><IMG style="border-style:none;" SRC="/se
</td>
</tr>
<tr>
<td class="rand-links">
<IMG SRC="/securita/images/empty.gif" ALT="">

```

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> ...



```
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
```

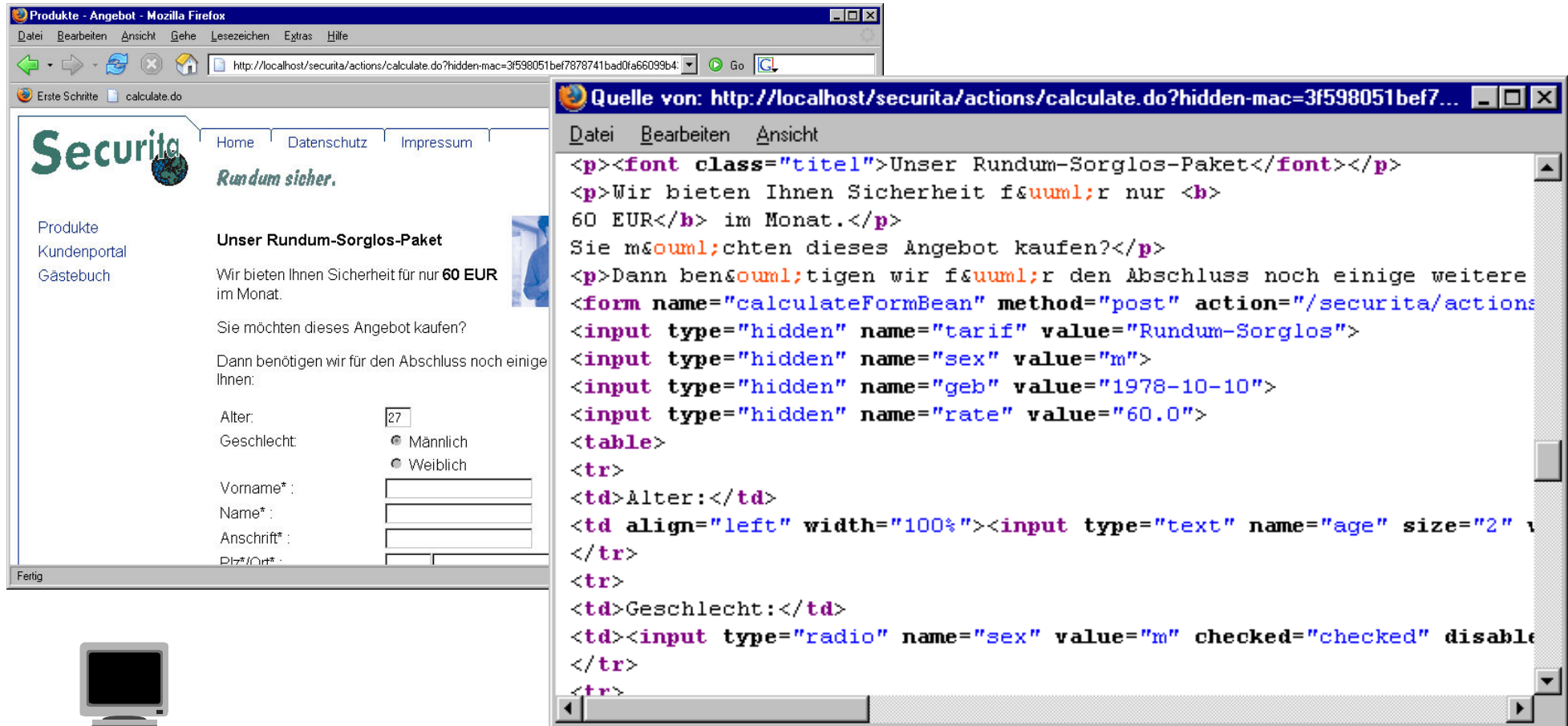
```
Keep-Alive: 300
```

```
Connection: keep-alive
```



Client

Hidden Field Manipulation



The screenshot shows a Mozilla Firefox browser window displaying a web page titled 'Produkte - Angebot - Mozilla Firefox'. The page content includes a navigation menu with 'Home', 'Datenschutz', and 'Impressum'. The main heading