cms garden

10 Tipps für eine sichere (CMS)-Webseite

13. März, Infoarena III, Internet World Expo 2019, München

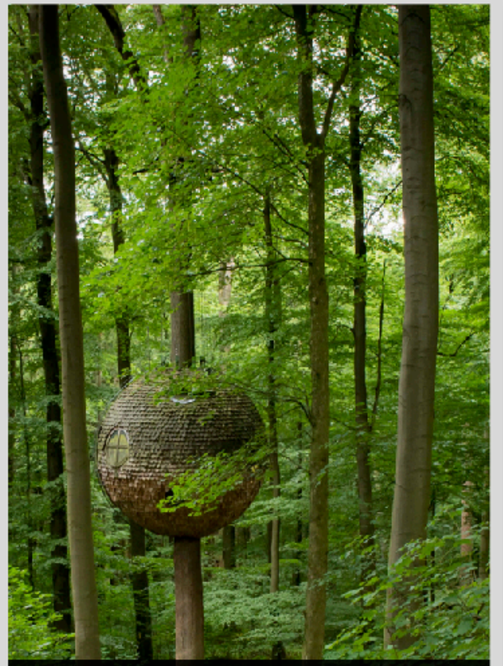
cms garden

Drupal™ Joomla! NEOS Plone Scientific MS TYPO3 umbraco WordPress

cms garden

ASSOCIATION OF FREE AND OPEN SOURCE CONTENT MANAGEMENT SYSTEMS

Contao
CONTENIDO
Drupal™
Joomla!™
NEOS
Plone
Scientific CMS
TYPO3
umbraco
WordPress



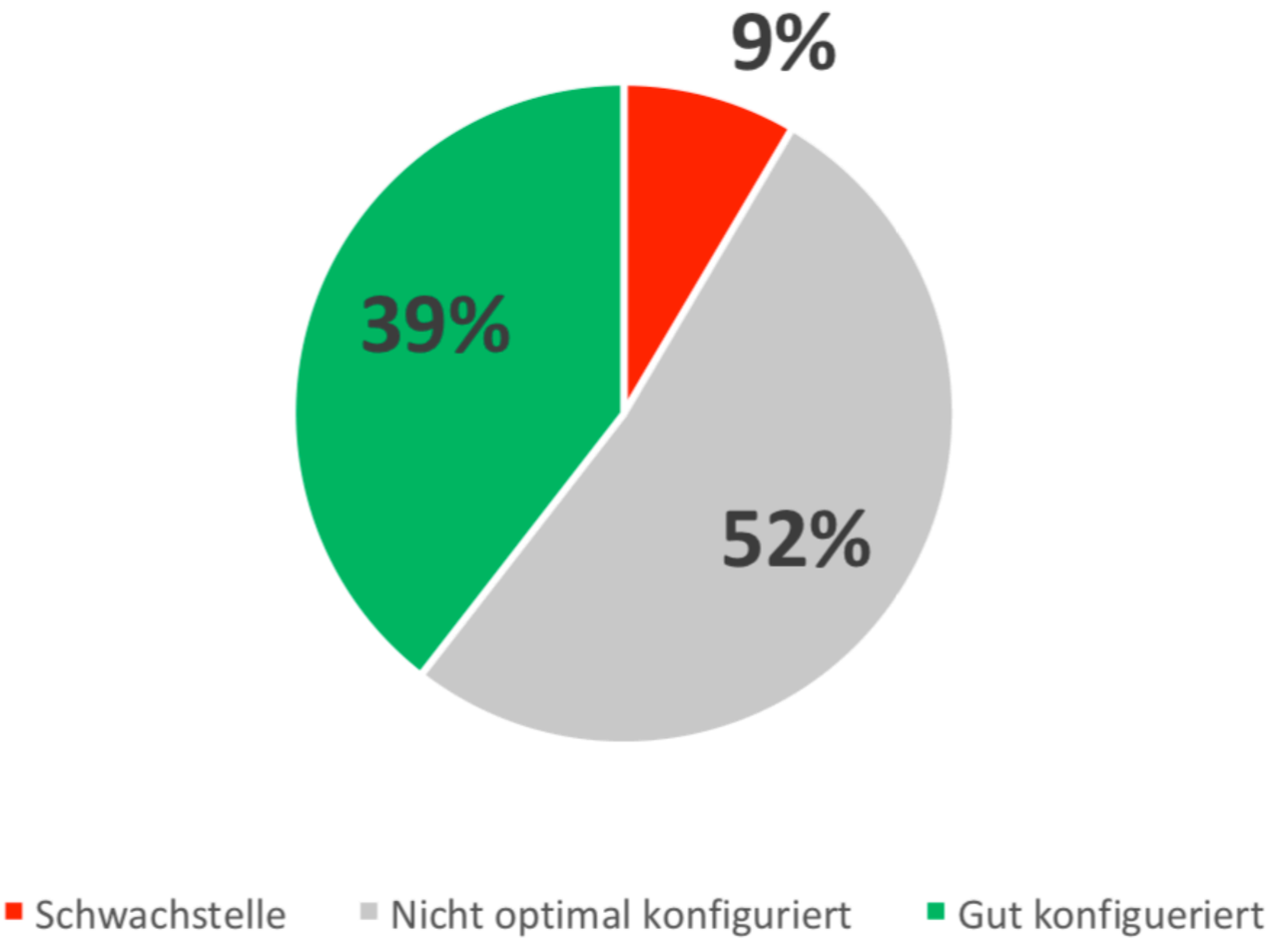
FOR UNCONVENTIONAL IDEAS


Sam Mortenson
@DrupalSAM
Folgen
One neat part of the Drupal security update yesterday is that core now uses a @typo3 package to protect sites against malicious .phar files. Always nice to see communities come together for good. 💪
07:51 - 17. Jan. 2019
https://github.com/TYPO3/phar-stream-wrapper


@ischmitt
SAP
SEGEL BUNDES LIGA
BAY

KMU Webseiten Check 2018

Über die Hälfte aller KMU Webseiten sind aus Sicherheitssicht nicht optimal konfiguriert: Fast jede 10. Webseite weist eklatante Sicherheitsmängel auf.



