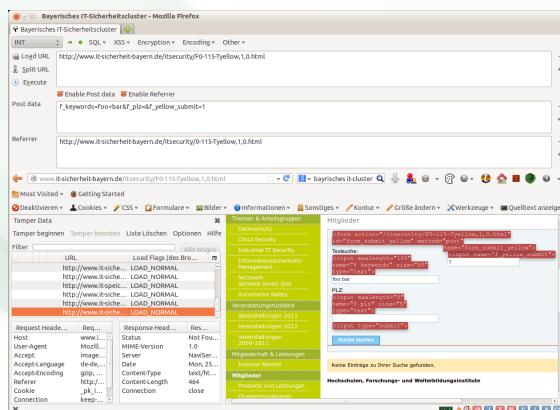




Weil Ihre Daten unbezahlbar sind.

## Hacker-Tool Browser von der Webanwendung zu den Kronjuwelen



Ralf Reinhardt  
28.11.2013, 16:40 Uhr

Roadshow „Sicheres Internet“

aiti-Park

Werner-von-Siemens-Str. 6  
86159 Augsburg

# Hacker-Tool Browser

## Über sic[!]sec und Ralf Reinhardt

Wie "ticken" Web-Anwendungen?

OWASP und die Top 10, Version 2013

Top 10, A3: Cross-Site Scripting (XSS)

Top 10, A4: Unsichere direkte Objektreferenzen

Top 10, A1: Injection

Hacker-Tools: Webbrowser, Add-Ons und Proxys

# Über die sic[!]sec GmbH

- sic[!]sec GmbH in Gröbenzell bei München  
[www.sicsec.de](http://www.sicsec.de), [info@sicsec.de](mailto:info@sicsec.de)
- gegründet 2010 von Achim Hoffmann und Ralf Reinhardt  
als unabhängiges Beratungshaus / InfoSec Service Provider
- Schwerpunkt Web Application Security / Information Security
  - Penetrationstests Web-Application-Security-Ebene
  - Penetrationstests Netzwerk- und System-Ebene
  - Source Code Analysen, Code Reviews, Reverse Engineering, Exploits
  - Web Application Firewalls, Software- und Infrastruktur-Architekturen
  - Guidelines und Policys, Workshops und Seminare, Awareness
  - Social Engineering, Physical Security
  - Prozessoptimierung, Datenschutz, Compliance, usw.

## Über die sic[!]sec GmbH

- Gründungsmitglied



WIDU • Verband zum Schutz des Rohstoffes Wissen in deutschen Unternehmen e.V.

- Mitglied



Member of the Bavarian IT Security & Safety Cluster

- Teilnehmer

Allianz für  
Cyber-Sicherheit



- Unterstützer



Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[!]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>

## Über Ralf Reinhardt

- Principal Consultant und GF der sic[!]sec GmbH
- Lehrbeauftragter für Web Application Security an der Technischen Hochschule Nürnberg
- OWASP Mitglied, Project Leader und Contributor
- Mitglied des ISSECO (International Secure Software Engineering Council)
- 27 Jahre IT-Erfahrung, darunter Client-, Server- und Datenbankprogrammierung, Administration (AIX, Linux, Oracle), IT-Projektleitung, Rollout, Betrieb, ITIL, usw.
- Diverse Zertifizierungen und sonstige Mitgliedschaften

Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[!]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>

# Hacker-Tool Browser

Über sic[!]sec und Ralf Reinhardt

## Wie "ticken" Web-Anwendungen?

OWASP und die Top 10, Version 2013

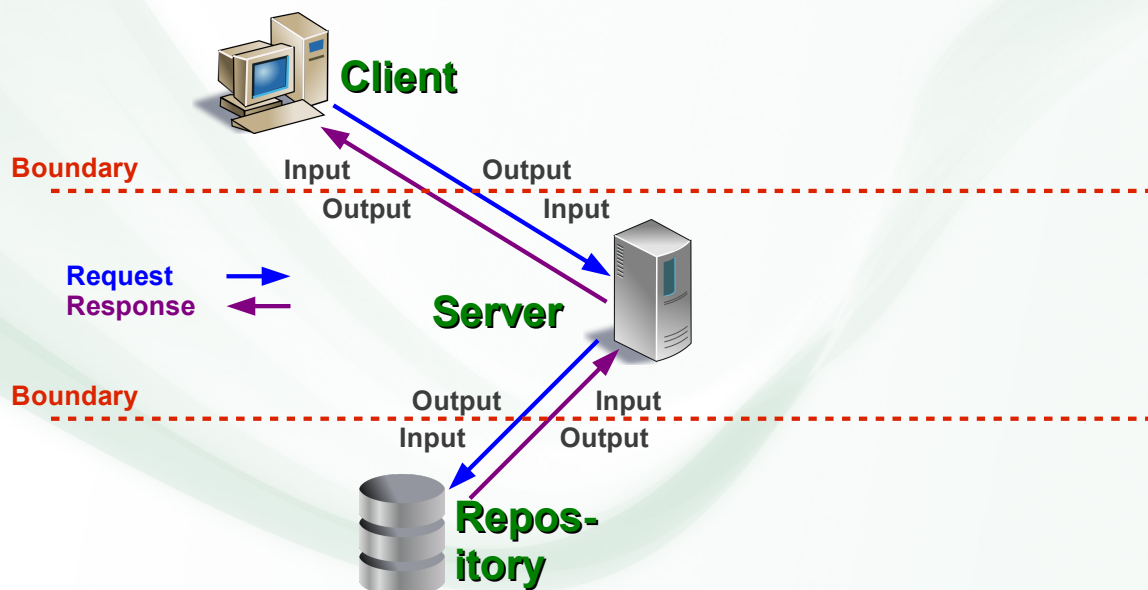
Top 10, A3: Cross-Site Scripting (XSS)

Top 10, A4: Unsichere direkte Objektreferenzen

Top 10, A1: Injection

Hacker-Tools: Webbrowser, Add-Ons und Proxys

## Wie "ticken" Web-Anwendungen?



# Hacker-Tool Browser

Über sic[!]sec und Ralf Reinhardt

Wie "ticken" Web-Anwendungen?