is 'Securita Rundum sicher.' followed by 'Unser Rundum-Sorglos-Paket'. The text describes a security package for 60 EUR per month. Below the text is a form with the following fields:

- Alter:
- Geschlecht: Männlich Weiblich
- Vorname*:
- Name*:
- Anschrift*:
- Plz*/Ort*:

The source code window shows the following HTML code for the form:

```
<form name="calculateFormBean" method="post" action="/securita/actions/abschluss.do?hidden-mac=3f598051bef7878741bad0fa66099b4">
  <input type="hidden" name="tarif" value="Rundum-Sorglos">
  <input type="hidden" name="sex" value="m">
  <input type="hidden" name="geb" value="1978-10-10">
  <input type="hidden" name="rate" value="60.0">
  <table>
    <tr>
      <td>Alter:</td>
      <td align="left" width="100%"><input type="text" name="age" size="2" value="27">
    </tr>
    <tr>
      <td>Geschlecht:</td>
      <td><input type="radio" name="sex" value="m" checked="checked" disabled=""> Männlich
        <input type="radio" name="sex" value="f"> Weiblich
      </td>
    </tr>
    <tr>
      <td>Vorname:</td>
      <td><input type="text" name="first_name">
    </tr>
    <tr>
      <td>Name:</td>
      <td><input type="text" name="last_name">
    </tr>
    <tr>
      <td>Anschrift:</td>