https://siwecos.de/images/presse/SIWECOS_KMU_Studie.pdf

cms garden

10 Tipps für eine sichere (CMS)-Webseite

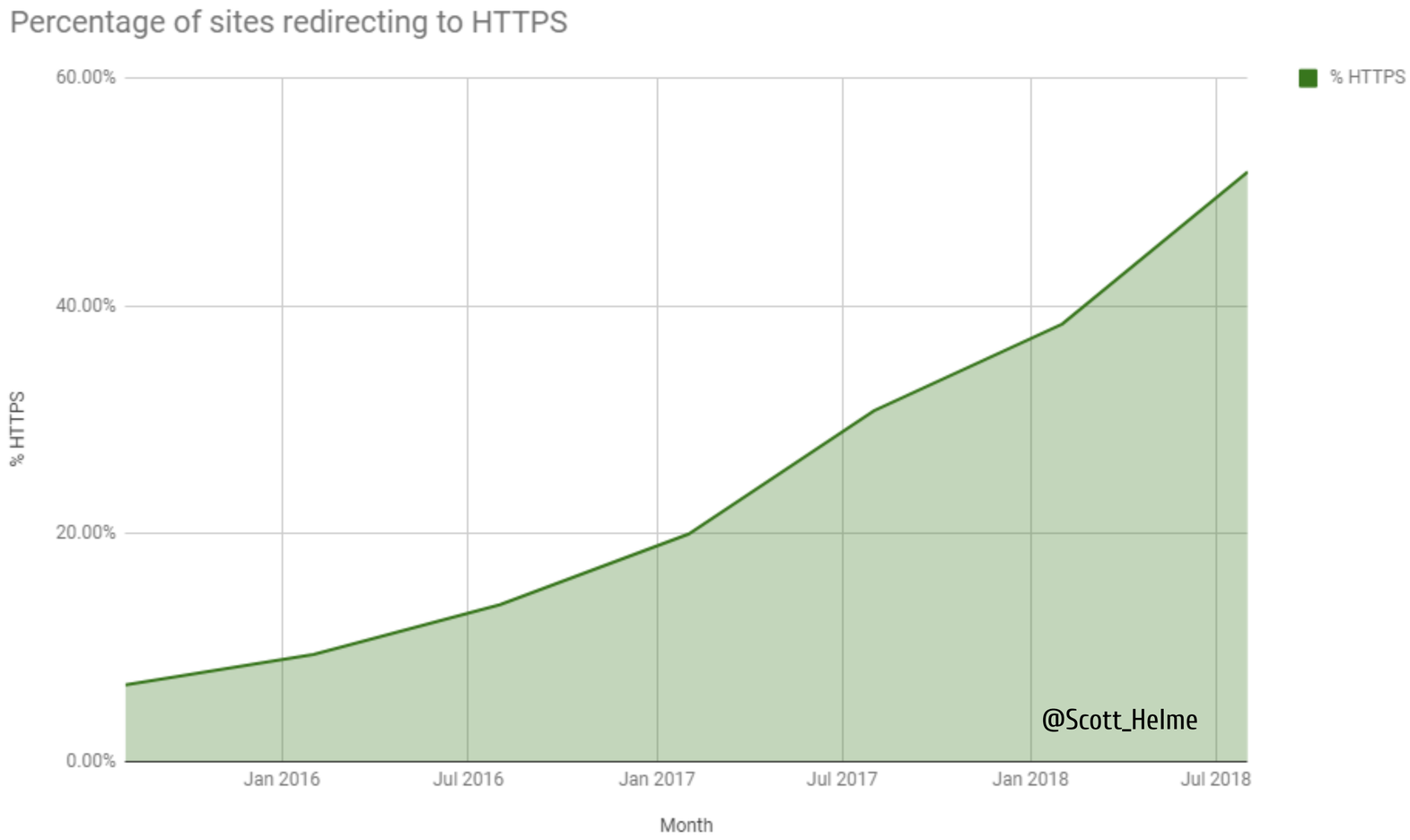
13. März, Infoarena III, Internet World Expo 2019, München

0

- SSL: Ende zu Ende Verschlüsselung der Daten von der Webseite zum Nutzer
  - Einfach
  - Kostengünstig
  - Sicher

+ Google Ranking

https://crawler.ninja



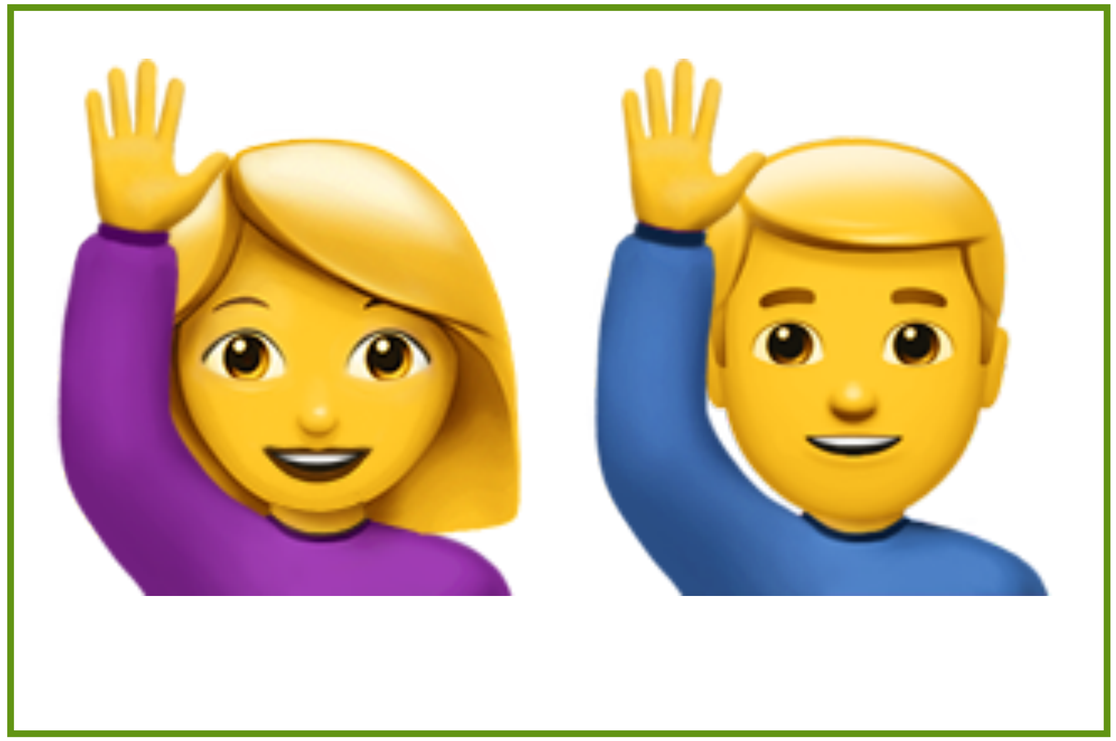
SSL Verschlüsselung. Immer.