## OWASP und die Top 10, Version 2013

Top 10, A3: Cross-Site Scripting (XSS)

Top 10, A4: Unsichere direkte Objektreferenzen

Top 10, A1: Injection

Hacker-Tools: Webbrowser, Add-Ons und Proxys

# Über OWASP

- Open Web Application Security Project
- „not-for-profit worldwide charitable organisation focused on improving the security of application software“
- ca. 160 Chapter in 80 Ländern
- „free and open to the public“
- Struktur: Board, Chapter, „Stammtisch“, Mitglied
- <http://www.owasp.de/>, <http://muc.owasp.de>  
<https://www.owasp.org/>  
<https://lists.owasp.org/mailman/listinfo/owasp-germany>



# OWASP Top 10, Version 2013



Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Grobenzell, Germany. - For personal use only. - <http://www.sicsec.de>

# OWASP Top 10, Version 2013

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Grobenzell, Germany. - For personal use only. - <http://www.sicsec.de>

# Hacker-Tool Browser

Über sic[!]sec und Ralf Reinhardt

Wie "ticken" Web-Anwendungen?

OWASP und die Top 10, Version 2013

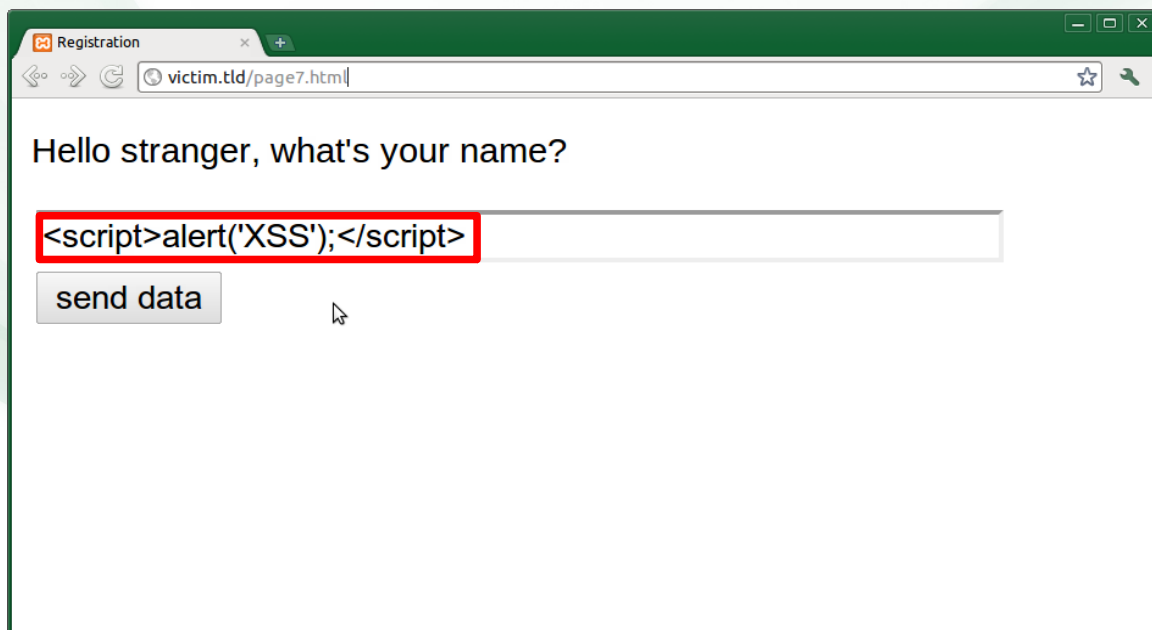
## Top 10, A3: Cross-Site Scripting (XSS)