      <td><input type="text" name="address">
    </tr>
    <tr>
      <td>Plz/Ort:</td>
      <td><input type="text" name="zip">
    </tr>
  </table>
  <input type="submit" value="Abschließen">
</form>
```

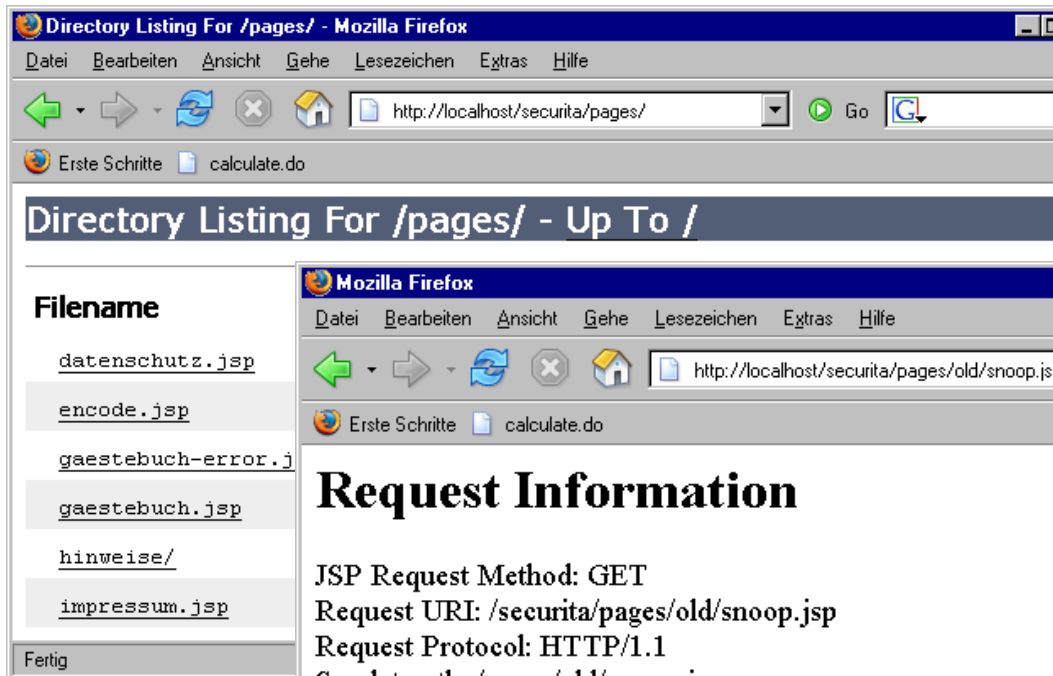


Client

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

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

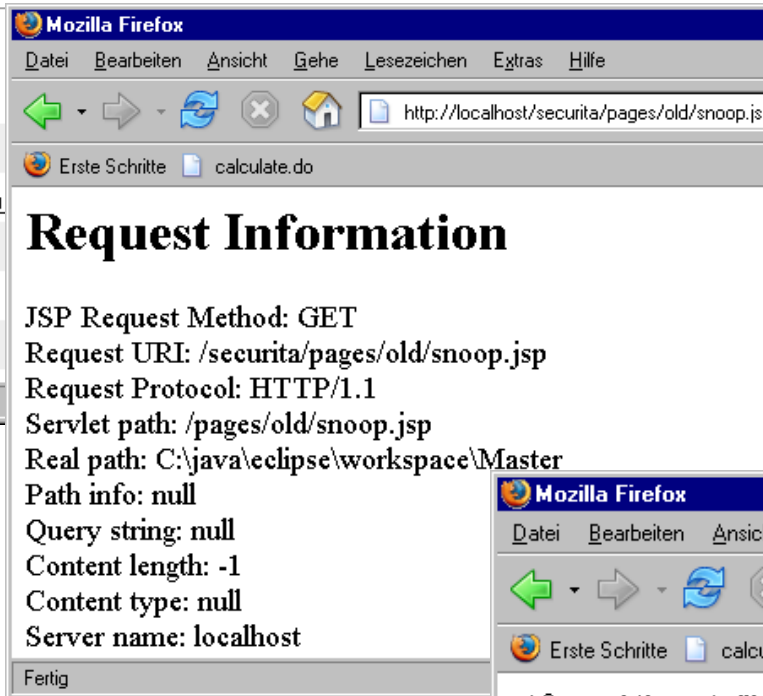
Forceful Browsing



Directory Listing For /pages/ - Up To /

Filename
datenschutz.jsp
encode.jsp
gaestebuch-error.jsp
gaestebuch.jsp
hinweise/
impressum.jsp

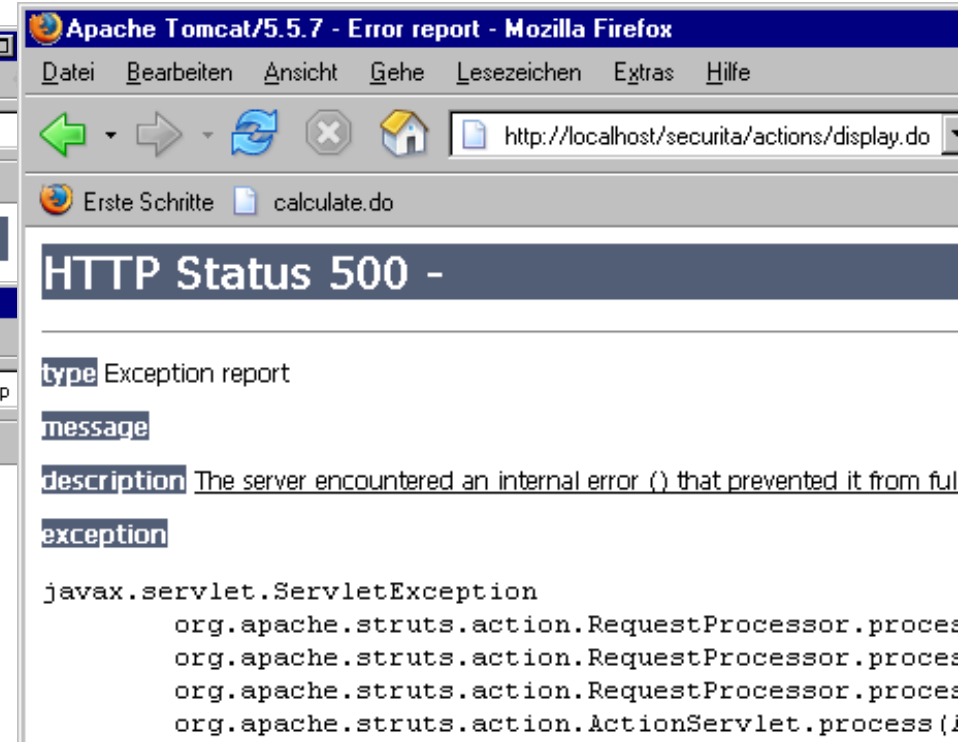
Fertig



