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

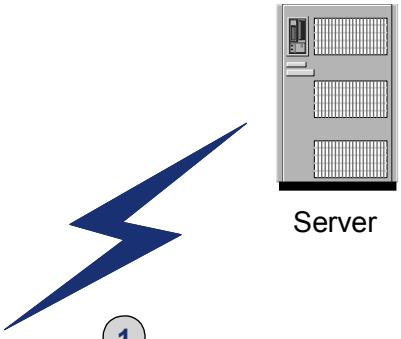
Vortrag zum Industrieseminar der FH Trier
Hans-Jürgen Stemmer
23.06.2006

Inhalt

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

- Internet
- HTML
- HTTP
- Demonstration
- Web-Server
- Application-Server
- Datenbank
- Web-Application Firewall

Internet



Server

Der Server wertet die Anfrage aus und sendet eine Antwort an den Client (Response).

2

1

Client

Der Client sendet eine Anfrage an den Server (Request).

3

Der Client wertet die Antwort aus bzw. stellt sie dar (HTML).

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

HTML

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

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="">
```

HTML

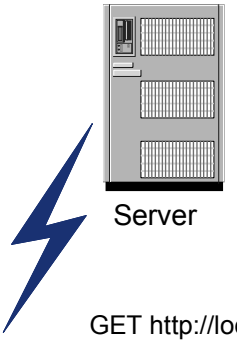
FACHHOCHSCHULE **TRIER**
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences

- Auszeichnungssprache für Internetseiten
- Sprachauszeichnungen (Tags) führen zu einem Kontextwechsel
- Verlinkungen führen zu einem Netzwerk von Internetressourcen
- Verlinkungen können auf beliebige (andere) Server verweisen
- IMG-Tag mit SRC-Attribut erzeugt automatisch einen Request, in dem das Bild geladen wird
- A-Tag mit HREF-Attribut erzeugt einen Request, wenn der Anwender den Link anklickt