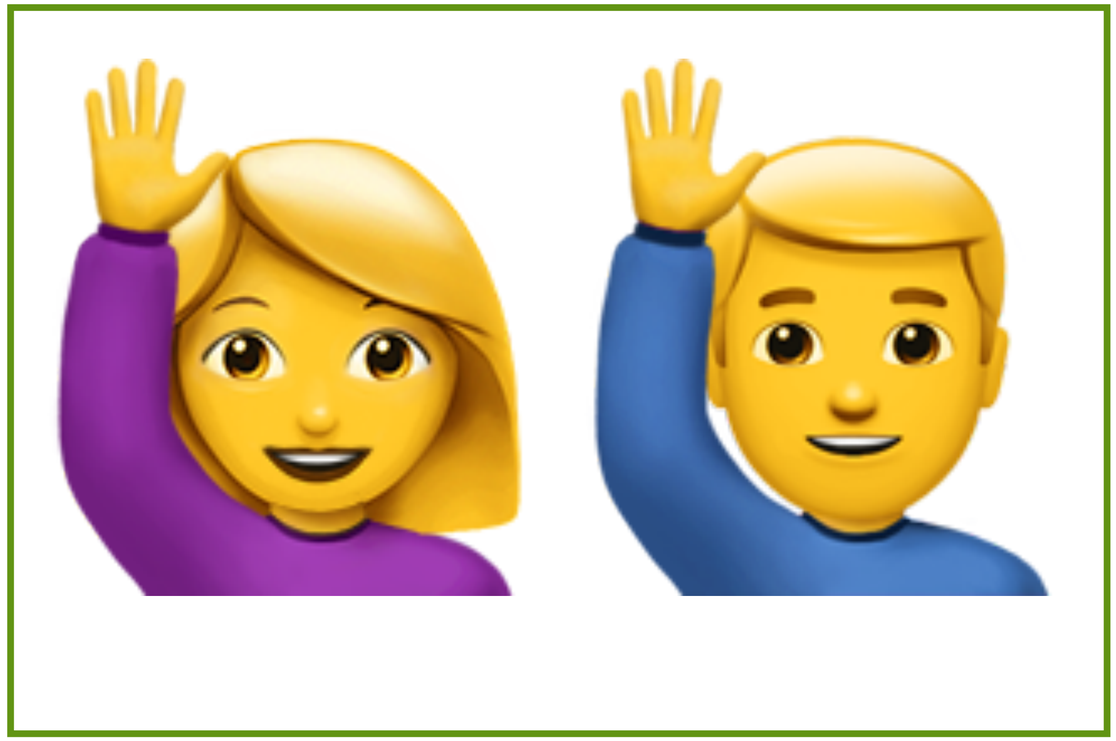
1

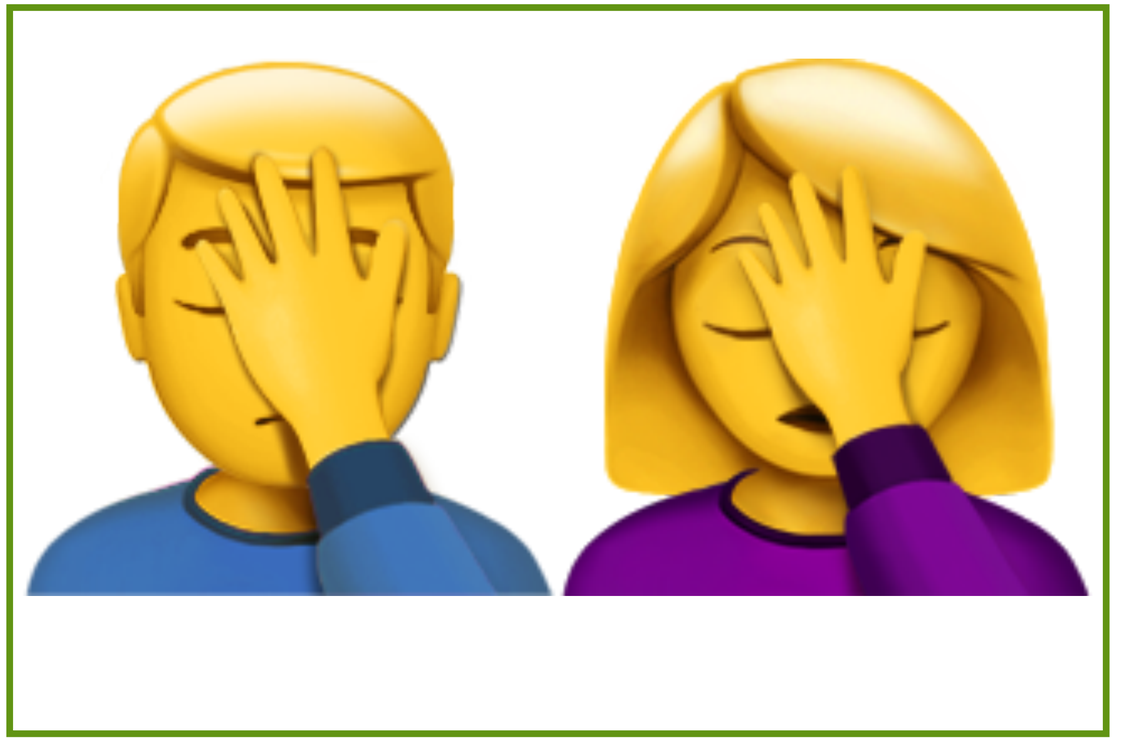
Wer kann mir mal das Passwort für das CMS geben?

Das ist doch der Geburtstag vom Geschäftsführer!

Also Nutzer „redaktion“ und Passwort „25.04.1963“







Risiken bei geteilten Zugängen

- Unkontrollierte Weitergabe der Zugangsdaten
  - Keine Zuordnung zwischen Änderung und Nutzer

Risiken bei geteilten Zugängen

- Unkontrollierte Weitergabe der Zugangsdaten
  - Keine Zuordnung zwischen Änderung und Nutzer
- Sehr hoher Aufwand bei Fluktuation
  - **wird so oder so nie gemacht!**

Risiken bei geteilten Zugängen

- Unkontrollierte Weitergabe der Zugangsdaten
  - Keine Zuordnung zwischen Änderung und Nutzer
- Sehr hoher Aufwand bei Fluktuation
  - **wird so oder so nie gemacht!**

Persönliche Accounts.

Top Ten deutscher Passwörter

HPI Hasso Plattner Institut

1. 123456	6. hallo123
2. 12345	7. hallo
3. 123456789	8. 123
4. ficken	9. passwort
5. 12345678	10. master

17.01.2019 09:59 Uhr | Security

Passwort-Sammlung mit 773 Millionen Online-Konten im Netz aufgetaucht

Eine riesige Sammlung mit Zugangsdaten zu Online-Diensten zirkuliert in Untergrund-Foren. Die Passwörter von Millionen Nutzern sind betroffen.

https://hpi.de/pressemitteilungen/2018/die-top-ten-deutscher-passwoerter.html
https://www.heise.de/security/meldung/Passwort-Sammlung-mit-773-Millionen-Online-Konten-im-Netz-aufgetaucht-4279375.html

Passwortrichtline

- Weitergabe
- Länge / Komplexität
- Nutzung
- Rotation
- Speicherung (Passwortmanager)

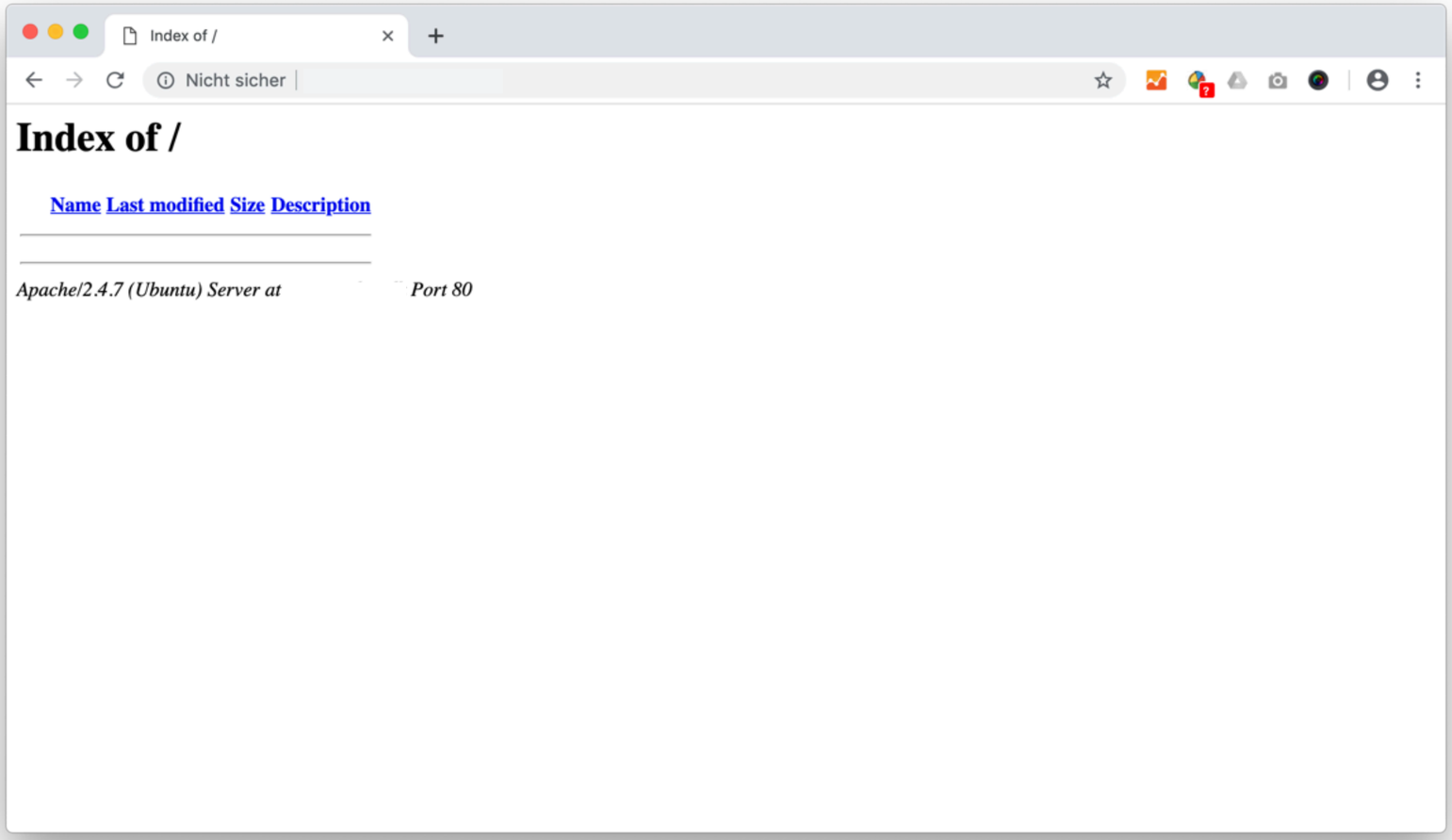
Schulung!

immer

wieder!