Request Information

JSP Request Method: GET
Request URI: /securita/pages/old/snoop.jsp
Request Protocol: HTTP/1.1
Servlet path: /pages/old/snoop.jsp
Real path: C:\java\eclipse\workspace\Master
Path info: null
Query string: null
Content length: -1
Content type: null
Server name: localhost

Fertig



Apache Tomcat/5.5.7 - Error report - Mozilla Firefox

HTTP Status 500 -

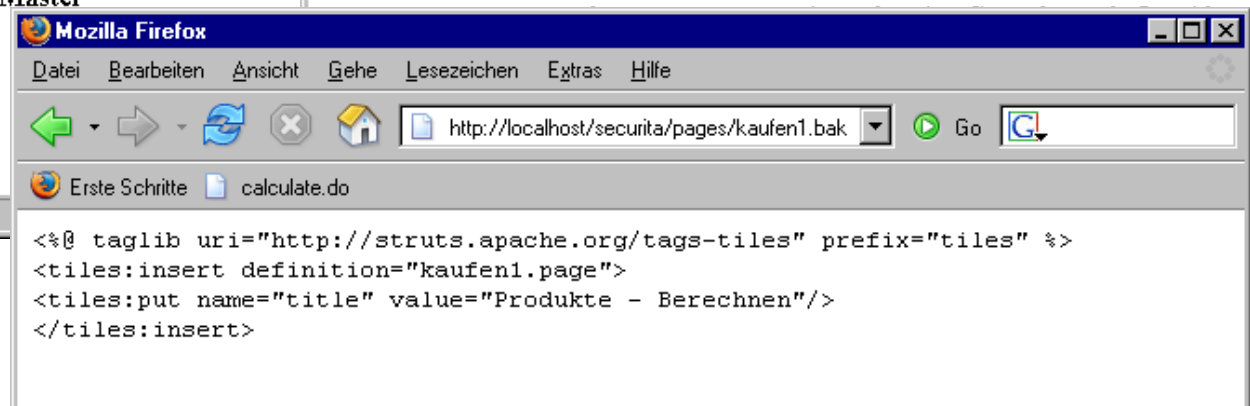
type Exception report

message

description The server encountered an internal error () that prevented it from ful

exception

```
javax.servlet.ServletException  
    org.apache.struts.action.RequestProcessor.process  
