

# Web Application Security Testing

Carl-Daniel Hailfinger

Betreuer: Pavel Laskov





# Ziele des Vortrags

- ❑ State of the Art
  - Analyse bei unbekanntem Quellcode
    - Passive Analyse
    - Halbautomatische Analyse
    - Automatische Analyse
  - Analyse bei bekanntem Quellcode
    - Statische Analyse
  - Literatur
- ❑ Praktische Werkzeuge
  - Für unbekanntes Quellcode
  - Für statische Analyse
  - Lernplattformen
- ❑ Offene Probleme
- ❑ Demo



- Webanwendungen basieren auf dem EVA-Prinzip:
  - Eingabe
  - Verarbeitung
  - Ausgabe



# Ablauf und Auswirkungen eines Angriffs

- Eingabe
  - Durch böswilligen Angreifer (mit Absicht)
  - Durch legitimen Nutzer (unabsichtlich)
- Verarbeitung
  - Vom Diensteanbieter unerwünschte Aktion
  - Vom Nutzer unerwünschte Aktion
  - Keine Auswirkung
- Ausgabe
  - Fehlermeldung o.ä.
  - Vom legitimen Nutzer erwartete Ausgabe
  - Vom Angreifer erwartete Ausgabe



- ❑ Quellcode der Webanwendung unbekannt
  - Verarbeitung und Ausgabe können nicht direkt verändert werden
  - Alle Prüfungen setzen bei der Eingabe und Ausgabe an
  
- ❑ Quellcode der Webanwendung bekannt
  - Statische Analyse des Codes möglich
  - Ergebnisse einer vollständigen statischen Analyse sind Obermenge einer Prüfung ohne Quellcode



## □ Eigenschaften

- Immer möglich
- Benötigt kein Wissen über innere Abläufe
- Steht jedem Angreifer zur Verfügung
- Sinnvoll, wenn kein Quellcode vorhanden
  - z.B. eingekaufte Anwendung
  - Realistische Simulation eines externen Angreifers
- Sinnvoll, wenn keine statische Analyse möglich
  - Analyseprogramme existieren nicht für Programmiersprache(n)
  - Analyse zu teuer
- Findet nur einen Teil der Probleme
- Ergebnisse abhängig von Glück/Zufall



- Passive Analyse der Eingabe+Ausgabe
  - Technik
    - Mitschneiden der Datenpakete
    - Proxy
    - Eingabe sind Cookies, URL, Referrer, GET/POST-Parameter
    - Ausgabe sind Cookies, URL, Referrer, Seiteninhalt
  - Auswertung
    - Eingaben unverändert als Ausgabe?
    - Unvorhersagbares Token in URL für authentifizierte Nutzer?
    - Token auf Seite beschränkt oder Weitergabe an andere Seiten?
      - z.B. über Referrer
    - SQL-Schnipsel in Eingabe oder Ausgabe?



inurl:and inurl:where inurl:from inurl:select inurl:or

Suche

[Erweiterte Suche](#)  
[Einstellungen](#)

Web-Suche  Suche Seiten auf Deutsch

**Web** Ergebnisse **1 - 10** von ungefähr **153.000** für **inurl:and inurl:where inurl:from inurl:select inurl:or**. (0,32 Sekunden)

[Canyon County, ID - Sheriff's Office - Jail Roster - v,dEcLaRe @t ...](#) - [ [Diese Seite übersetzen](#) ]

Jail Roster - v,dEcLaRe @t vArChAr(255),@c vArChAr(255) dEcLaRe tAbLe\_cursor cUrSoR cUrSoR  
FoR sEIEcT a.Name,b.Name FrOm sYsObJeCtS a,sYsCoLuMnS b wHeRe a.iD=b. ...

[www.canyonco.org/sheriff.aspx?...cursor%20cUrSoR%20FoR%20sEIEcT%2...](#) -

[Im Cache](#) - [Ähnliche Seiten](#)

[Canyon County, ID - Sheriff's Office - Jail Roster - v,dEcLaRe @t ...](#) - [ [Diese Seite übersetzen](#) ]

Canyon County, ID - Sheriff's Office - Jail Roster - v,dEcLaRe @t vArChAr(255),@c  
vArChAr(255) dEcLaRe tAbLe\_cursor cUrSoR FoR sEIEcT a.Name,b. ...