Top 10, A4: Unsichere direkte Objektreferenzen

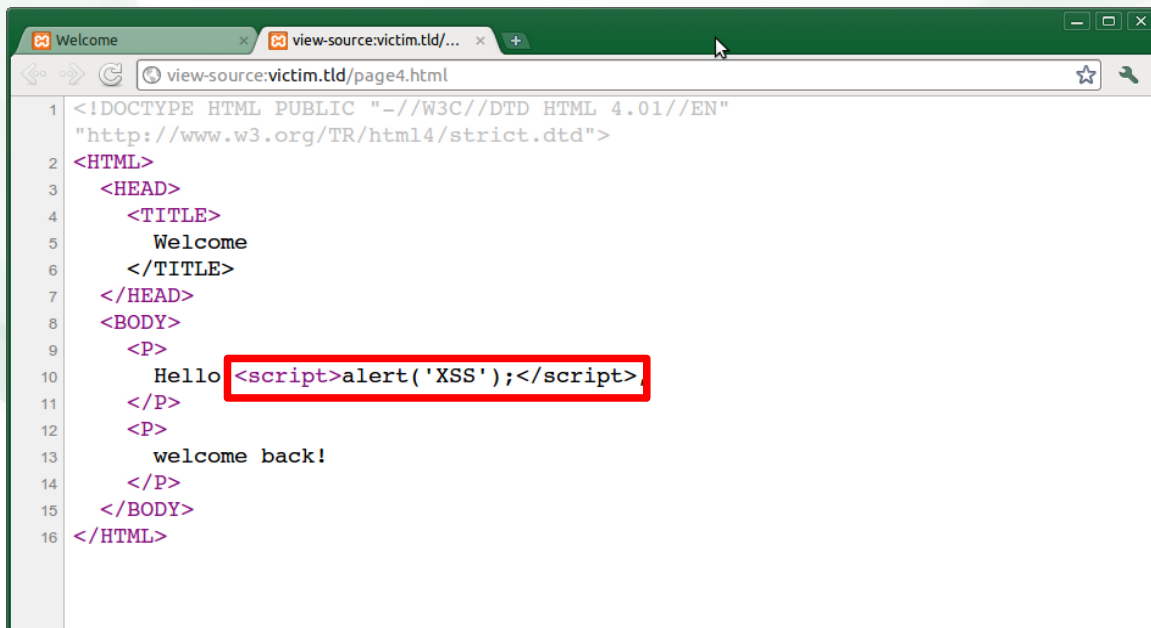
Top 10, A1: Injection

Hacker-Tools: Webbrowser, Add-Ons und Proxys

# Cross-Site Scripting, Eingabe



# Cross-Site Scripting, Quellcode



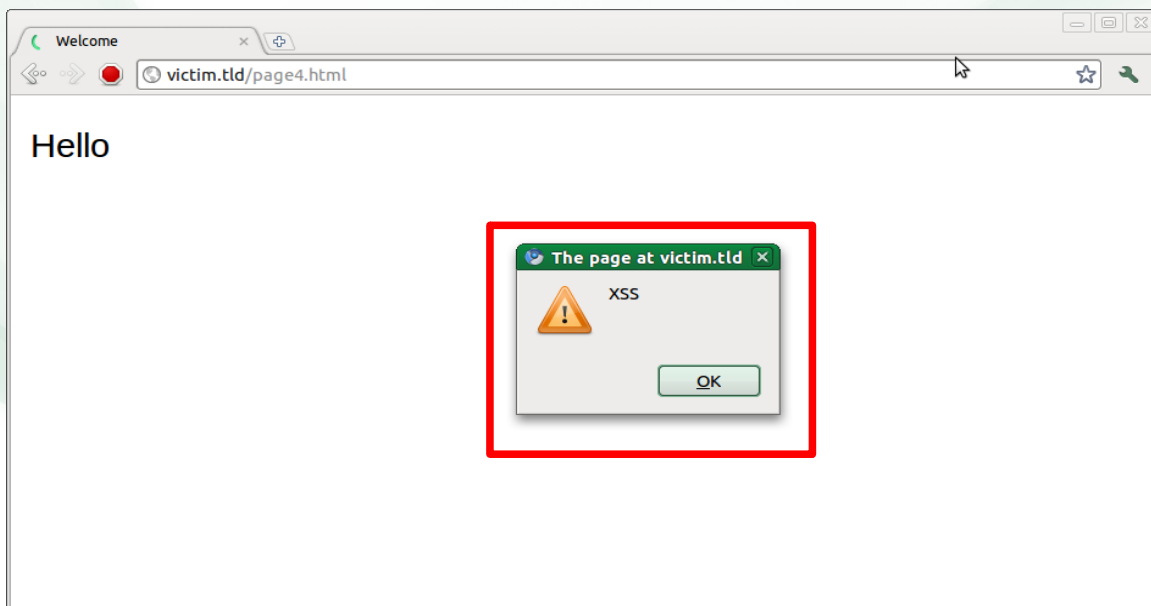
```
1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
  "http://www.w3.org/TR/html4/strict.dtd">
2 <HTML>
3   <HEAD>
4     <TITLE>
5       Welcome
6     </TITLE>
7   </HEAD>
8   <BODY>
9     <P>
10    Hello <script>alert('XSS');</script>
11   </P>
12   <P>
13     welcome back!
14   </P>
15 </BODY>
16 </HTML>
```

Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Grobenzell, Germany. - For personal use only. - <http://www.sicsec.de>

# Cross-Site Scripting Angriff (I / II)



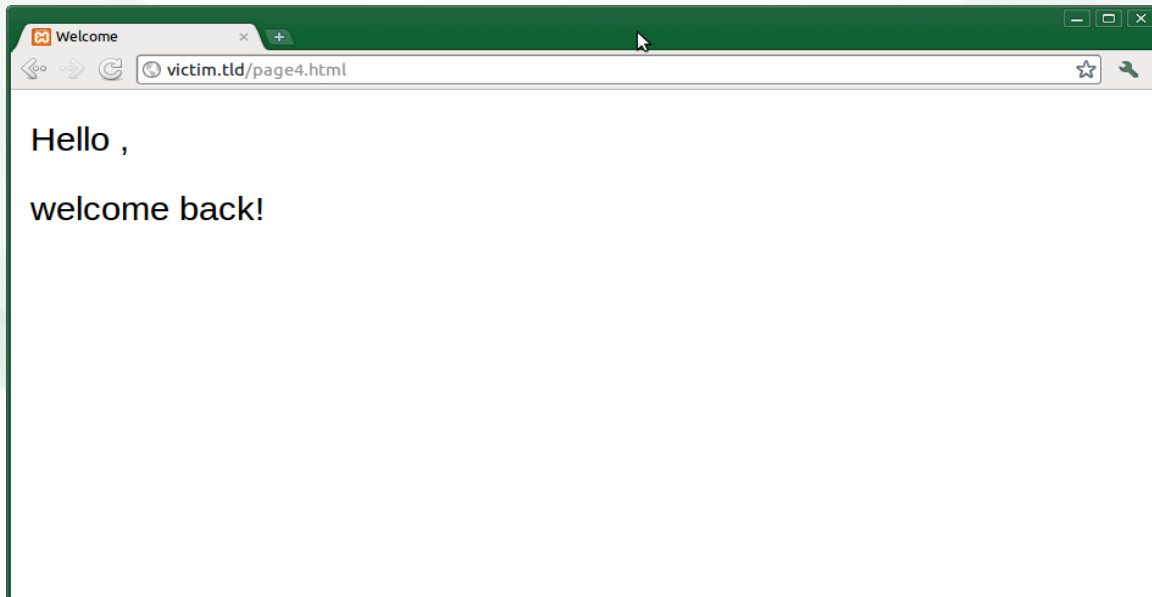
Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Grobenzell, Germany. - For personal use only. - <http://www.sicsec.de>