- Auch Formulare arbeiten (beim Auslösen) mit Links. Durch Java-Script-Befehle kann ein Formular auch automatisch ausgelöst werden.
- Der Anwender wird sich den Quelltext einer Seite in der Regel nicht ansehen und Folgerequests (z.B. durch IMG-Tags) nicht bewußt wahrnehmen.

HTTP

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

Hyper-Text-Transfer-Protocol



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

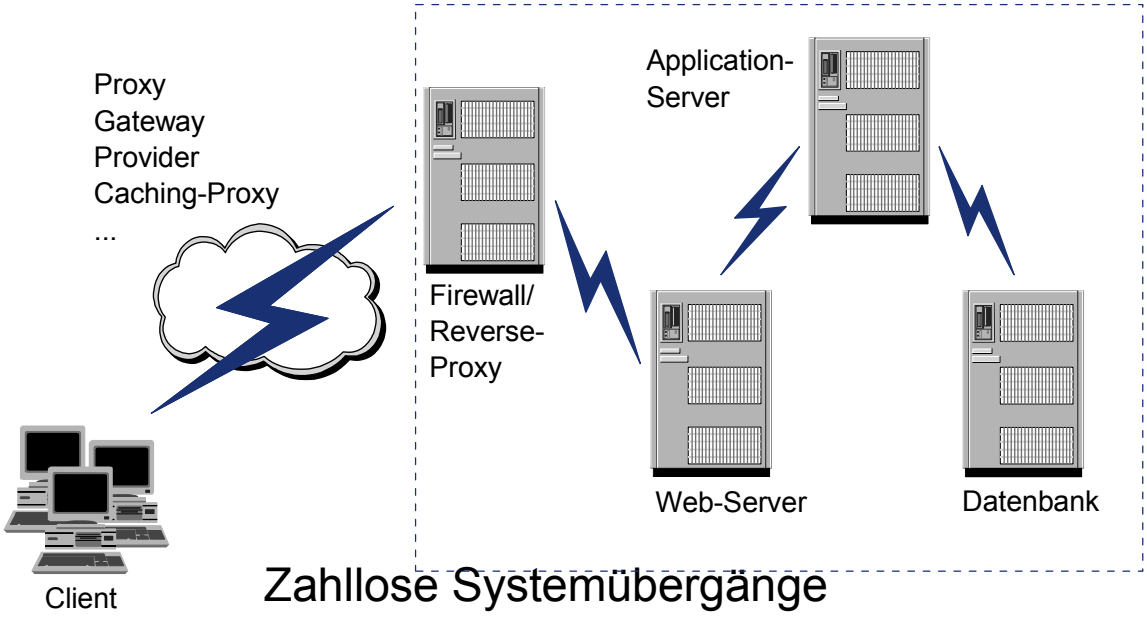
HTTP

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

- Klartextprotokoll, d.h. der Client sendet und empfängt Textnachrichten
- HTTPS verhindert das Abhören/Mitlesen einer Nachricht auf dem Weg vom Client zum Server (oder zurück), betrifft das HTTP-Protokoll darüber hinaus aber nicht.
- Alle Parameter (aus Formularen und in der URL) werden in Textform übermittelt.
- GET-Anfragen übertragen Parameter in der URL (schlecht)
- POST-Anfragen übertragen Parameter im Rumpf der Anfrage (besser)

Internet

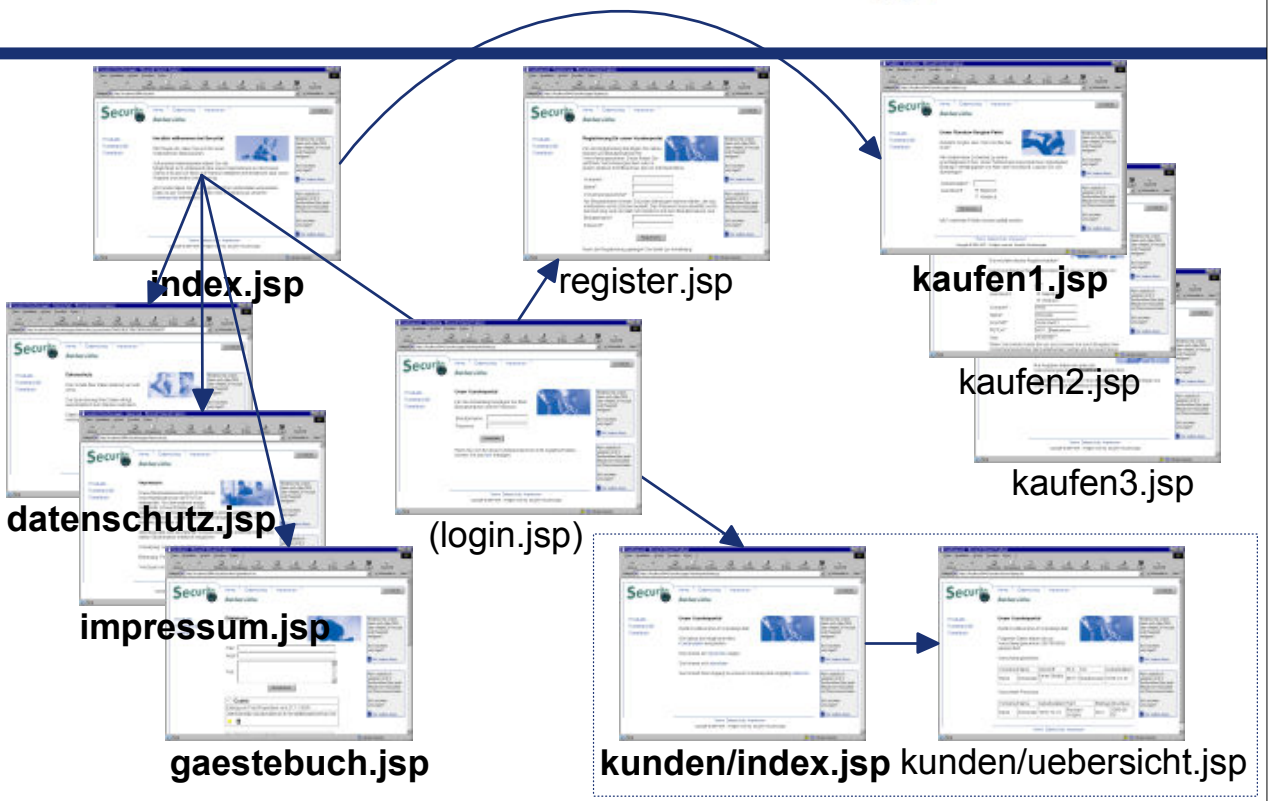
FACHHOCHSCHULE TRIER
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences



Zahllose Systemübergänge

Demonstration

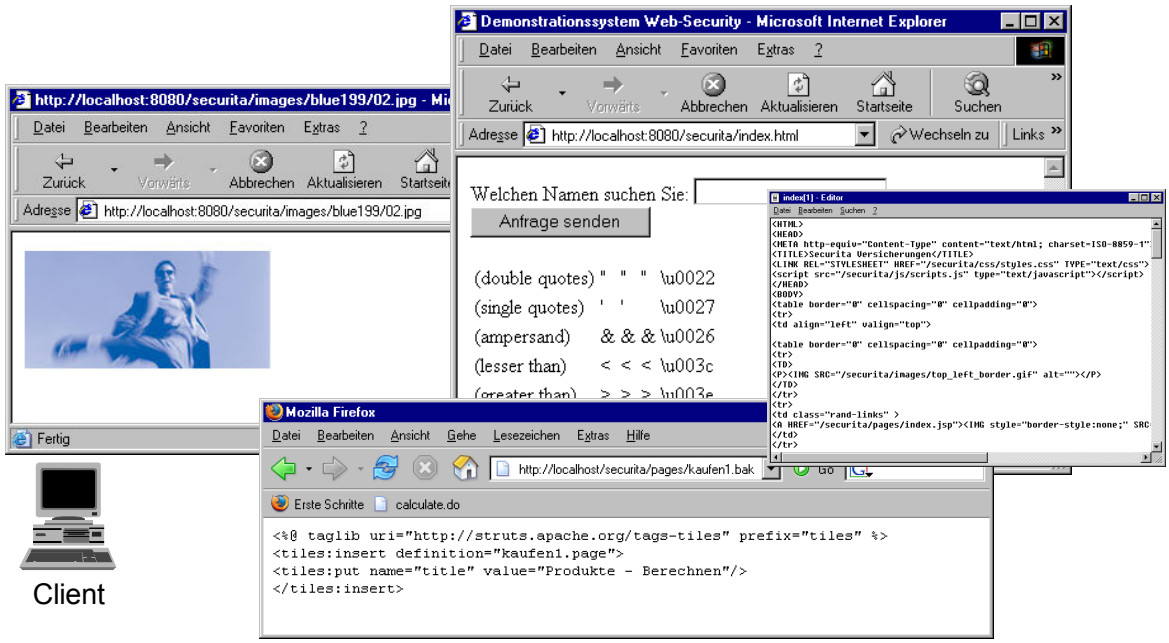
FACHHOCHSCHULE TRIER
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences



Web-Server

Forceful Browsing

