CONTAO SICHER BETREIBEN

EIN LEITFADEN FÜR ADMINS

contao academy

Contao KONFERENZ 2023

Weltweit werden täglich
circa 30.000 Websites gehackt.

Von: **Google Search Console Team** Abbestellen
An: Christian Feneberg

13.02.16, 22:18

Message type: [WNC-633200]

Google Search Console

Gehackte Inhalte auf http://[redacted] erkannt

An: Webmaster von [redacted],

Google hat festgestellt, dass Ihre Website von Dritten gehackt wurde, die schädliche Inhalte auf einigen Ihrer Seiten erstellt haben. Dies ist ein schwerwiegendes Problem, denn der Ruf Ihrer Website wird ausgenutzt, um potenziellen Besuchern unerwartete oder schädliche Inhalte auf Ihrer Website oder in Suchergebnissen zu zeigen. Darüber hinaus wird dadurch die Qualität der Ergebnisse für Nutzer der Google-Suche gemindert. Aus diesem Grund haben wir eine manuelle Maßnahme an Ihrer Website vorgenommen. Nutzer erhalten ab sofort eine Warnung vor gehackten Inhalten, sobald Ihre Website in den Suchergebnissen erscheint. Wenn diese Warnung wieder entfernt werden soll, müssen Sie die gehackten Inhalte bereinigen und einen Antrag auf erneute Überprüfung stellen. Sobald wir feststellen konnten, dass sich auf Ihrer Website keine gehackten Inhalte mehr befinden, wird diese manuelle Maßnahme aufgehoben.

Im Folgenden finden Sie einige Beispiel-URLs mit Seiten, die offenbar manipuliert wurden. Sehen Sie sich diese Seiten an, um ein besseres Verständnis dafür zu bekommen, wo der gehackte Inhalt erscheint. Die Liste ist nicht vollständig.

[redacted]/system/scripts/ck6ourwju/akibat-tidak-memakai-celana-dalam-saat-tidur.php

So beheben Sie dieses Problem:

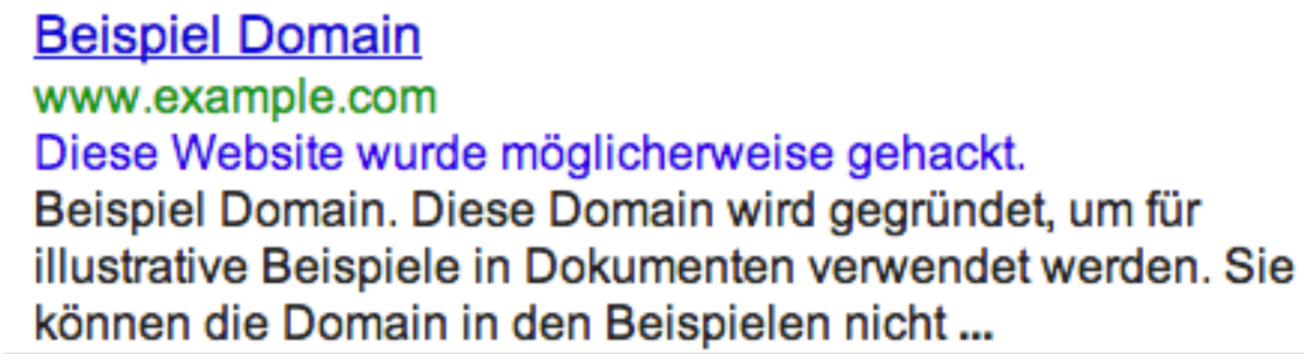
1 Details zu dem Hackerangriff unter "Sicherheitsprobleme" nachlesen

Im Bericht zu Sicherheitsproblemen der

Sicherheitsprobleme

Meldung „Diese Website wurde möglicherweise gehackt“

Die Meldung „Diese Website wurde möglicherweise gehackt“ wird angezeigt, wenn wir Grund zur Annahme haben, dass ein Hacker einen Teil der bestehenden Seiten der Website geändert oder Spamseiten hinzugefügt hat. Wenn Sie die Website besuchen, werden Sie möglicherweise zu Spam oder Malware weitergeleitet.



CHRISTIAN FENEBERG

Kempten im Allgäu

seit 2010

#Frontend #Schulung #Wartung #Support

@ChristianFene

christianfeneberg

@contaoacademy

kontakt@contao-academy.de

https://contao-academy.de

contao academy

trakked

Contao PREMIUM PARTNER

Contao TV

ASSOCIATION MEMBER

AGENDA

01 OWASP TOP 10

02 8 MASSNAHMEN FÜR MEHR SICHERHEIT

03 CONTAO SECURITY POLICY

WEBSITE GEHACKT - WAS TUN? 04

GESCHENK  05

FRAGEN 06

- Das **O**pen **W**orldwide **A**pplication **S**ecurity **P**roject (OWASP) ist eine offene Community, die sich für die Verbesserung der Sicherheit von Software einsetzt.
- Mission: „**No more insecure software**“
- https://owasp.org/
- Weltweit 250+ lokale „Chapters“
- Top 10 der häufigsten Sicherheitsrisiken für Webanwendungen