# Cross-Site Scripting Angriff (II / II)

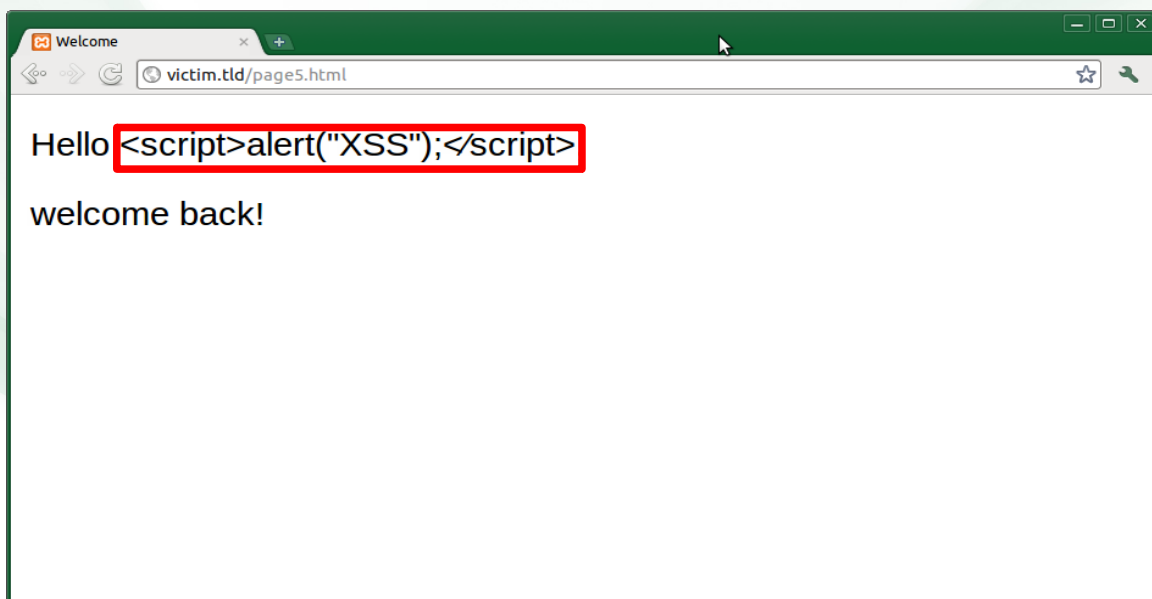


Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Grobenzell, Germany. - For personal use only. - <http://www.sicsec.de>

# Kein Cross-Site Scripting!



Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Grobenzell, Germany. - For personal use only. - <http://www.sicsec.de>

# Korrektes Escaping :-)

```

1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
  "http://www.w3.org/TR/html4/strict.dtd">
2 <HTML>
3   <HEAD>
4     <TITLE>
5       Welcome
6     </TITLE>
7   </HEAD>
8   <BODY>
9     <P>
10      Hello &lt;script&gt;alert(&quot;XSS&quot;);&lt;&frasl;script&gt;
11    </P>
12    <P>
13      welcome back!
14    </P>
15  </BODY>
16 </HTML>

```

Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Grobenzell, Germany. - For personal use only. - <http://www.sicsec.de>

# Risiken im Zusammenspiel mit Cross-Site Scripting

**Arten (und beispielhafte Angriffsvektoren):**  
**Reflektiert (E-Mail), Persistent (Gästebuch)**

- Defacement, Spoofing, Phishing, ...

**In Zusammenspiel mit Top 10, „A2: Broken Authentication and Session Management“:**

- Session Hijacking, Cookie-Manipulationen, ...

**In Zusammenspiel mit Top 10, „A8: Cross-Site Request Forgery“ oder „A7: Missing Functional Level Access Control“:**

- Privilege Escalation, Unterschieben fremder Requests, ...

Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Grobenzell, Germany. - For personal use only. - <http://www.sicsec.de>

# Hacker-Tool Browser

Über sic[!]sec und Ralf Reinhardt

Wie "ticken" Web-Anwendungen?

OWASP und die Top 10, Version 2013

Top 10, A3: Cross-Site Scripting (XSS)

**Top 10, A4: Unsichere direkte Objektreferenzen**

Top 10, A1: Injection

Hacker-Tools: Webbrowser, Add-Ons und Proxys

## Unsichere direkte Objektreferenzen (I / III)

1) Ziel des Benutzers einer Webanwendung:

Prüfen der eigenen Kontoumsätze bei seiner Hausbank.

2) Bankanwendung bietet dafür einen Link

„Kontoumsätze“ an.

Dieser ruft folgende URL auf:

**`https://badbank.tld/umsatz?konto=4711`**

## Unsichere direkte Objektreferenzen (II / III)

3) Benutzer klickt Link

`https://badbank.tld/umsatz?konto=4711`

4) Benutzer sieht die Umsätze seines  
Kontos 4711 und ist glücklich.

5) Benutzer wird neugierig...

## Unsichere direkte Objektreferenzen (III / III)

6) Benutzer testet direkte URL-Eingabe

`https://badbank.tld/umsatz?konto=4712`

7) Benutzer sieht die Umsätze des **Kontos 4712**;  
dieses Konto **gehört ihm nicht**.

8) Ist Benutzer Hacker, ist er jetzt noch glücklicher.

# Hacker-Tool Browser

Über sic[!]sec und Ralf Reinhardt

Wie "ticken" Web-Anwendungen?