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



Web-Server

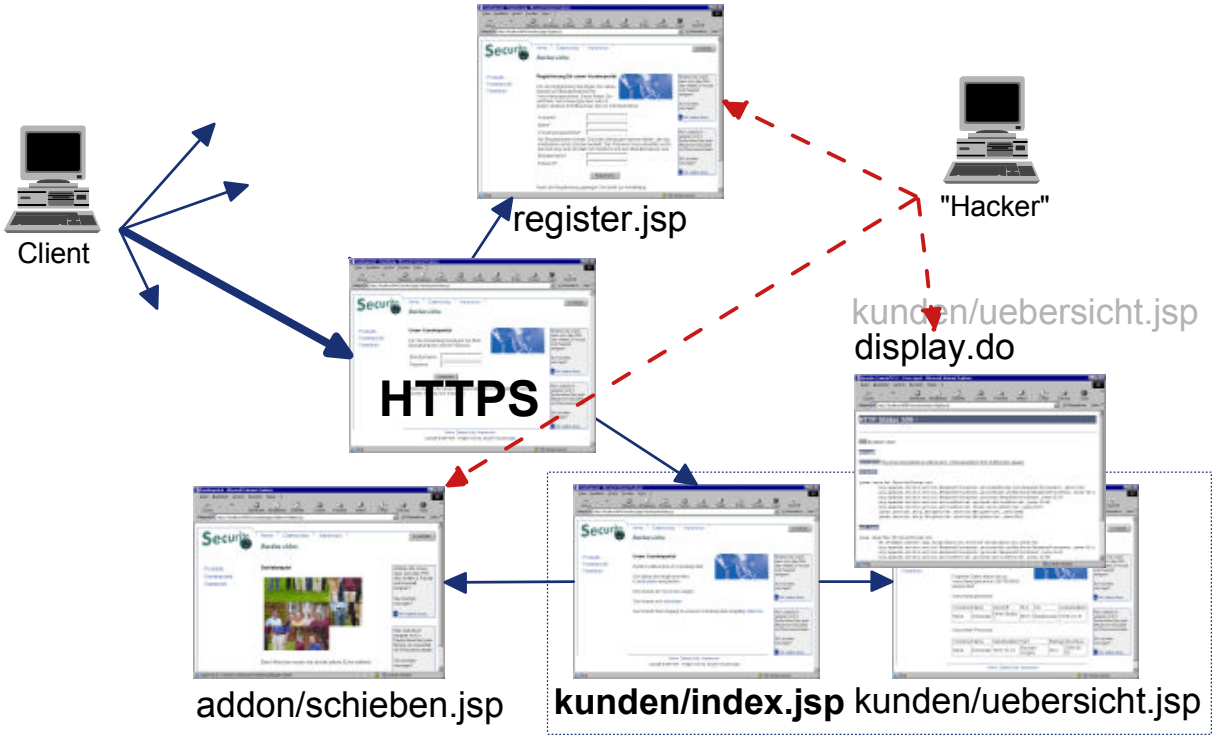
FACHHOCHSCHULE TRIER
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences

- Jede Ressource, deren Pfad (URL) der Web-Server auflösen kann, wird an den Aufrufer geschickt.
  - z.B. http://localhost:8080/securita/images/blue199/02.jpg
- Zu Anfragen, die der Web-Server nicht bedienen kann, erzeugt er eine Meldung (z.B. 404 Not Found).
- Verzeichnisse für Webseiten sollen nur Ressourcen enthalten, die für den Betrieb erforderlich sind.
- Sicherheitskopien, Test- und Konfigurationsfiles, ... sollen nicht auf das Produktivsystem kopiert werden. (Diese werden u.U. anderes verarbeitet als die Originale. *.bak wird z.B. nicht durch das JSP-Servlet compiliert.)
- Das Verzeichnis WEB-INF wird durch den Web-Server geschützt.

Web-Server

Broken Access Control

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



Web-Server

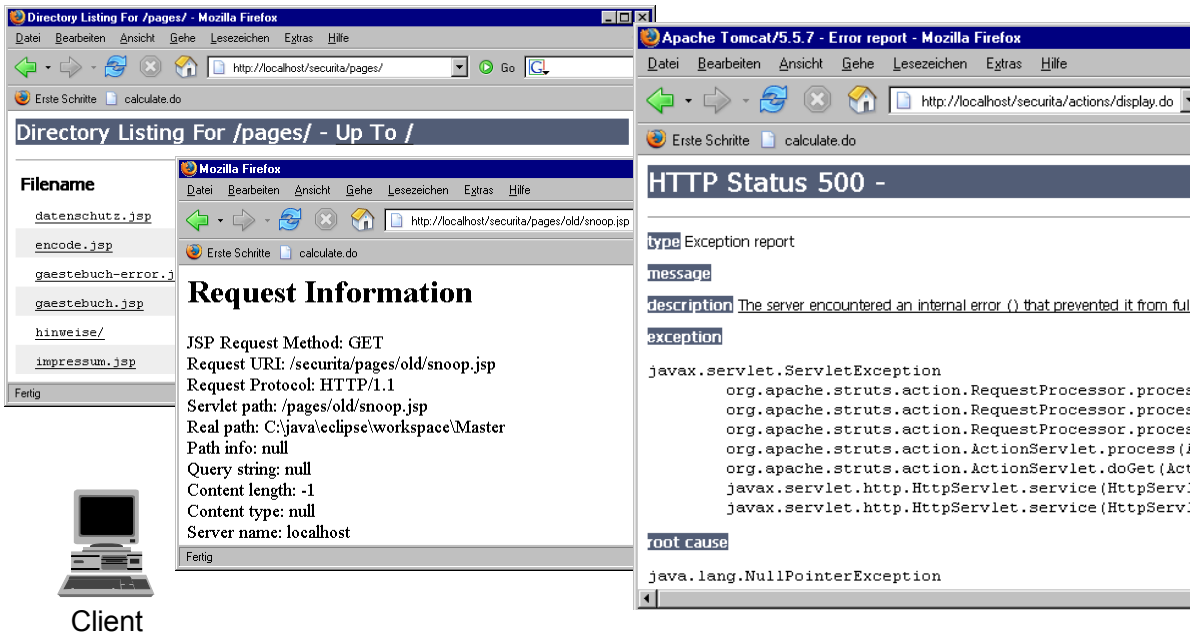
FACHHOCHSCHULE TRIER
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences

- Für den geschützen Bereich kunden/* ist eine Anmeldung (login) erforderlich.
- Die Anmeldung erzwingt einen Protokollwechsel zu HTTPS.
- Ressourcen (URLs), die von geschützten Seiten verlinkt werden, sollten i.d.R. ebenfalls geschützt sein.