Persönliche Accounts.
Passwort Richtlinie.

2



Nutzer hat im FTP Client zufällig das Verzeichnis verschoben.

Zugriffsrechte

- Nur die Rechte vergeben, die für die Arbeit unbedingt notwendig sind
- Auf fachliche Qualifikation achten!
- Module, die nicht benötigt werden, nicht anzeigen!
  - Einfachere Nutzung des Backends

Passgenaue Zugriffsrechte.

3

Photo by Daria Shevtsova from Pexels

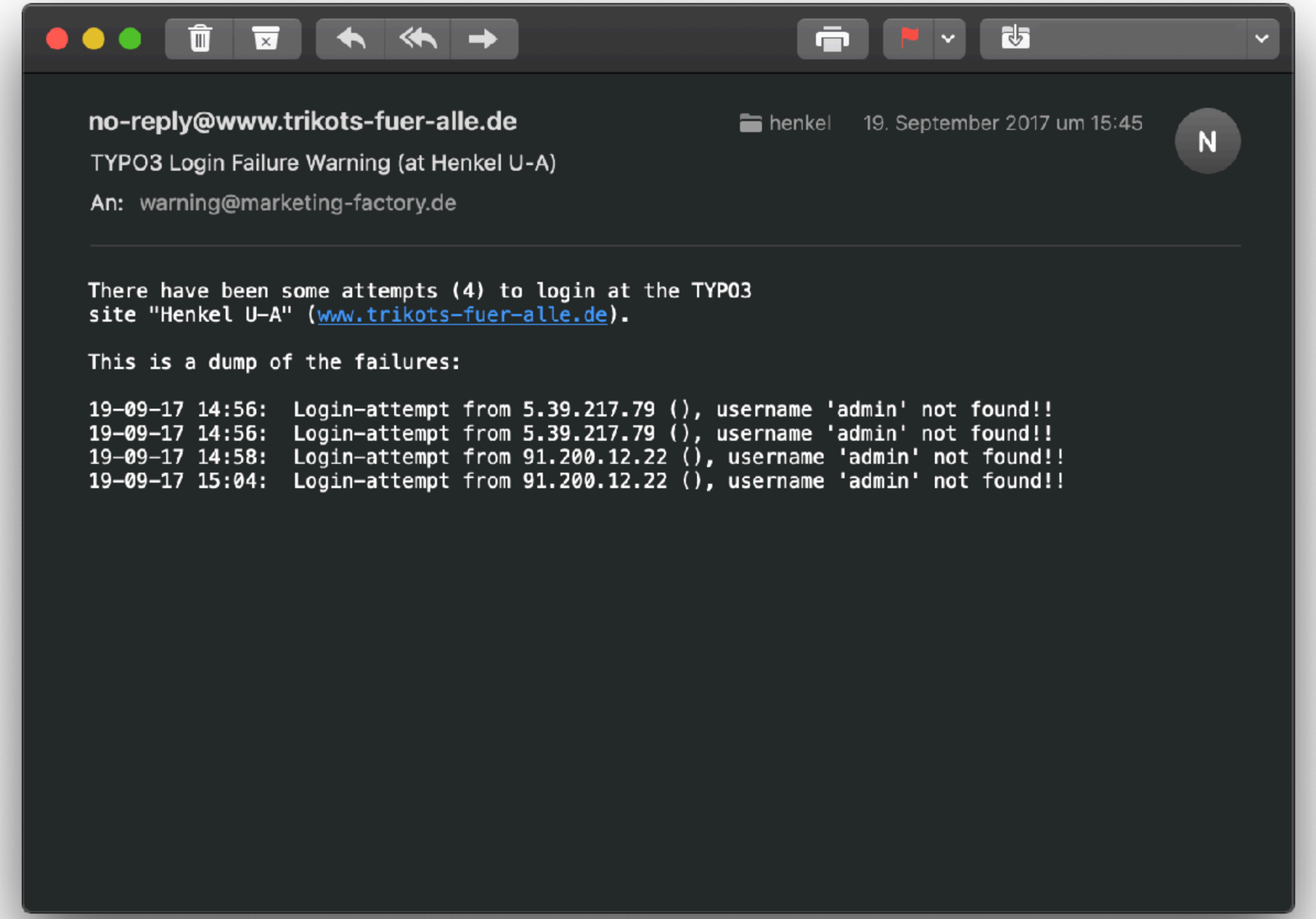
Photo by Oleksandr Pidvalnyi from Pexels

Zusätzliche Absicherung des Backends

- Einschränken des IP-Bereichs für den Login
  - IP Range des Unternehmes
  - VPN für extern
- 2-Faktor-Authentifizierung
- Single-Sign-On
- Captcha bei Login-Problemen

4

Photo credit: NASA/Lauren Harnett



no-reply@www.trikots-fuer-alle.de

henkel 19. September 2017 um 15:45

N

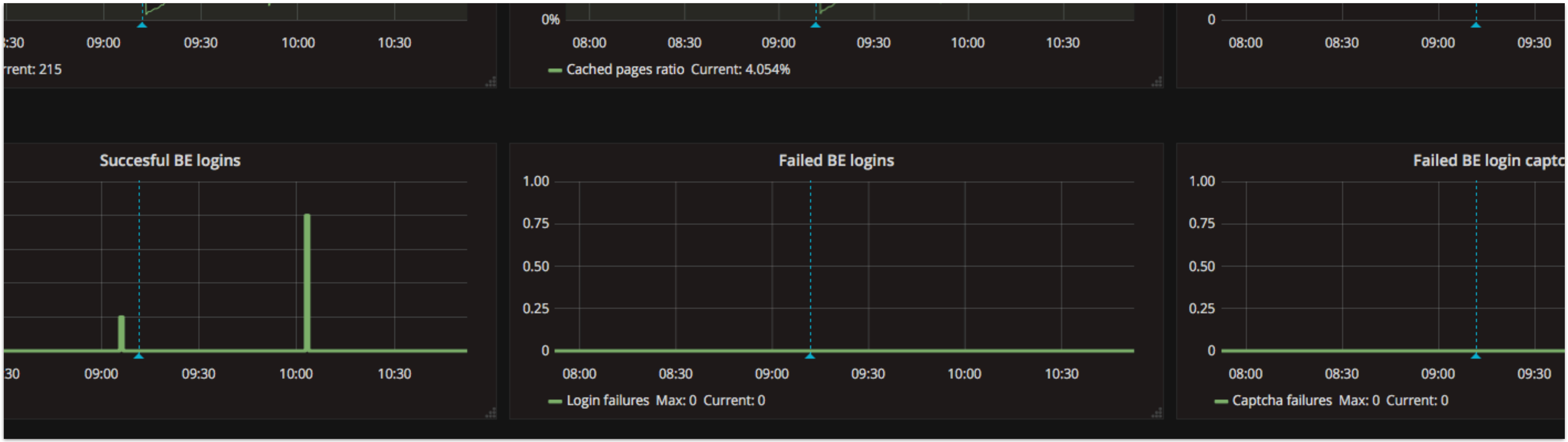
TYPO3 Login Failure Warning (at Henkel U-A)

An: warning@marketing-factory.de

There have been some attempts (4) to login at the TYPO3
site "Henkel U-A" (www.trikots-fuer-alle.de).