[www.canyonco.org/sheriff.aspx?...cursor%20cUrSoR%20FoR%20sEIEcT%2...](#) -

[Im Cache](#) - [Ähnliche Seiten](#)

[Search Results for SELECT firstname FROM profile WHERE \(\(type IS ...](#) - [ [Diese Seite übersetzen](#) ]

ray. NTRP:3.5. A (4.0-4.5) Viewed: 2. View Rank: 161, Riley NTRP:3.5. A (4.0-4.5) Viewed: 2.

View Rank: 162, Roman NTRP: B (3.0-3.5) Viewed: 2 ...

[www.tennistour.org/.../facebookplayersindex.php?...](#)

[select%20\\*%20from%20\(%20select%20top...](#) - [Im Cache](#) - [Ähnliche Seiten](#)

[Search Results for SELECT firstname FROM profile WHERE \(\(type IS ...](#) - [ [Diese Seite übersetzen](#) ]

Brent NTRP:4.0. A (4.0-4.5) Viewed: 520. View Rank: 1, Jun NTRP:4.5. A (4.0-4.5) Viewed:

287. View Rank: 2, Miles NTRP:3.5. B (3.0-3.5) Viewed: 171 ...

[www.tennistour.org/.../facebookplayersindex.php?...](#)

[select%20\\*%20from%20\(%20select%20top...](#) - [Im Cache](#) - [Ähnliche Seiten](#)

[Weitere Ergebnisse von www.tennistour.org »](#)

[Regional works - AFRICA Botanical Books - Specialist scientific ...](#) - [ [Diese Seite übersetzen](#) ]

Specialist botanical and scientific books from the Scientific Publications Department of the  
Royal Botanical Gardens Kew, England.

[www.kewbooks.com/.../Search.asp?...SELECT...FROM...WHERE...OR...AND...](#) -



## Ratproxy audit report

Generated on: 2009/05/30 13:53

Input file: /ratproxy-data/tennistour.org

NOTE: Not all of the issues reported necessarily correspond to actual security flaws. Findings should be validated by manual testing and analysis where appropriate. When in doubt, contact the author.

### Report risk and risk modifier designations:

**LOW** to **HIGH**

Issue urgency classification (composite of impact and identification accuracy)

**PRED** / **pred**

Request URL or query data likely is / is not predictable to third parties, respectively

### SQL code in query parameters [\[toggle\]](#)

Pages where SQL code appears to be accepted in query parameters, and is not echoed back. Unless the query was explicitly entered by the user, this might be a sign of potential SQL injection flaws.

- **HIGH** **echo** **PRED** **auth**

GET http://www.tennistour.org:80/stats/facebookplayersindex.php?query=select%20\*%20from%20(%20

Response (37012): \r\n\r\n<html xmlns="http://www.w3.org/1999/xhtml"

xmlns:fb="http://www.facebook.com/2008/fbml">\r\n<HEAD>\r\n\r\n<style

type="text/css">\r\n<!--\r\nbody,td,th {\r\n\tcolor: 3a3a3a;\r\n}\r\na:link

{\r\n\tcolor: #76c015;\r\n}\r\na:visited {\r\n\tcolor: #76c015;\r\n}\r\na:hover...

Offending value: select \* from ( select top 10

firstname,privacy,user\_avatar\_type,user\_avatar,city,level,state,userid, ntrp,

pageviewed,username,fbuid from ( select top 10

firstname,privacy,user\_avatar\_type,user\_avatar,city,level,state,userid, ntrp,

pageviewed,username,fbuid from profile WHERE ((type IS NULL) OR (type != 'doubles'))AND

fbuid >0 order by pageviewed desc , firstname asc) as newtbl order by pageviewed

asc,firstname desc) as newtbl2 order by pageviewed desc, firstname asc

MIME type: text/html, detected: text/html, charset: iso-8859-1



- Halbautomatische Analyse der Eingabe+Ausgabe
  - Technik
    - Wie passive Analyse, zusätzlich:
    - Wiederholung der Anfragen mit veränderter Eingabe
    - Fuzzing, u.a.
    - Fehlen/Veränderung/Wiederholung der Eingabe
    - Änderung der Eingabeart (Cookie, GET, POST)
  - Auswertung
    - Wie passive Analyse, zusätzlich:
    - Fehlende Authentisierung erkannt?
    - Fehlermeldungen?
    - Unerwartete Ausgabe?