- Teile der Seiten, die aus dem geschützten Bereich verlinkt sind, können (wenn die URL bekannt ist) auch ohne Anmeldung aufgerufen werden.
- Der Weg eines Anwenders/Aufrufers durch eine Anwendung, ist nicht vorhersehbar und (ohne Programmierung) nicht steuerbar.

Application-Server

Forceful Browsing, Insecure Configuration, Improper Error Handling

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



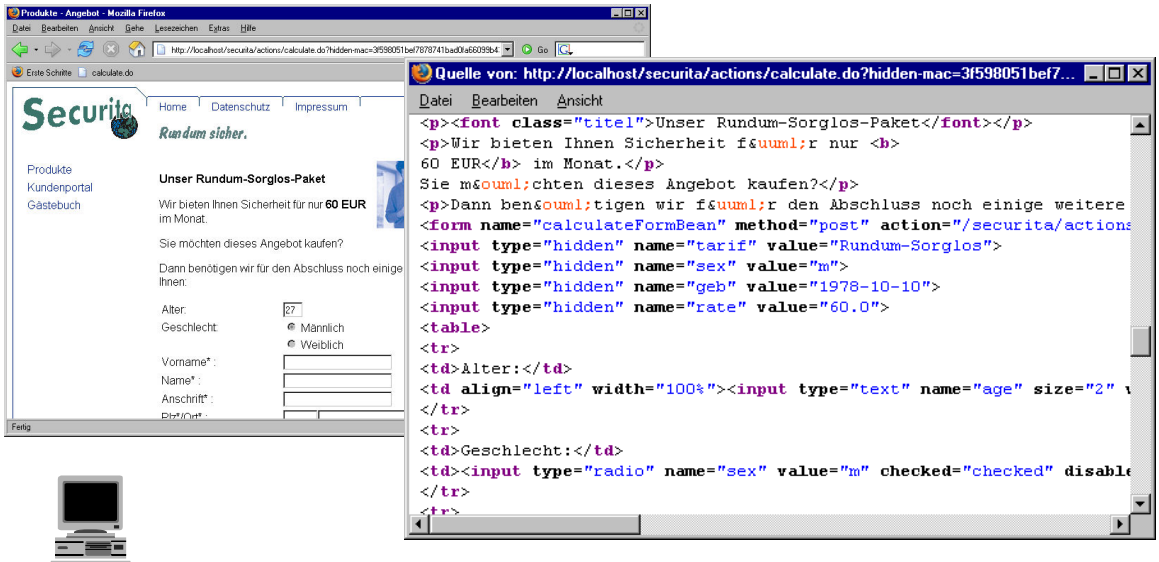
Application-Server

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

- In der Konfiguration wird festgelegt, welche Anfragen (URLs) der Web-Server zur Bearbeitung an den Application-Server weiterleitet.
- Ein JSP-Servlet erzeugt zu allen *.jsp-Seiten ein Servlet (=Java-Programm).
- Das Default-Servlet erzeugt zu Pfaden, die auf / enden, ein Verzeichnislisting.
- Das Invoker-Servlet ruft Servlets statt über einen logische Namen über den qualifizierten Klassennamen des Java-Programmes direkt auf.
- Testprogramme, Testzugänge, Testseiten, ... nicht auf das Produktivsystem kopieren.
- Fehlermeldungen des Servers sollen nicht ungefiltert an den Client geschickt werden. Stack-Traces verraten einem Angreifer viel über das System und können u.U. Eingaben für das Invoker-Servlet sein.

Application-Server