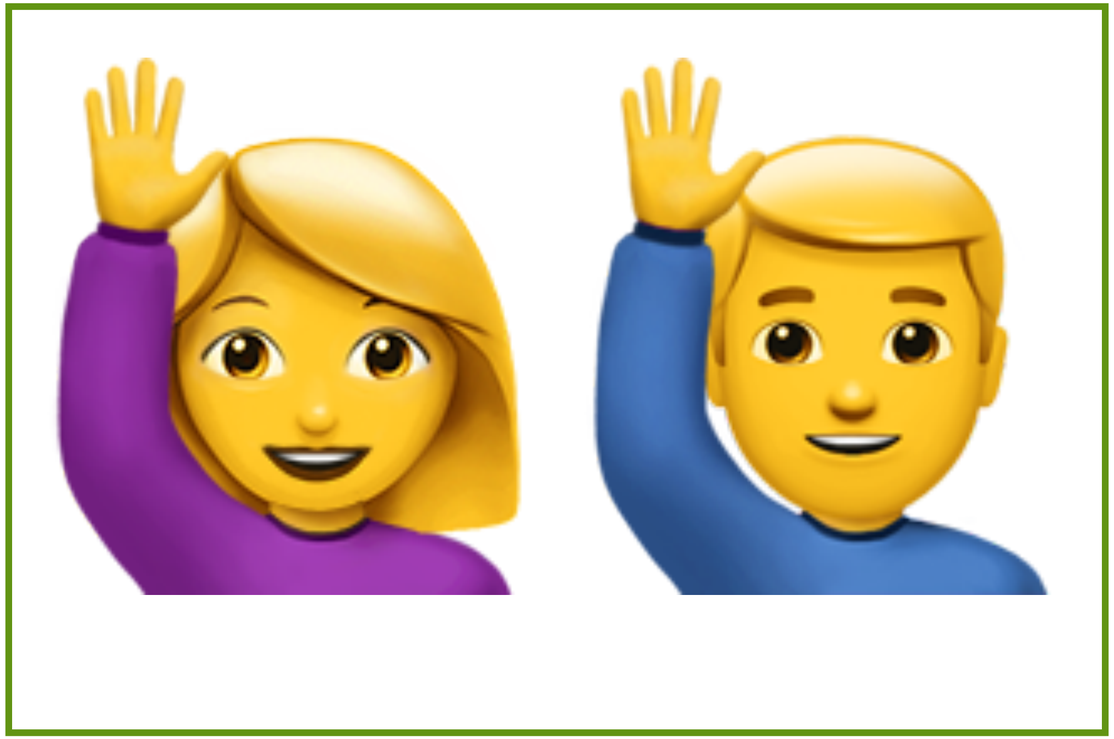
This is a dump of the failures:

19-09-17 14:56: Login-attempt from 5.39.217.79 (), username 'admin' not found!!
19-09-17 14:56: Login-attempt from 5.39.217.79 (), username 'admin' not found!!
19-09-17 14:58: Login-attempt from 91.200.12.22 (), username 'admin' not found!!
19-09-17 15:04: Login-attempt from 91.200.12.22 (), username 'admin' not found!!

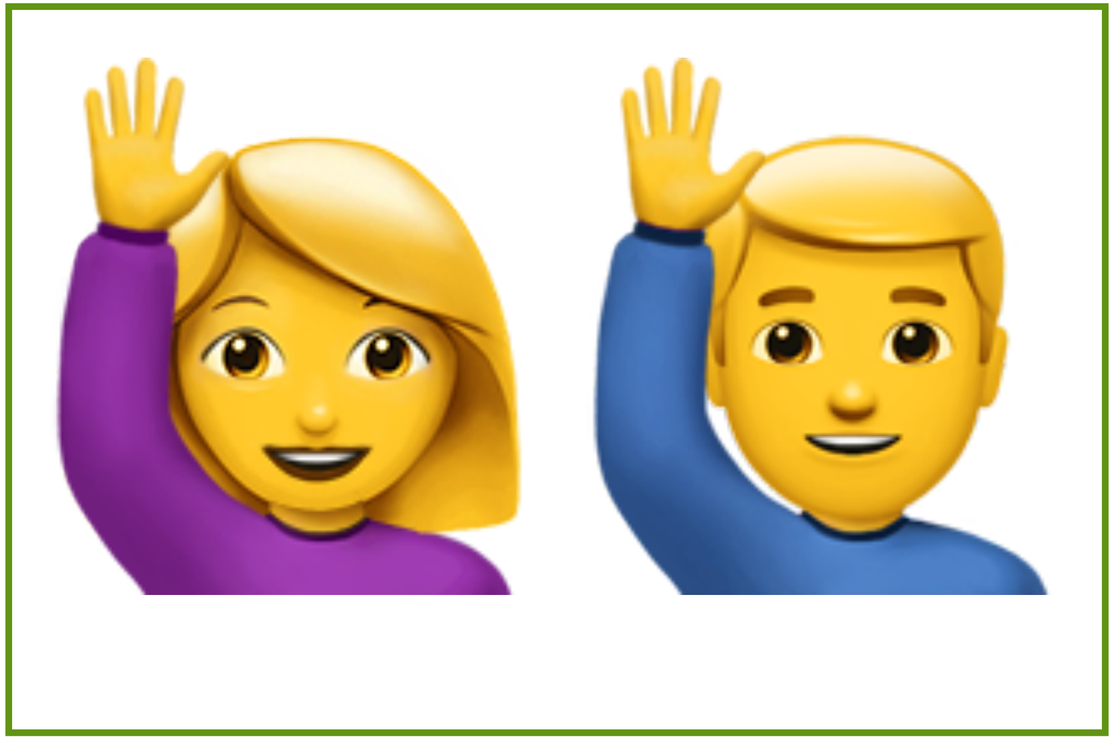

:30
09:00
09:30
10:00
10:30
rrent: 215
0%
08:00
08:30
09:00
09:30
10:00
10:30
Cached pages ratio Current: 4.054%
0
08:00
08:30
09:00
09:30
Succesful BE logins
30
09:00
09:30
10:00
10:30
Failed BE logins
1.00
0.75
0.50
0.25
0
08:00
08:30
09:00
09:30
10:00
10:30
Login failures Max: 0 Current: 0
Failed BE login captc
1.00
0.75
0.50
0.25
0
08:00
08:30
09:00
09:30
Captcha failures Max: 0 Current: 0

System monitoring.

5




Kein Backup?
Kein Mitleid.




BACKUP IS IMPORTANT
BUT RESTORE IS IMPORTANTER!