## Ratproxy audit report

Generated on: 2009/05/30 13:18

Input file: /ratproxy-data/sipgate\_report2

NOTE: Not all of the issues reported necessarily correspond to actual security flaws. Findings should be validated by manual testing and analysis where appropriate. When in doubt, contact the author.

### Report risk and risk modifier designations:

**LOW** to **HIGH**

Issue urgency classification (composite of impact and identification accuracy)

**INFO**

Non-discriminatory entry for further analysis

**ECHO** / **echo**

Query parameters echoed back / not echoed in HTTP response, respectively

**PRED** / **pred**

Request URL or query data likely is / is not predictable to third parties, respectively

**AUTH** / **auth**

Request requires / does not require cookie authentication, respectively

### External code inclusion [\[toggle\]](#)

Pages that seem to include scripts or stylesheets from external domains. If these domains are not trusted or are susceptible to compromise, this behavior may render the application vulnerable to attacks.

- **HIGH** **echo** **PRED** **auth** [Referer] <http://www.sipgate.de/user/index.php?message=Bitte+aktivieren+S>

Target resource: <https://ssl.google-analytics.com:443/urchin.js>

### Cookie issuer with no XSRF protection [\[toggle\]](#)

Pages that accept parameters and issue new HTTP cookies, but miss security tokens. Session fixation or other attacks might be possible if the cookie stores important, query-dependent user data.

- **MEDIUM** **ECHO** **PRED** **auth** GET <http://www.sipgate.de:80/user/index.php?message=Bitte+aktivieren+S>

Response (22247): <HTML>\n<HEAD>\n<title>sipgate.de - Ihr kostenloser  
Internet Telefonanschluss (title)\n<META NAME="TITLE" CONTENT="sipgate.de - Ihr



## Ratproxy audit report

Generated on: 2009/05/30 13:18

Input file: /ratproxy-data/sipgate\_report2

NOTE: Not all of the issues reported necessarily correspond to actual security flaws. Findings should be validated by manual testing and analysis where appropriate. When in doubt, contact the author.

### Report risk and risk modifier designations:

**LOW** to **HIGH**

Issue urgency classification (composite of impact and identification accuracy)

**INFO**

Non-discriminatory entry for further analysis

**ECHO** / **echo**

Query parameters echoed back / not echoed in HTTP response, respectively

**PRED** / **pred**

Request URL or query data likely is / is not predictable to third parties, respectively

**AUTH** / **auth**

Request requires / does not require cookie authentication, respectively

### XSS candidates [toggle](#)

Pages where non-trivial query parameters appear to be echoed back on the page. Most or all of these resources might be safe - but they constitute prime candidates for further manual or automated XSS vulnerability testing.

- INFO** **ECHO** **PRED** **auth** GET http://www.sipgate.de:80/user/index.php?message=Bitte+aktivieren+Sie- Response (22247): <HTML>\n<HEAD>\n<title>sipgate.de - Ihr kostenloser Internet-Telefonanschluss.</title>\n<META NAME="TITLE" CONTENT="sipgate.de - Ihr kostenloser Internet-Telefonanschluss.">\n<META NAME="DESCRIPTION" CONTENT="VoIP mit kostenloser geographischer Wunschrufnummer, netzintern weltweit kostenlosen... Cookies set: PHPSESSID=6c141870e877a8122926aafd67af8185; Country\_Code=de; Lang=de; DomainCode=de Offending value: message MIME type: text/html, detected: text/html, charset: ISO-8859-1

Username Passwort 
[Start](#)
[Einführung](#)
[Rufnummern](#)
[Tarife](#)
[Hardware](#)
[Downloads](#)
[Anmeldung](#)
[Hilfe-Center](#)

Wir haben die Preise gesenkt! Teilnehmer am Seminar innovative Internet Technologien zahlen bei uns jetzt fast nix. Das Angebot gilt nur, falls es keine Nachfrage gibt. Betreten der Seite verboten! Eltern haften fuer ihre Kinder. Besonders freut uns, dass diese Nachricht sinnlos ist und trotzdem mit unserem SSL-Zertifikat beglaubigt ist.