OWASP TOP 10

A01:2021	Fehler im Zugriffsmanagement
A02:2021	Kryptografische Fehler
A03:2021	Injection
A04:2021	Unsicheres Design
A05:2021	Sicherheitsrelevante Fehlkonfiguration
A06:2021	Nutzung von Komponenten mit bekannten Schwachstellen
A07:2021	Sicherheitslücken in der Authentifizierung und Sitzungsverwaltung
A08:2021	Software- und Daten Integritätsfehler
A09:2021	Unzureichendes Logging & Monitoring
A10:2021	Server-Side Request Forgery (SSRF)

https://owasp.org/Top10/

OWASP TOP 10

A01:2021	**Fehler im Zugriffsmanagement**
A02:2021	Kryptografische Fehler
A03:2021	Injection
A04:2021	Unsicheres Design
A05:2021	Sicherheitsrelevante Fehlkonfiguration
A06:2021	Nutzung von Komponenten mit bekannten Schwachstellen
A07:2021	Sicherheitslücken in der Authentifizierung und Sitzungsverwaltung
A08:2021	Software- und Daten Integritätsfehler
A09:2021	Unzureichendes Logging & Monitoring
A10:2021	Server-Side Request Forgery (SSRF)

https://owasp.org/Top10/

OWASP TOP 10

A01:2021	Fehler im Zugriffsmanagement
A02:2021	**Kryptografische Fehler**
A03:2021	Injection
A04:2021	Unsicheres Design
A05:2021	Sicherheitsrelevante Fehlkonfiguration
A06:2021	Nutzung von Komponenten mit bekannten Schwachstellen
A07:2021	Sicherheitslücken in der Authentifizierung und Sitzungsverwaltung
A08:2021	Software- und Daten Integritätsfehler
A09:2021	Unzureichendes Logging & Monitoring
A10:2021	Server-Side Request Forgery (SSRF)

https://owasp.org/Top10/

OWASP TOP 10

A01:2021	Fehler im Zugriffsmanagement
A02:2021	Kryptografische Fehler
A03:2021	**Injection**
A04:2021	Unsicheres Design
A05:2021	Sicherheitsrelevante Fehlkonfiguration
A06:2021	Nutzung von Komponenten mit bekannten Schwachstellen
A07:2021	Sicherheitslücken in der Authentifizierung und Sitzungsverwaltung
A08:2021	Software- und Daten Integritätsfehler
A09:2021	Unzureichendes Logging & Monitoring
A10:2021	Server-Side Request Forgery (SSRF)

https://owasp.org/Top10/

OWASP TOP 10

A01:2021	Fehler im Zugriffsmanagement
A02:2021	Kryptografische Fehler
A03:2021	Injection
A04:2021	**Unsicheres Design**
A05:2021	Sicherheitsrelevante Fehlkonfiguration
A06:2021	Nutzung von Komponenten mit bekannten Schwachstellen
A07:2021	Sicherheitslücken in der Authentifizierung und Sitzungsverwaltung
A08:2021	Software- und Daten Integritätsfehler
A09:2021	Unzureichendes Logging & Monitoring
A10:2021	Server-Side Request Forgery (SSRF)

https://owasp.org/Top10/

OWASP TOP 10

A01:2021	Fehler im Zugriffsmanagement
A02:2021	Kryptografische Fehler
A03:2021	Injection
A04:2021	Unsicheres Design
A05:2021	**Sicherheitsrelevante Fehlkonfiguration**
A06:2021	Nutzung von Komponenten mit bekannten Schwachstellen
A07:2021	Sicherheitslücken in der Authentifizierung und Sitzungsverwaltung
A08:2021	Software- und Daten Integritätsfehler
A09:2021	Unzureichendes Logging & Monitoring
A10:2021	Server-Side Request Forgery (SSRF)

https://owasp.org/Top10/

OWASP TOP 10

A01:2021	Fehler im Zugriffsmanagement
A02:2021	Kryptografische Fehler
A03:2021	Injection
A04:2021	Unsicheres Design
A05:2021	Sicherheitsrelevante Fehlkonfiguration
A06:2021	**Nutzung von Komponenten mit bekannten Schwachstellen**
A07:2021	Sicherheitslücken in der Authentifizierung und Sitzungsverwaltung
A08:2021	Software- und Daten Integritätsfehler
A09:2021	Unzureichendes Logging & Monitoring
A10:2021	Server-Side Request Forgery (SSRF)

https://owasp.org/Top10/

OWASP TOP 10

A01:2021	Fehler im Zugriffsmanagement
A02:2021	Kryptografische Fehler
A03:2021	Injection
A04:2021	Unsicheres Design
A05:2021	Sicherheitsrelevante Fehlkonfiguration
A06:2021	Nutzung von Komponenten mit bekannten Schwachstellen
A07:2021	**Sicherheitslücken in der Authentifizierung und Sitzungsverwaltung**
A08:2021	Software- und Daten Integritätsfehler
A09:2021	Unzureichendes Logging & Monitoring
A10:2021	Server-Side Request Forgery (SSRF)