Backups und funktionierendes Restore

6

Entfernen nicht benötigter Komponenten

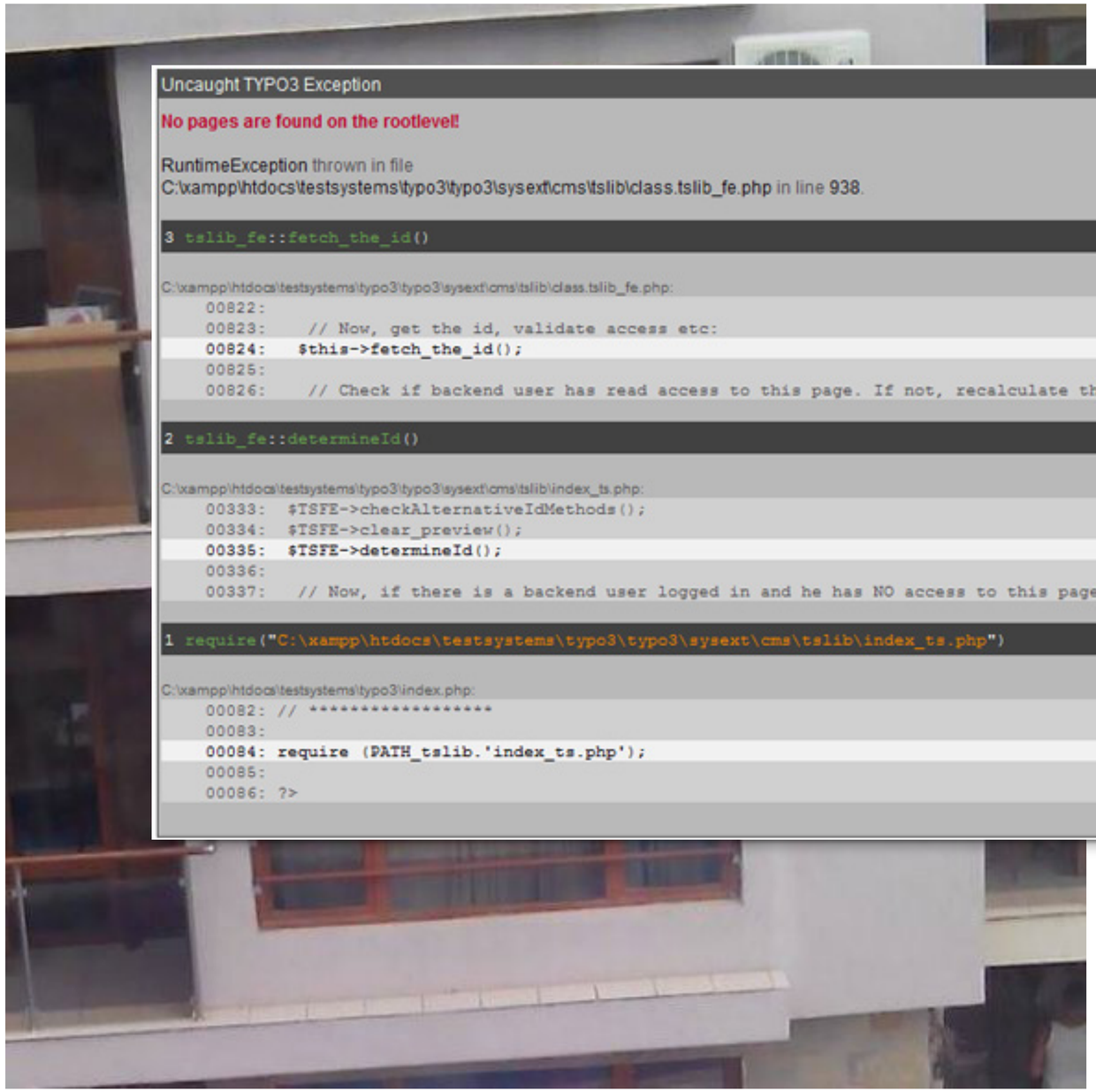
- Nicht benötige Plugins / Extensions
- Nicht benötigte Software
- Schließen nicht benötigter Ports in der Firewall

Wenig Angriffsfläche bieten.

7

Keine Entwicklung auf dem Live-System

- Stress
- Fehleranfällig
  - Webseite down
  - Webseite Verlust
  - Debug Ausgabe
  - Dateileichen



Uncaught TYPO3 Exception

No pages are found on the rootlevel!

RuntimeException thrown in file
C:\xampp\htdocs\testsystems\typo3\typo3\sysext\cms\tslib\class.tslib_fe.php in line 938.

3 tslib_fe::fetch_the_id()

C:\xampp\htdocs\testsystems\typo3\typo3\sysext\cms\tslib\class.tslib_fe.php:

```
00822:
00823:    // Now, get the id, validate access etc:
00824:   $this->fetch_the_id();
00825:
00826:    // Check if backend user has read access to this page. If not, recalculate the id.
```

2 tslib_fe::determineId()

C:\xampp\htdocs\testsystems\typo3\typo3\sysext\cms\tslib\index_ts.php:

```
00333:  $TSFE->checkAlternativeIdMethods();
00334:  $TSFE->clear_preview();
00335:  $TSFE->determineId();
00336:
00337:   // Now, if there is a backend user logged in and he has NO access to this page, then re-evaluate the id shown!
```

1 require("C:\xampp\htdocs\testsystems\typo3\typo3\sysext\cms\tslib\index_ts.php")

C:\xampp\htdocs\testsystems\typo3\index.php:

```
00082: // ******************
00083:
00084: require (PATH_tslib.'index_ts.php');
00085:
00086: ?>
```