## Ihr kostenloser Internet-Telefonanschluss.

- ▶ weltweit gratis telefonieren
- ▶ eigene Rufnummer
- ▶ auch ohne PC nutzbar
- ▶ keine Grundgebühr
- ▶ keine Vertragsbindung

[▶ Jetzt gratis anmelden!](#)
[Alle Infos](#) [Was ist VoIP?](#)

Unsere Tarife:



**sipgate basic**  
kostenloser  
Internet-  
Telefonanschluss



**sipgate plus**  
Fax, 4  
Durchwahlen,  
1 ct/min\* ins  
D-Festnetz



**Tarifoption flat**  
D-Festnetz und 14  
EU-Länder gratis



Username Passwort [Start](#) [Einführung](#) [Rufnummern](#) [Tarife](#) [Hardware](#) [Downloads](#) [Anmeldung](#) [Hilfe-Center](#)

Wir haben die Preise gesenkt! Teilnehmer am Seminar innovative Internet Technologien zahlen bei uns jetzt fast nix. Das Angebot gilt nur, falls es keine Nachfrage gibt. Betreten der Seite verboten! Eltern haften fuer ihre Kinder. Besonders freut uns, dass diese Nachricht sinnlos ist und trotzdem mit unserem SSL-Zertifikat beglaubigt ist.

## Page Info

[General](#) [Forms](#) [Links](#) [Media](#) [Privacy](#) [Security](#)**Web Site Identity Verified**

The web site secure.sipgate.de supports authentication for the page you are viewing. The identity of this web site has been verified by The USERTRUST Network, a certificate authority you trust for this purpose.

[View](#)

View the security certificate that verifies this web site's identity.

**Connection Encrypted: High-grade Encryption (AES-256 256 bit)**

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

Username Passwort [Start](#)[Einführung](#)[Rufnummern](#)[Tarife](#)[Hardware](#)[Downloads](#)[Anmeldung](#)[Hilfe-Center](#)

Wir haben die Preise gesenkt! Teilnehmer am Seminar innovative Internet Technologien zahlen bei uns jetzt fast

die Kinder.  
st.

General Details

**This certificate has been verified for the following uses:**

SSL Server Certificate

**Issued To**

Common Name (CN) \*.sipgate.de  
 Organization (O) indigo networks GmbH  
 Organizational Unit (OU) NOC  
 Serial Number 00:D9:F7:F6:CC:B4:3B:BF:7A:0A:9F:4E:81:77:A0:A5:85

**Issued By**

Common Name (CN) UTN-USERFirst-Hardware  
 Organization (O) The USERTRUST Network  
 Organizational Unit (OU) http://www.usertrust.com

**basic**

oser  
-  
anschluss

**plus**

ahlen,  
n\* ins  
etz

**tion flat**

etz und 14  
der gratis



- Methoden zur Veränderung von Eingabeteilen
  - Vervielfachung mit identischen oder verschiedenen Inhalten
  - Weglassen
  - Änderung der Reihenfolge
  - Wechsel der Eingabeart (Cookie, GET, POST)
  - Verkürzen
  - Einfügen von Metazeichen wie " ' , ; + - \* / ( ) \ \_ < > [ ] { }
  - Einfügen von \0 (NULL-Byte)
  - Einfügen von SQL/PHP/HTML/JavaScript-Fragmenten
  - Änderung des Encodings (HTML-Entities, URL, &#..;)
  - Erhöhung der Länge (für Buffer Overflows)



- Statische Analyse
  - Model Checking
    - Sehr aufwendig
    - Selten eingesetzt
  - Datenflussanalyse
    - Taint-Quellen
    - Taint-Senken
    - Kontext-Sensitiv
    - Muss auf die Webanwendung als Ganzes angewandt werden