OWASP und die Top 10, Version 2013

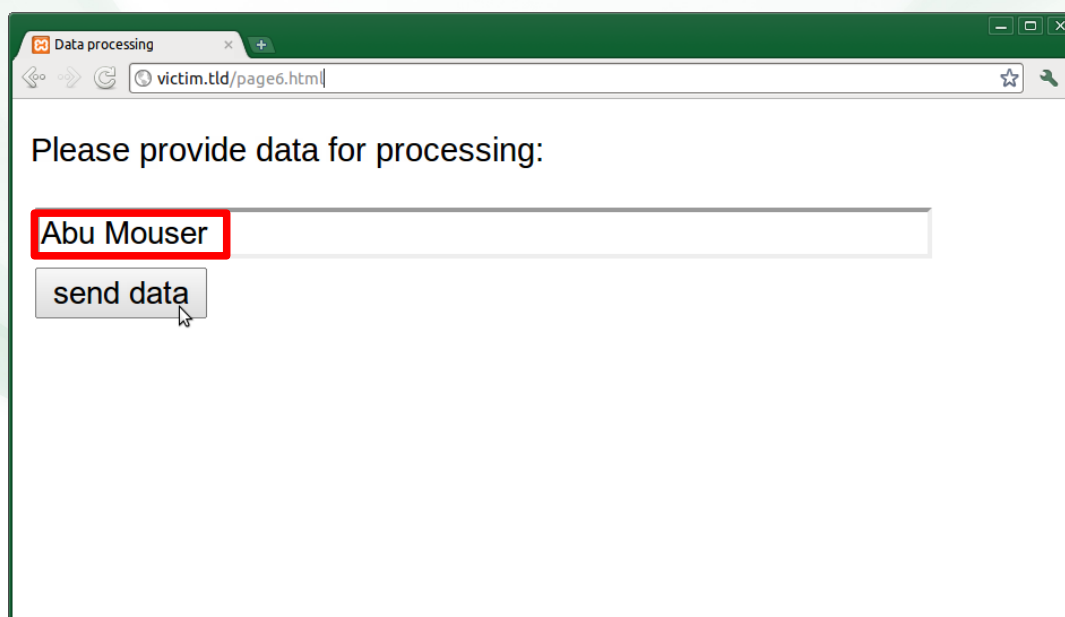
Top 10, A3: Cross-Site Scripting (XSS)

Top 10, A4: Unsichere direkte Objektreferenzen

## Top 10, A1: Injection

Hacker-Tools: Webbrowser, Add-Ons und Proxys

# Datenbankabfrage durch Client



# SQL-Statement im Server „regulären Anfrage“

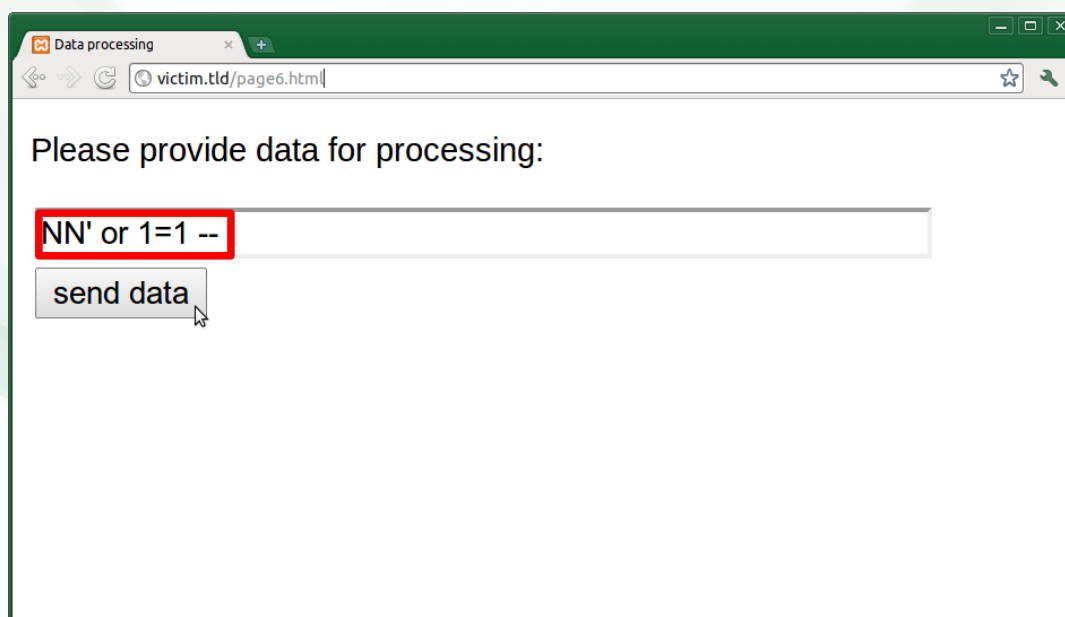
```
1 Connection connection = /* some DB connection */;  
2 Statement statement = connection.createStatement();  
3  
4 String queryString = "SELECT nicename, email, institution FROM user"  
5   + "WHERE nicename = " + request.getParameter("nicename") + """;  
6  
7 ResultSet results = statement.executeQuery(queryString);
```

```
1 SELECT nicename, email, institution FROM user WHERE  
2 nicename = 'Abu Mouser';
```

Ergebnis der Ausgabe am Client:

- „Abu Mouser, abu@mouser.tld, Einkauf“

# SQL-Injection über Client





# Resultat der SQL-Injection im Backend

```
1 Connection connection = /* some DB connection */;  
2 Statement statement = connection.createStatement();  
3  
4 String queryString = "SELECT nickname, email, institution FROM user"  
5   + "WHERE nickname = '" + request.getParameter("nickname") + "'";  
6  
7 ResultSet results = statement.executeQuery(queryString);
```

```
1 SELECT nickname, email, institution FROM user WHERE  
2 nickname = 'NN' or 1=1 -';
```