Hidden Field Manipulation, Parameter Tampering, Web-Trojaner



Client

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

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

Application-Server

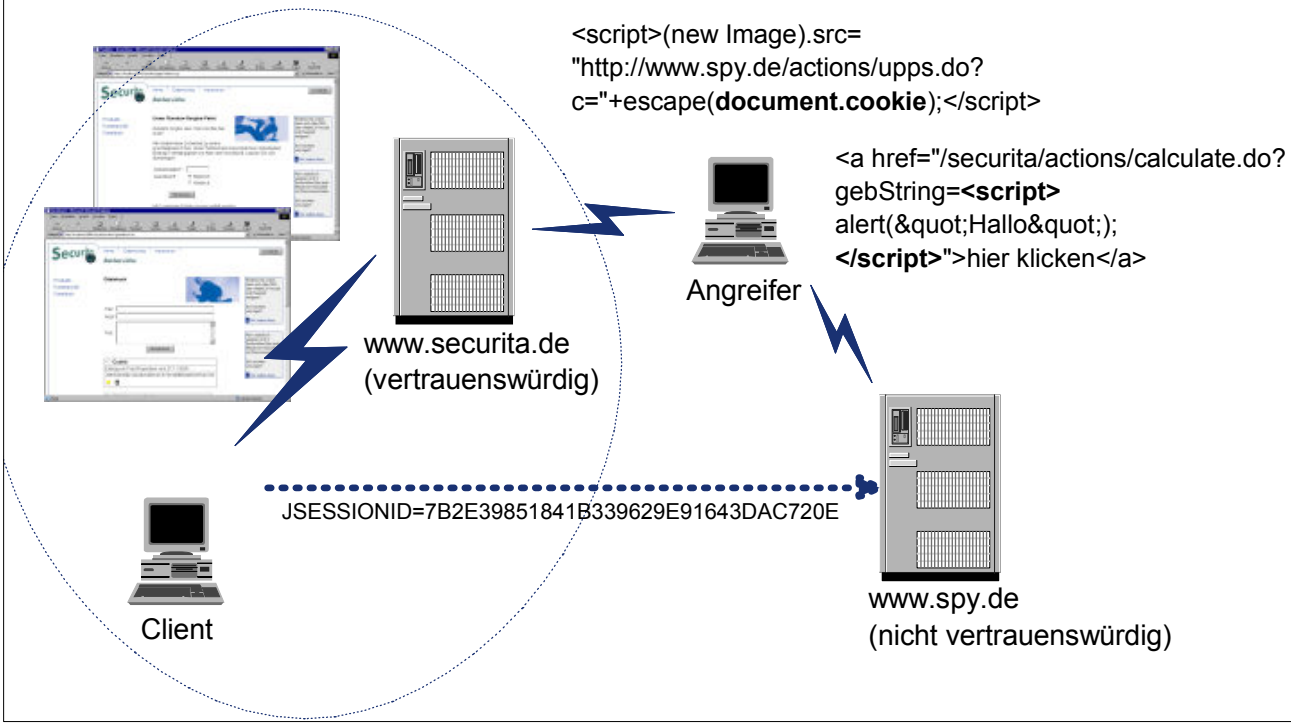
FACHHOCHSCHULE TRIER
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences

- Hidden Values können genutzt werden, um das Speichern von Sitzungsdaten auf dem Server zu umgehen. Hidden Values werden durch den Client als einfache Parameter übertragen und sind nicht geschützt.
- Eingaben in HTML beschränken
  - Auswahllisten/-felder, maxlength-Attribut verwenden
  - Nur solche Daten an den Client schicken, die dort auch benötigt werden
  - Wichtige Daten in einer Session (auf dem Server) ablegen
- Werte, die vom Client gesendet werden, müssen (trotzdem) immer(!) überprüft/validiert werden.
- Wenn ein einzelner Aufruf (mit Parametern) einen Verkauf etc. auslöst, kann dieser Aufruf, eingebunden in beliebige (fremde) Seiten, mißbraucht werden, um von dort besagte Transaktion zu triggern, ohne dass der Aufrufer sich dessen bewußt wird (Web-Trojaner).

Application-Server

Cross-Site-Scripting XSS

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



Application-Server

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

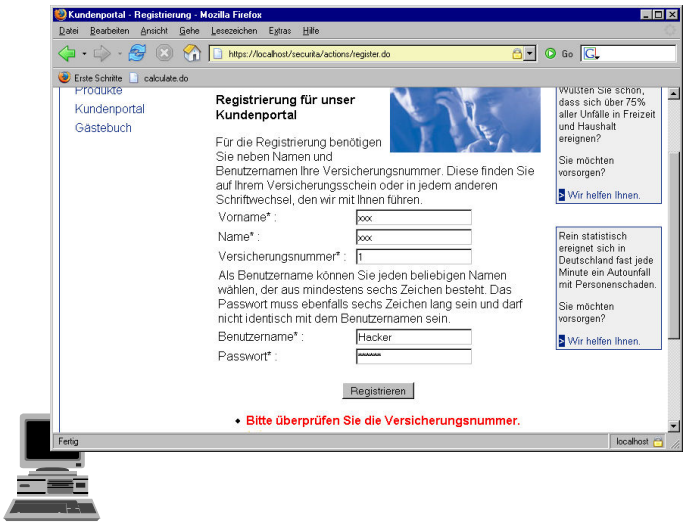