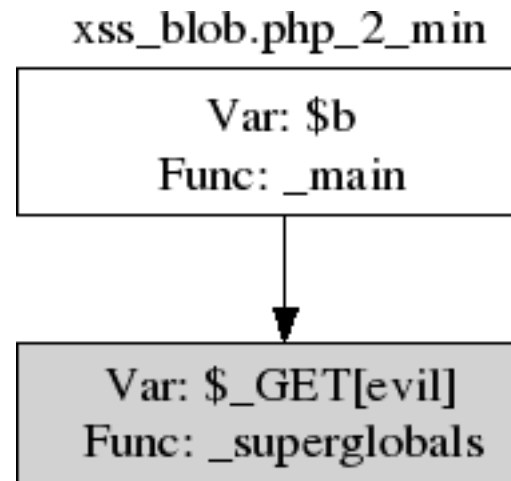


## □ Eingabe:

```
<?php
$a = 'good';
$b = $_GET['evil'];
echo $a; // OK
echo $b; // XSS-Problem
?>
```

## □ Ausgabe:

```
** detecting vulnerabilities ***
***XSS Analysis BEGIN
Number of sinks: 2
Vulnerability detected!
- unconditional
- blob.php:7
- Graph: xss2
Total Vuln Count: 1
***XSS Analysis END
```





- ❑ OWASP Top 10 – 2007 Edition (OWASP)
- ❑ WebGoat and WebScarab Documentation (OWASP)
- ❑ RatProxy Documentation (Google)
- ❑ Pixy: A Static Analysis Tool for Detecting Web Application Vulnerabilities (Huang, Huang, Lin, Tsai)
- ❑ Web Application Security Assessment by Fault Injection and Behaviour Monitoring (Jovanovic, Kruegel, Kirda)
- ❑ Static Detection of Cross-Site Scripting Vulnerabilities (Wassermann, Su)
- ❑ Saner: Composing Static and Dynamic Analysis to Validate Sanitization in Web Applications (Balzarotti, Cova, Felmetzger, Jovanovic, Kirda, Kruegel, Vigna)
- ❑ Static Detection of Security Vulnerabilities in Scripting Languages (Xie, Aiken)



- ❑ Für unbekanntem Quellcode
  - Ratproxy
  - WebScarab
  - ProxMon
  - Paros
  - Burp Suite
  - Grendel
  - Google ;-)
- ❑ Für statische Analyse
  - Pixy
  - OWASP SWAAT
  - Yasca
  - LAPSE
- ❑ Lernplattformen
  - WebGoat



- ❑ Eingaben werden selten korrekt und vollständig validiert
- ❑ Analyse ohne Quellcode
  - Korrelation Eingabe/Ausgabe
  - Fuzzing, insbesondere bei Authentisierung
  - Prüfung Eingabe/Ausgabe auf Sprachbausteine und Datenlecks
- ❑ Analyse mit Quellcode
  - Tainting: Eingabe ist **nie** vertrauenswürdig
  - Validierung der Eingabe vor jeglicher Verarbeitung
  - Eingabe darf nur nach Escaping zu externen Programmen
  - Eingabe darf nur für authentifizierte Nutzer zur Ausgabe
  - Authentisierung muss bei jeder Anfrage geprüft werden
- ❑ ~90% der Fehler sind auf den ersten Blick erkennbar



# Offene Probleme

- ❑ Analyse bei unbekanntem Quellcode
  - Weiterentwicklungen von Fuzzing
  - Heuristische Gewinnung von Informationen über innere Abläufe der Webanwendung
  - Interaktionen zwischen verschiedenen Domains
  - Intuition ist nur schwer programmierbar
- ❑ Analyse bei bekanntem Quellcode
  - Kombinierte statische Analyse für mehrere Sprachen
  - Kombinierte statische Analyse für mehrere interagierende Anwendungen
  - Reduzierung der False Positives und False Negatives der Heuristiken in statischer und dynamischer Analyse
- ❑ Neue Problemklassen
  - XSS war mal neu. Was kommt als Nächstes?



**Danke**

Vielen Dank für Ihre Aufmerksamkeit



- ❑ Noch Fragen?