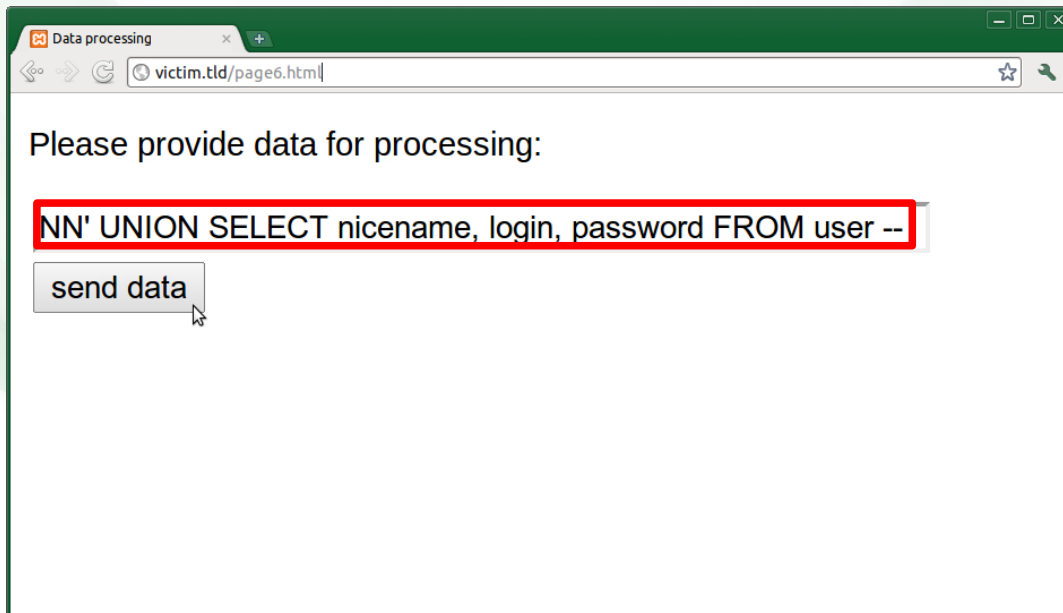
Ergebnis der Ausgabe am Client:

- „Name, E-Mail, Abteilung“ für **alle** Benutzer!

# Tabellenstruktur der Datenbank

- Annahme: In der Datenbank existiert eine **Tabelle** namens **USER** mit den Spalten
  - NICENAME
  - EMAIL
  - INSTITUTION
  - LOGIN
  - PASSWORD

# SQL-Injection mit „union“



Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Grobenzell, Germany. - For personal use only. - http://www.sicsec.de

# Resultat der „union“-SQL-Injection im Backend

```

1 Connection connection = /* some DB connection */;
2 Statement statement = connection.createStatement();
3
4 String queryString = "SELECT nickname, email, institution FROM user"
5   + "WHERE nickname = '" + request.getParameter("nickname") + "'";
6
7 ResultSet results = statement.executeQuery(queryString);

```

```

1 SELECT nickname, email, institution FROM user WHERE
2 nickname = 'NN'
3 UNION
4 SELECT nickname, login, password FROM user --';

```

Ergebnis der Ausgabe am Client:

- „Name, **Login, Passwort**“ für **alle** Benutzer!

Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Grobenzell, Germany. - For personal use only. - http://www.sicsec.de

# Hacker-Tool Browser

Über sic[!]sec und Ralf Reinhardt

Wie "ticken" Web-Anwendungen?

OWASP und die Top 10, Version 2013

Top 10, A3: Cross-Site Scripting (XSS)

Top 10, A4: Unsichere direkte Objektreferenzen

Top 10, A1: Injection

## Hacker-Tools: Webbrowser, Add-Ons und Proxys

# Wahl des richtigen Browsers

- Firefox bietet aktuell die meisten Add-ons, aber auch andere Browser wie Chrome oder diverse Open-Source-Entwicklungen sind nutzbar



# Proxy-Plugin, „Tamper Data“

**Tamper Data Aktuelle Requests**

Tamper beginnen Tamper beenden Liste Löschen Optionen Hilfe

Filter: stammtisch Alle zeigen

Uhrzeit	Dauer	Gesa...	Größe	Method	Cont...	URL	Load Fl...
20:12:48...	663 ms	1630 ms	-1	GET	200	text/html https://www.owasp.org/index.php?search=stammtisch&go...	LOAD_DOCU...
20:12:49...	88 ms	88 ms	35	GET	200	image/gif https://ssl.google-analytics.com/_utm.gif?utmwv=5.4.6&ut...	LOAD_NOR...
20:13:18...	728 ms	13723 ms	-1	GET	200	text/html https://www.owasp.org/index.php?search=stammtisch&go...	LOAD_DOCU...
20:13:32...	81 ms	81 ms	35	GET	200	image/gif https://ssl.google-analytics.com/_utm.gif?utmwv=5.4.6&ut...	LOAD_NOR...
20:13:32...	155 ms	155 ms	832	GET	200	applicati... https://engine.adzerk.net/ados?t=1385406812463&request...	LOAD_NOR...
20:16:10...	623 ms	1596 ms	-1	GET	200	text/html https://www.owasp.org/index.php/OWASP_German_Chapt...	LOAD_DOCU...
20:16:11...	107 ms	107 ms	35	GET	200	image/gif https://ssl.google-analytics.com/_utm.gif?utmwv=5.4.6&ut...	LOAD_NOR...
20:16:11...	436 ms	436 ms	833	GET	200	applicati... https://engine.adzerk.net/ados?t=1385406971618&request...	LOAD_NOR...
20:16:45...	831 ms	1601 ms	-1	GET	200	text/html https://www.owasp.org/index.php?search=stammtisch&go...	LOAD_DOCU...
20:16:46...	116 ms	116 ms	35	GET	200	image/gif https://ssl.google-analytics.com/_utm.gif?utmwv=5.4.6&ut...	LOAD_NOR...