Stress

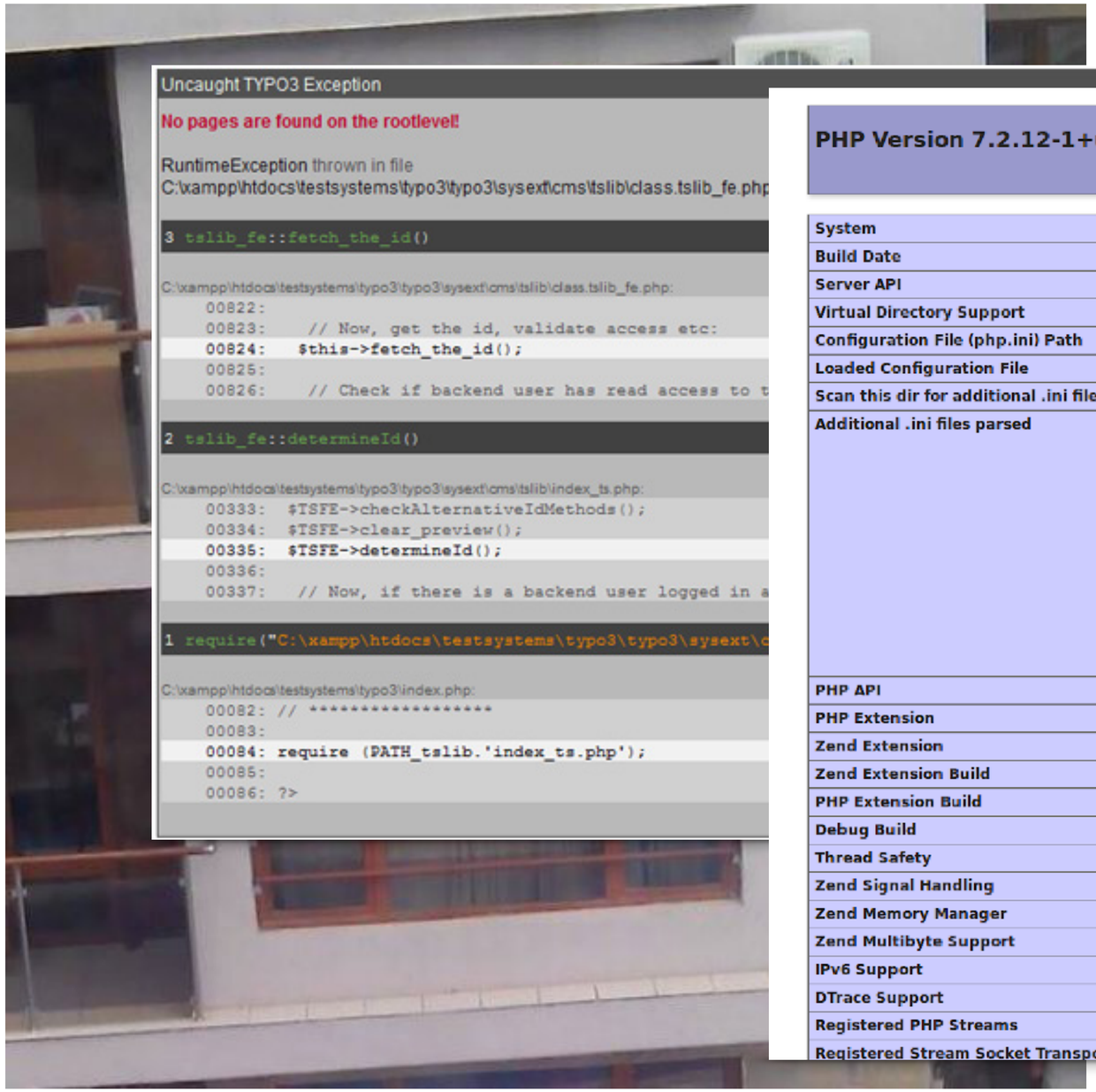
eranfällig

ebseite down

ebseite Verlust

bug Ausgabe

teileichen



Uncaught TYPO3 Exception

No pages are found on the rootlevel!

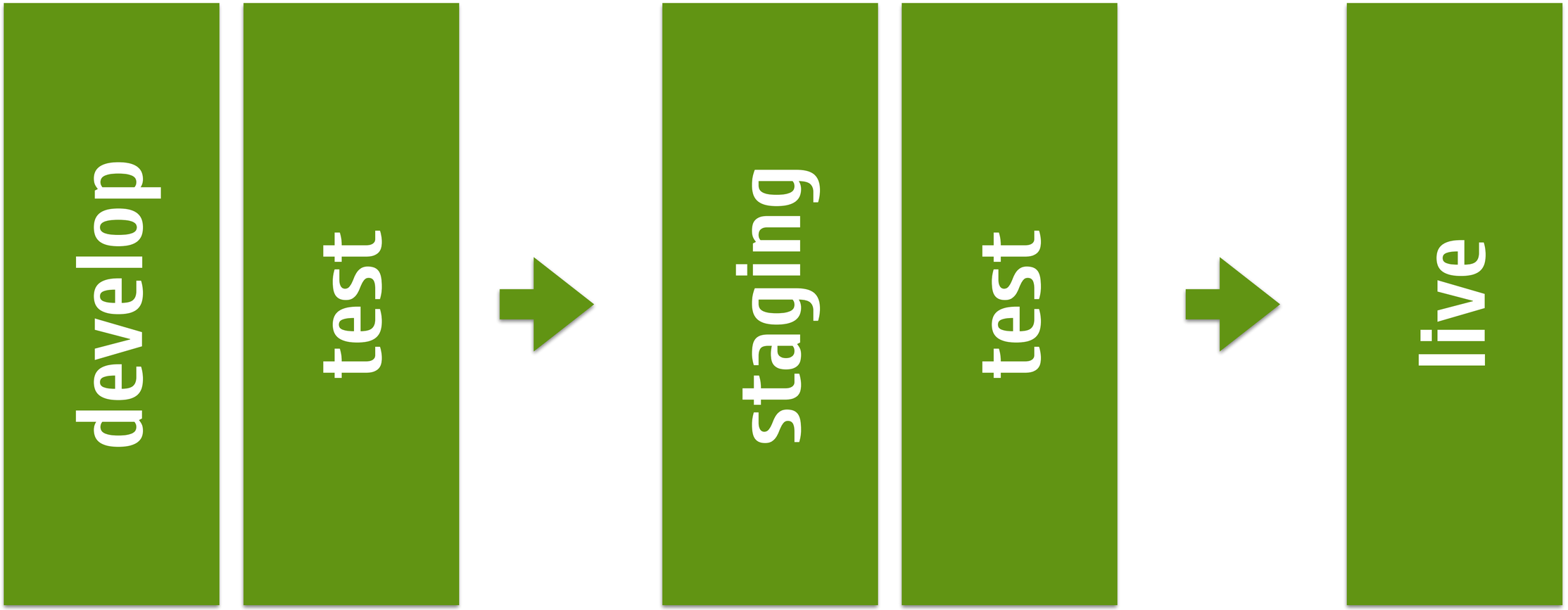
RuntimeException thrown in file
C:\xampp\htdocs\testsystems\typo3\typo3\sysext\cms\tslib\class.tslib_fe.php

```
3 tslib_fe::fetch_the_id()

C:\xampp\htdocs\testsystems\typo3\typo3\sysext\cms\tslib\class.tslib_fe.php:
    00822:
    00823:     // Now, get the id, validate access etc:
    00824:   $this->fetch_the_id();
    00825:
    00826:     // Check if backend user has read access to t

2 tslib_fe::determineId()

C:\xampp\htdocs\testsystems\typo3\typo3\sysext\cms\tslib\index_ts.php:
    00333:  $TSFE->checkAlternativeIdMethods();
    00334:  $TSFE->clear_preview();
    00335:  $TSFE->determineId();
    00336:
    00337:   // Now, if there is a backend user logged in a

1 require("C:\xampp\htdocs\testsystems\typo3\typo3\sysext\c

C:\xampp\htdocs\testsystems\typo3\index.php:
    00082: // ******************
    00083:
    00084: require (PATH_tslib.'index_ts.php');
    00085:
    00086: ?>
```

Stress

PHP Version 7.2.12-1+ubuntu16.04.1+deb.sury.org+1

System	Linux ubuntu 4.13.0-36-generic #40~16.04.1-Ubuntu SMP Fri Feb 16 23:25:58 UTC 2018 x86_64
Build Date	Nov 12 2018 09:55:12
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/15-xml.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-curl.ini, /etc/php/7.2/apache2/conf.d/20-dom.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-mbstring.ini, /etc/php/7.2/apache2/conf.d/20-mysqli.ini, /etc/php/7.2/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-simplexml.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini, /etc/php/7.2/apache2/conf.d/20-wddx.ini, /etc/php/7.2/apache2/conf.d/20-xmlreader.ini, /etc/php/7.2/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.2/apache2/conf.d/20-xsl.ini, /etc/php/7.2/apache2/conf.d/20-zip.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2


develop
test
staging
test
live

Nicht auf dem Livesystem entwickeln.

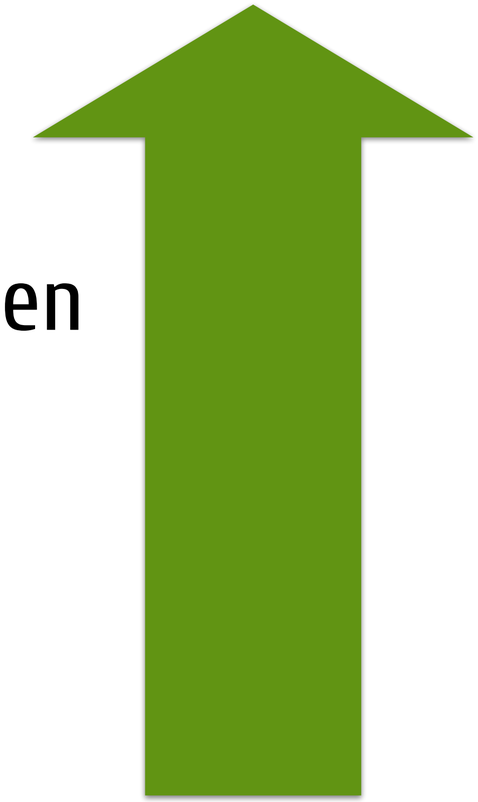
8

Teile einer Webseite

- CMS System (Core)
- Extensions / Plugins / Pakete aus öffentlichen Quellen
- Extensions / Plugins / Pakete aus privaten Quellen
- speziell entwickelte Extensions / Plugins / Pakete
- Templates und Layouts