- Jede Seite, die der Client von www.securita.de lädt, wird im Kontext dieser Domäne ausgeführt. Scripte können Cookies dieses Kontextes lesen.
- Gelingt es einem Angreifer bösartige Inhalte (z.B. Java-Script) in der Seite einer fremden Domäne einzubinden, führt der Browser des Opfer, beim Laden der Seite von dieser für ihn vertrauenswürdigen Domäne, Code des Angreifers im Kontext dieser Domäne aus.
- Niemals Daten, die vom Client gesendet werden, in der Ausgabeseite ungefiltert ausgeben.
- Ausgaben in HTML-Seiten immer maskieren (z.B. < zu <)
- Vorsicht bei HTML-e-Mails oder Verweisen in Gästebüchern, die zum Anklicken aufrufen
- Auch wenn die in der Statuszeile angezeigte URL zu einem Link keinen sicheren Schutz bietet, sollte sie vor dem Anklicken überprüft werden.

Datenbank

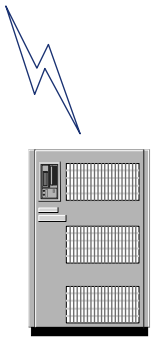
Injection Flaw

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



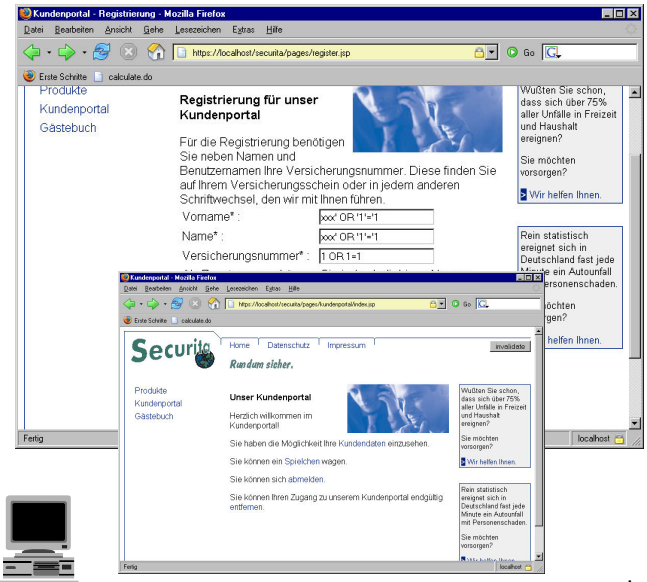
Datenbank

select * from vertrag where versnr=1

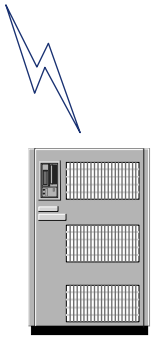
Datenbank

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'

Datenbank

- Eingabedaten bilden gemeinsam mit konstanten Anteilen eine Datenbankanfrage