Request Heade...	Request Header Wert	Response Header Name	Response Header Wert
Host	www.owasp.org	Status	OK - 200
User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:25.0) Ge	Date	Mon, 25 Nov 2013 19:16:05 GMT
Accept	text/html,application/xhtml+xml,application/xml;	Server	Apache
Accept-Language	de-de,de;q=0.8,en-us;q=0.5,en;q=0.3	X-Frame-Options	Deny
Accept-Encoding	gzip, deflate	X-XSS-Protection	1; mode=block
Referer	https://www.owasp.org/index.php?search=stamm	X-Content-Type-Options	nosniff
Cookie	_utma=77342603.1711988191.1383211793.13853	Content-Language	en
Connection	keep-alive	Vary	Accept-Encoding, Cookie
		Expires	Thu, 01 Jan 1970 00:00:00 GMT
		Cache-Control	private, must-revalidate, max-age=0
		Last-Modified	Sat, 23 Nov 2013 20:06:17 GMT
		Content-Encoding	gzip
		Keep-Alive	timeout=5, max=100

Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Grobenzell, Germany. - For personal use only. - http://www.sicsec.de

# „Cookies Manager+“

**Cookies Manager+ v1.5.2 [showing 5 of 2508, selected 1]**

Suchen: owasp Refresh

Website	Name	Content	Path	Http Only	
<input type="checkbox"/>	owasp.org	_utma	77342603.1711988191.1383211793...	/	No
<input type="checkbox"/>	owasp.org	_utmb	77342603.6.10.1385405154	/	No
<input type="checkbox"/>	owasp.org	_utmc	77342603	/	No
<input type="checkbox"/>	owasp.org	_utmz	77342603.1385405154.8.5.utmcscr=...	/	No
<input checked="" type="checkbox"/>	www.owasp.org	wikiUserName	Ralf+Reinhardt	/	Yes

**Edit Cookie+**

Name:  wikiUserName

Inhalt:  Ralf+Reinhardt

Host:  www.owasp.org

Pfad:  /

Senden für:  Nur verschlüsselte Verbindungen

Http Only:  Yes

Gültig bis:  date: May 13, 2014 12:31:21

Save as new Save Close

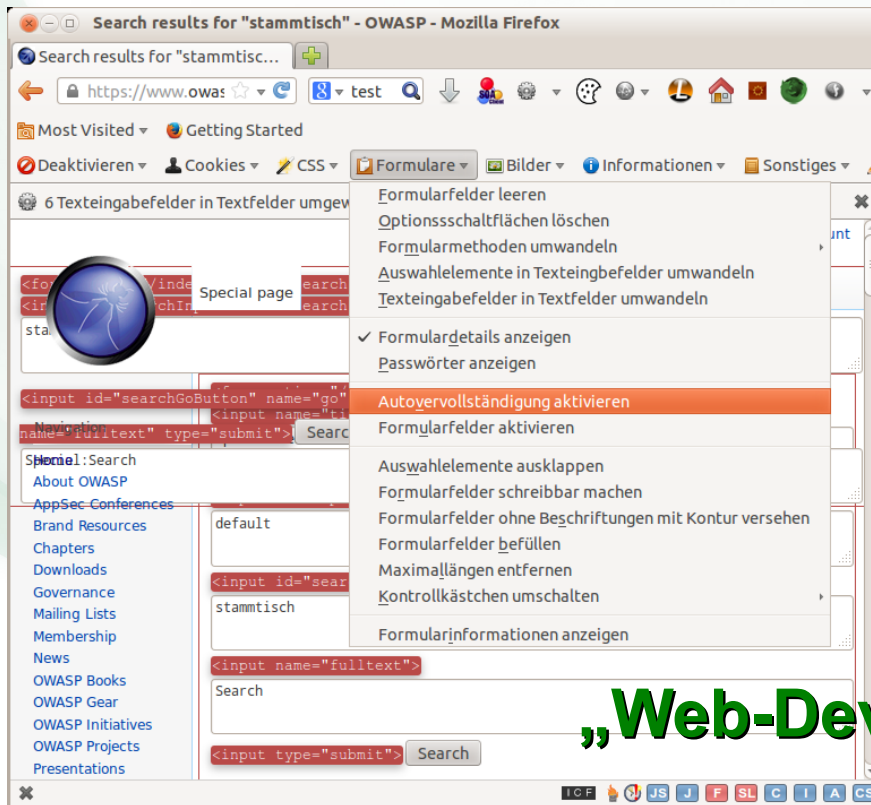
Name: wikiUserName  
Inhalt: Ralf+Reinhardt  
Host: www.owasp.org  
Pfad (H): /  
Senden für: Nur verschlüsselte Verbindungen  
Gültig bis (X): Di 13 Mai 2014 12:31:21 CEST

Add Edit Delete Schließen

Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Grobenzell, Germany. - For personal use only. - http://www.sicsec.de



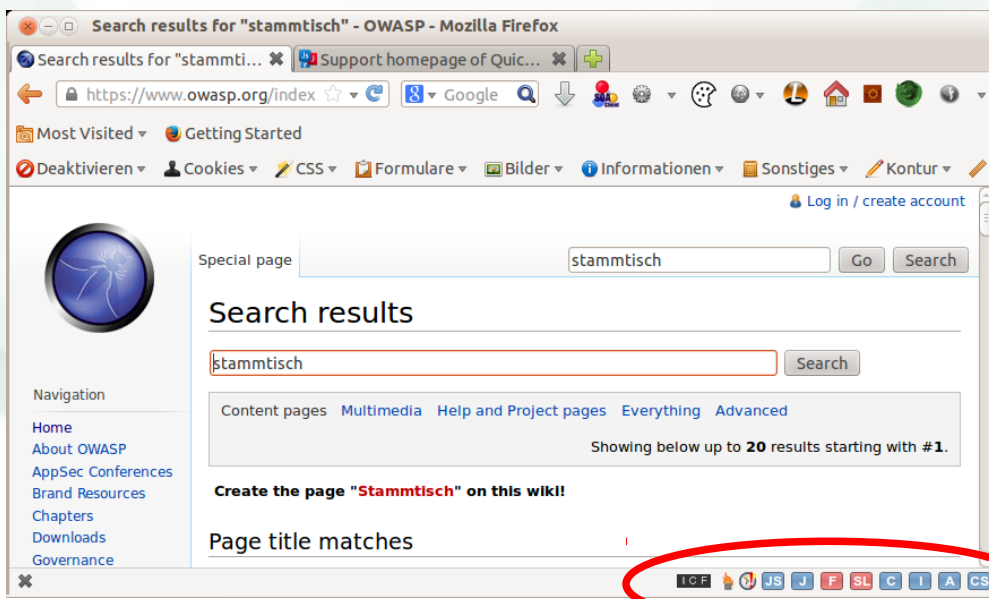
„Web-Developer“

Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Grobenzell, Germany. - For personal use only. - http://www.sicsec.de