    org.apache.struts.action.RequestProcessor.process  
    org.apache.struts.action.RequestProcessor.process  
    org.apache.struts.action.ActionServlet.process()
```



```
<%@ taglib uri="http://struts.apache.org/tags-tiles" prefix="tiles" %>  
<tiles:insert definition="kaufen1.page">  
<tiles:put name="title" value="Produkte - Berechnen"/>  
</tiles:insert>
```

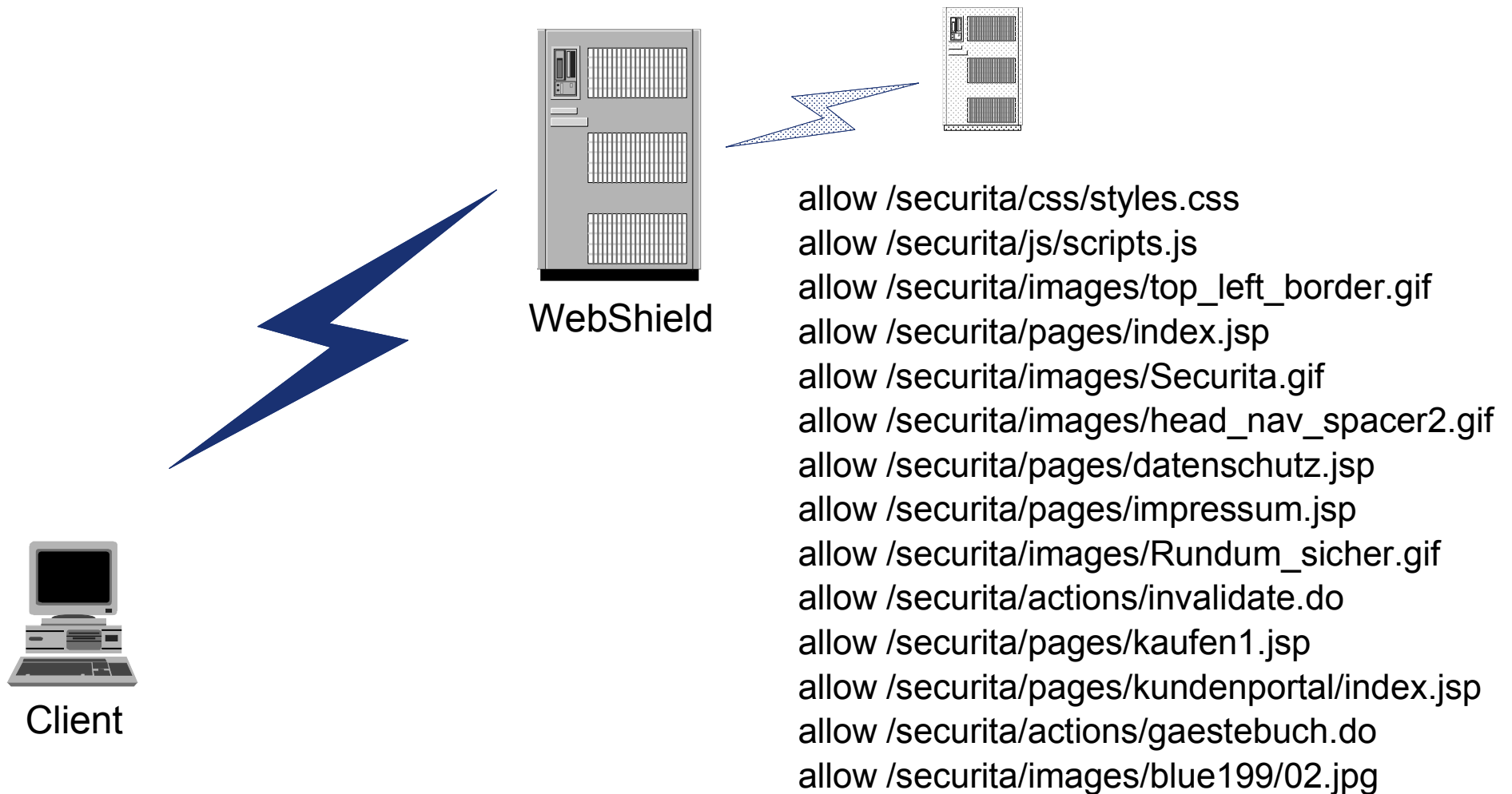


Client

Web-Application Firewall

WebShield

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

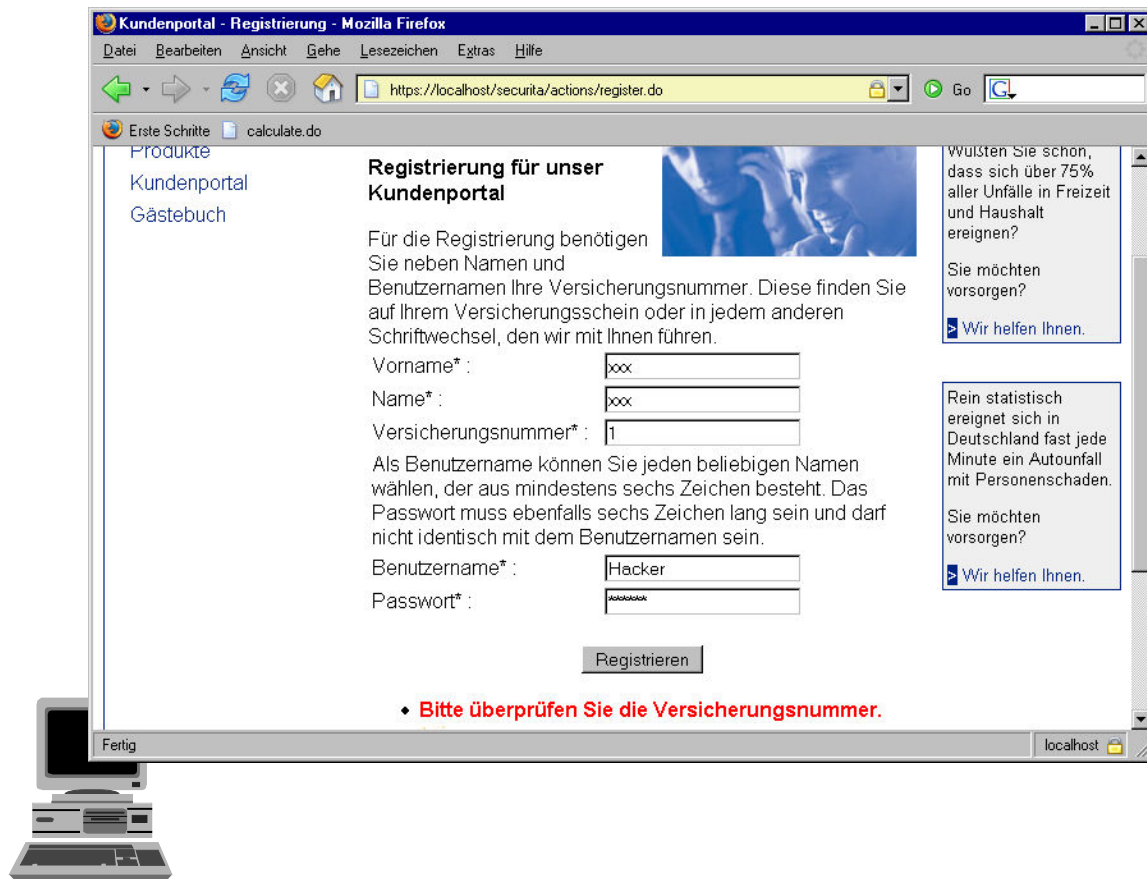


Fragen

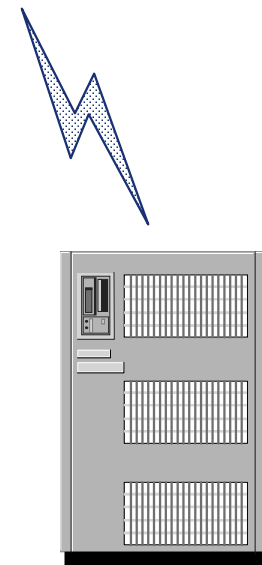
????????????????