- Der Angreifer wählt die Eingabe so, dass korrekte aber entfremdete SQL-Statements entstehen. So wird die Bedingung *where versnr=1 OR 1=1* immer wahr sein, da der zweite Ausdruck allgemeingültig ist.
- Eingabedaten einschränken (insbesondere Typ und Länge)
- Meta-Daten berücksichtigen (insbesondere " und ')
- Prepared statements verwenden (typsicher)
- Keine Fehlermeldungen der Datenbank an den Client senden

Web-Application Firewall

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

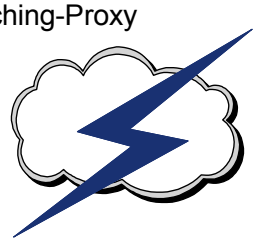
- Ausgehend von der Startseite ergibt sich ein Netz von URLs, da in jeder Seite alle URLs, die ein Anwender anwählen kann, stehen (vgl. Demonstration).
- Ein Teil der Felder in einem HTML-Formular kann Angaben über Länge und (erlaubte) Werte enthalten.
- Hidden-Values werden im Request wieder übertragen und dürfen dort nicht verändert sein (Einschränkung: JavaScript).
- Scripte beginnen in der Regel mit <script> oder javascript:
- Fehlerseiten sind am Status des Response zu erkennen (z.B. 404, 500, ...)

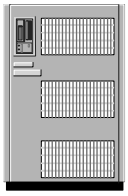
Web-Application Firewall

URL

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

Proxy
Gateway
Provider
Caching-Proxy
...





Web-Shield

Client

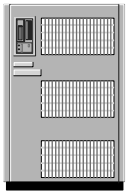
Parsen der Ausgabe, Erstellen einer white-list
allow /securita/css/styles.css
allow /securita/js/scripts.js