# „QickJava“ Schalter

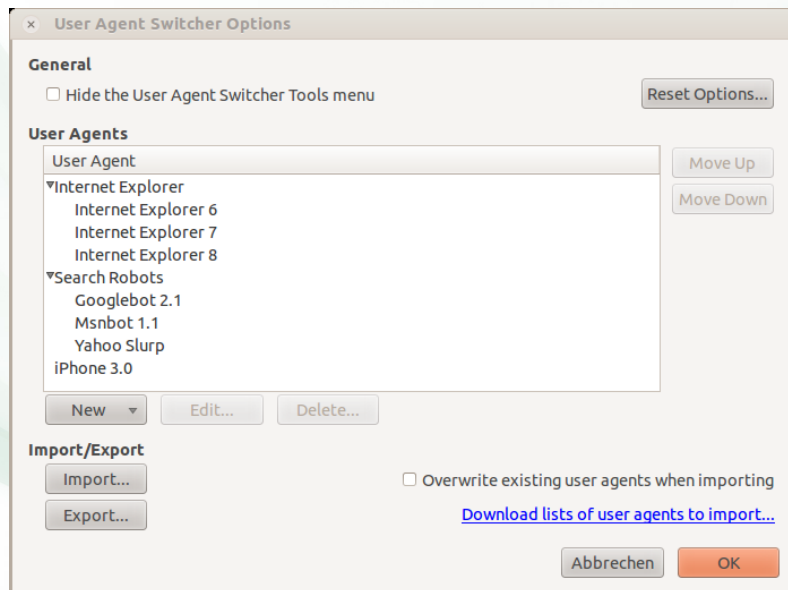


Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Grobenzell, Germany. - For personal use only. - http://www.sicsec.de

# „User Agent Switcher“

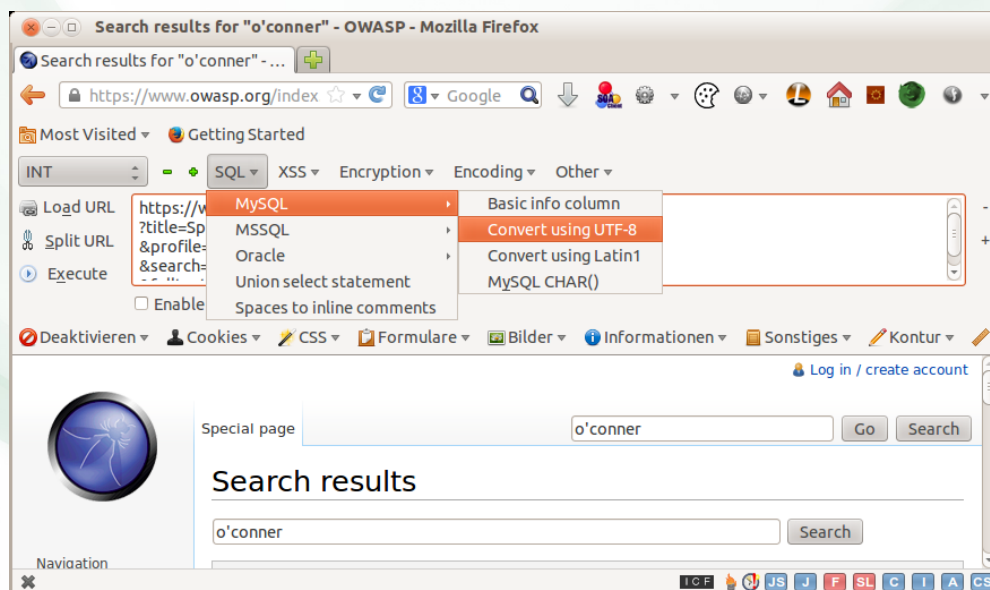


Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>

# „HackBar“



Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[✓]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>



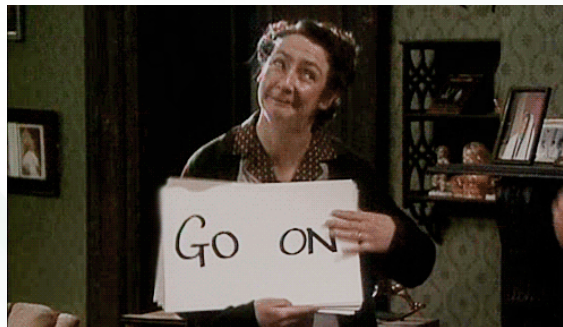
# „EnDe“ (Encoder / Decoder)

Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[!]sec GmbH in Grobenzell, Germany. - For personal use only. - <http://www.sicsec.de>

# Fragen, Anregungen?



ralf.reinhardt@sicsec.de  
ralf.reinhardt@owasp.org

sic[!]sec GmbH  
Industriestr. 29-31  
D-82194 Gröbenzell

[www.sicsec.de](http://www.sicsec.de)

Augsburg, 28.11.2013

Hacker-Tool Browser - von der Webanwendung zu den Kronjuwelen

© 2013 by sic[!]sec GmbH in Grobenzell, Germany. - For personal use only. - <http://www.sicsec.de>