Injection Flaw

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



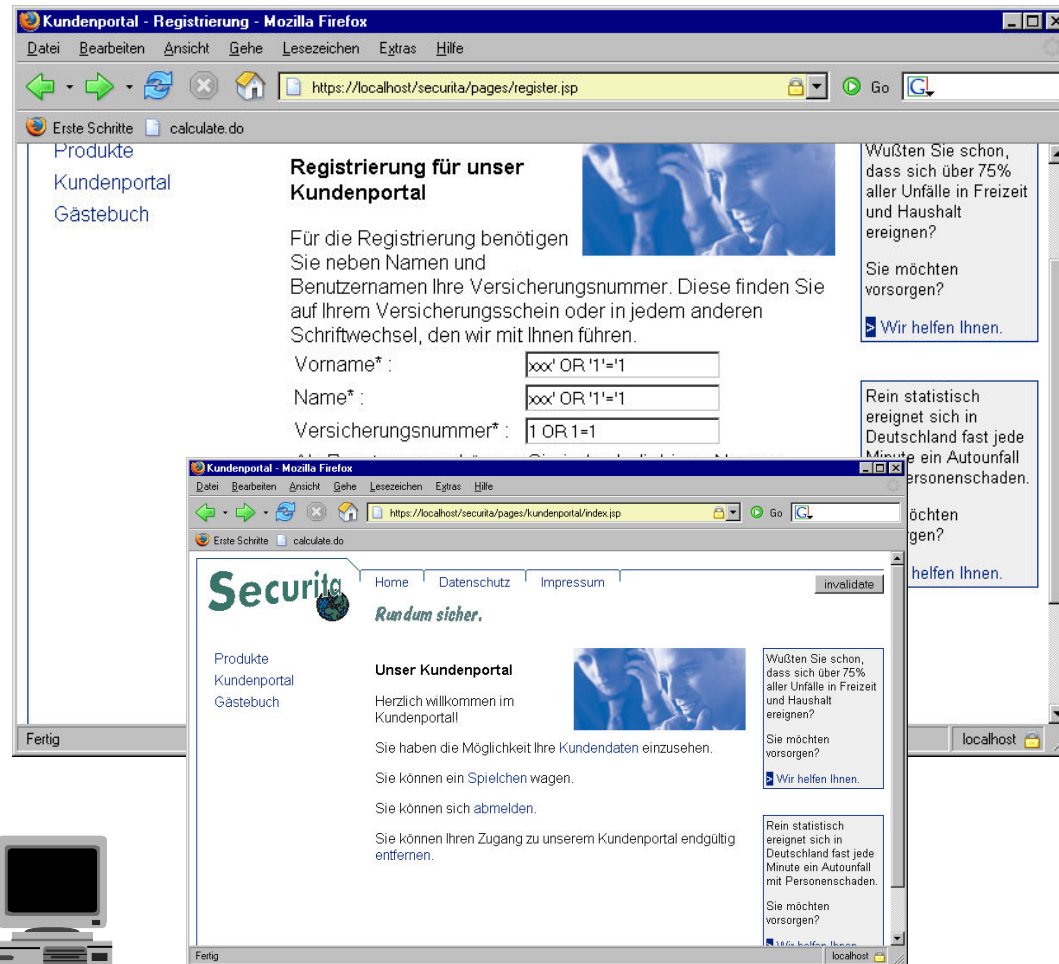
Client



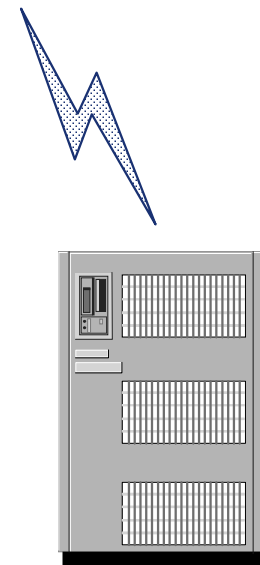
Datenbank

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

Injection Flaw



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'
```