allow /securita/images/top_left_border.gif
allow /securita/pages/index.jsp
allow /securita/images/Securita.gif
allow /securita/images/head_nav_spacer2.gif
allow /securita/pages/datenschutz.jsp
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

Web-Application Firewall

Input

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

Proxy
Gateway
Provider
Caching-Proxy
...



Web-Shield

Client

Eingabevalidierung
<input type="hidden" value="X">
<input... readonly="1">
<input... maxlenght="30" >
<input type="radio" value="X">
<input type="radio" value="Y">
<select name="auswahl">
<option>A</option>
<option>B</option>
</select>
javascript:, <script>, onload, ...

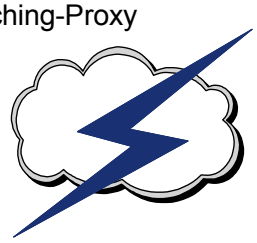
MAC (Message Authentication Code)
/securita/actions/abschluss.do
tarif+sex+geb+rate
hidden-mac=fa74138cc61bd5b4df6d51bbce3a97fcf5136469

Web-Application Firewall

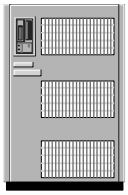
Output

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

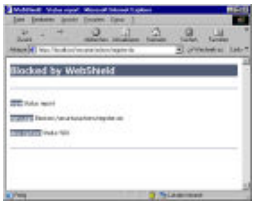
Proxy
Gateway
Provider
Caching-Proxy
...



Client



Web-Shield



200 OK
302 Moved Temporarily
401 Unauthorized
404 Not Found
500

Fragen

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

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

h.stemmer@gmx.de