Code Review

- CMS System (Core)
- Extensions / Plugins / Pakete aus öffentlichen Quellen
- Extensions / Plugins / Pakete aus privaten Quellen
- speziell entwickelte Extensions / Plugins / Pakete



Code Review

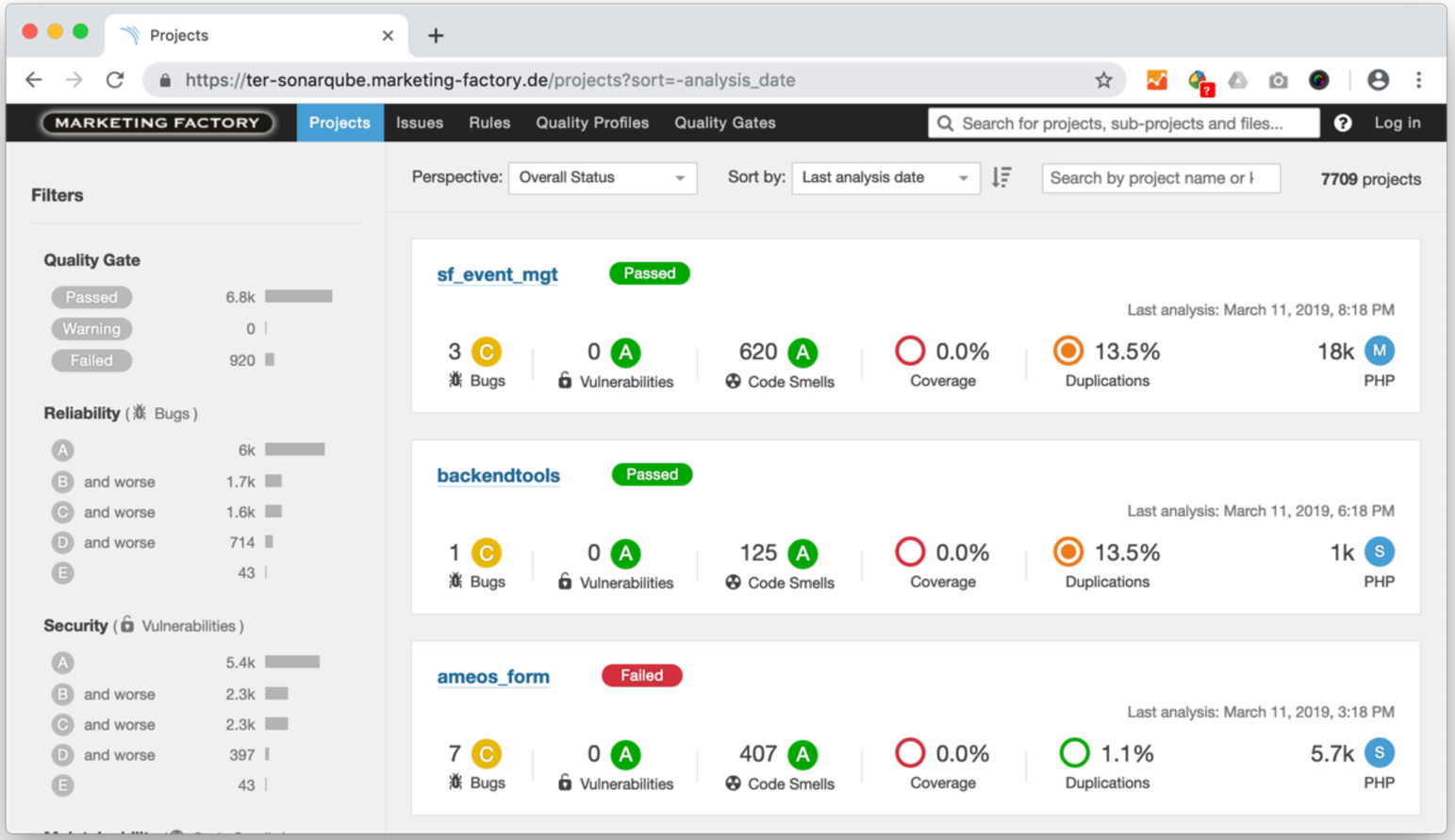
- CMS System (Core)
- Extensions / Plugins / Pakete aus öffentlichen Quellen
- Extensions / Plugins / Pakete aus privaten Quellen
- speziell entwickelte Extensions / Plugins / Pakete

Code Review

- Metriken
  - Nutzung des Plugins / Aktivität
  - Code Smells

Code Review

- Metriken
  - Nutzung des
  - Code Smells



Code Review

- Metriken
  - Nutzung des Plugins / Aktivität
  - Code Smells

Code Review

- Metriken
  - Nutzung des Plugins / Aktivität
  - Code Smells
- Unit Test

Code Review

- Metriken
  - Nutzung des Plugins / Aktivität
  - Code Smells
- Unit Test
- Code Review / Pair Programming

Code Review ist ein Teil des Entwicklungsprozess.

9

Hard Facts

- Know-How für die Anwendung von Scannern und Exploits einfach zu erlangen
- Notwendig:
  - Youtube
  - normaler Rechner mit normaler Internet-Verbindung

Diogo Constantino
@DMConstantino

Folgen

From a major CMS security team member, there's a time window of 8 to 10 hours to patch, after that you'll be automatically hacked.

#cmsgconf #FreeSoftware #Security

02:44 - 17. Nov. 2018

4 Retweets **8** „Gefällt mir“-Angaben

4 8

Core aktuell halten.

10

Hard Facts

- Know-How für die Anwendung von Scannern und Exploits einfach zu erlangen
- Notwendig:
  - Youtube
  - normaler Rechner mit normaler Internet-Verbindung

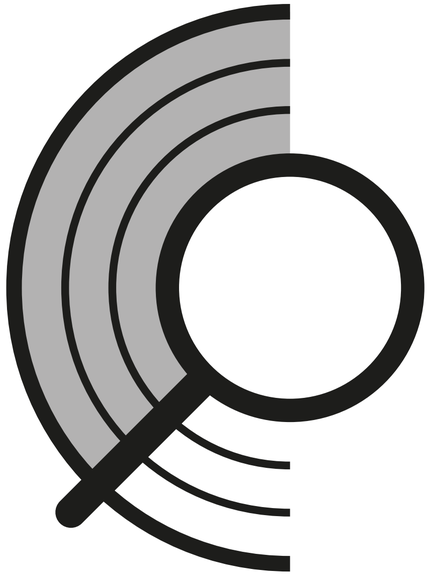

Diogo Constantino
@DMConstantino
Folgen
From a major CMS security team member, there's a time window of 8 to 10 hours to patch, after that you'll be automatically hacked.
#cmsgconf #FreeSoftware #Security
02:44 - 17. Nov. 2018
4 Retweets 8 „Gefällt mir“-Angaben
4
8

Extensions / Plugins / Pakete

- Regelmäßig aktualisieren
  - Schnelles Update bei Sicherheitsproblemen
- Abhängige Pakete ebenso aktualisieren
- Verwaiste Extensions / Plugins / Pakete ersetzen

Extensions / Plugins / Pakete aktuell halten.

bonus



SIWECOS

Auf der sicheren Seite

HACKMANIT

RUHR UNIVERSITÄT BOCHUM RUB

eco VERBAND DER INTERNETWIRTSCHAFT

cms garden

Kostenloser Check der Webseite

https://siwecos.de/

Danke!

Fragen?

cms garden

https://www.cms-garden.org

Ingo Schmitt

Twitter: @ischmitt

is@marketing-factory.de