https://owasp.org/Top10/

OWASP TOP 10

A01:2021	Fehler im Zugriffsmanagement
A02:2021	Kryptografische Fehler
A03:2021	Injection
A04:2021	Unsicheres Design
A05:2021	Sicherheitsrelevante Fehlkonfiguration
A06:2021	Nutzung von Komponenten mit bekannten Schwachstellen
A07:2021	Sicherheitslücken in der Authentifizierung und Sitzungsverwaltung
A08:2021	**Software- und Daten Integritätsfehler**
A09:2021	Unzureichendes Logging & Monitoring
A10:2021	Server-Side Request Forgery (SSRF)

https://owasp.org/Top10/

OWASP TOP 10

A01:2021	Fehler im Zugriffsmanagement
A02:2021	Kryptografische Fehler
A03:2021	Injection
A04:2021	Unsicheres Design
A05:2021	Sicherheitsrelevante Fehlkonfiguration
A06:2021	Nutzung von Komponenten mit bekannten Schwachstellen
A07:2021	Sicherheitslücken in der Authentifizierung und Sitzungsverwaltung
A08:2021	Software- und Daten Integritätsfehler
A09:2021	**Unzureichendes Logging & Monitoring**
A10:2021	Server-Side Request Forgery (SSRF)

https://owasp.org/Top10/

OWASP TOP 10

A01:2021	Fehler im Zugriffsmanagement
A02:2021	Kryptografische Fehler
A03:2021	Injection
A04:2021	Unsicheres Design
A05:2021	Sicherheitsrelevante Fehlkonfiguration
A06:2021	Nutzung von Komponenten mit bekannten Schwachstellen
A07:2021	Sicherheitslücken in der Authentifizierung und Sitzungsverwaltung
A08:2021	Software- und Daten Integritätsfehler
A09:2021	Unzureichendes Logging & Monitoring
A10:2021	**Server-Side Request Forgery (SSRF)**

https://owasp.org/Top10/

8 MASSNAHMEN FÜR MEHR SICHERHEIT

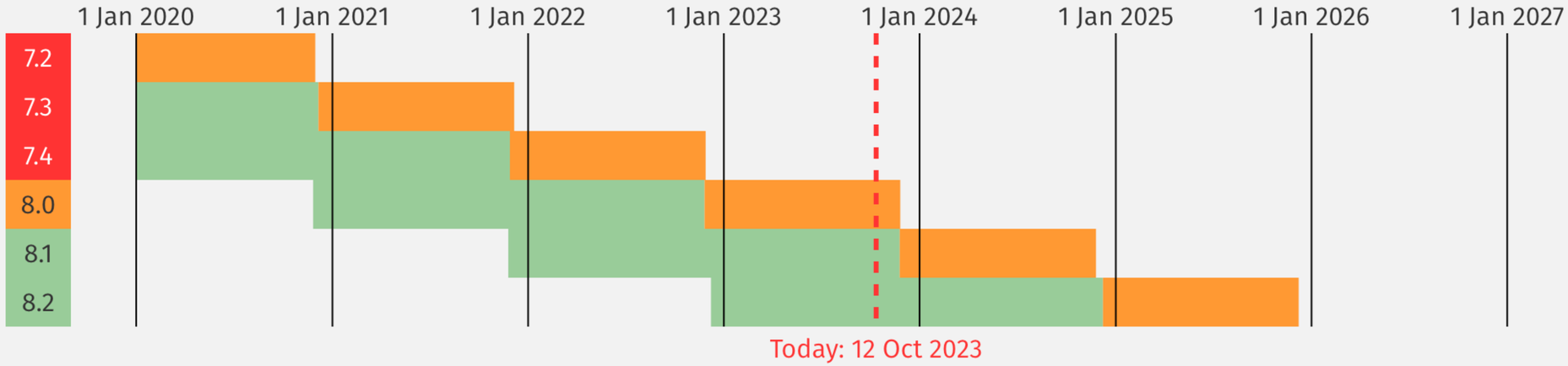
01
SERVER / HOSTING

KONFIGURATION

Currently Supported Versions

Branch	Initial Release		Active Support Until		Security Support Until	
8.0	26 Nov 2020	*2 years, 10 months ago*	26 Nov 2022	*10 months ago*	26 Nov 2023	*in 1 month*
8.1	25 Nov 2021	*1 year, 10 months ago*	25 Nov 2023	*in 1 month*	25 Nov 2024	*in 1 year, 1 month*
8.2	8 Dec 2022	*10 months ago*	8 Dec 2024	*in 1 year, 1 month*	8 Dec 2025	*in 2 years, 1 month*

Or, visualised as a calendar:



https://www.php.net/supported-versions.php

GETRENNTE SYSTEME

- Nur **ein System** pro Account
- Jeweils eine **eigene Datenbank** verwenden
- **Niemals** fremde Software (z. B. WordPress 😉, Matomo) parallel auf einem Account oder in einer Datenbank installieren
- **Minimum: eigene Datenbank, getrennte Verzeichnisstruktur!**

ZUGRIFF AUF DATEIEN SCHÜTZEN

Anzeige von Webverzeichnissen verhindern

- Konfiguration Webserver prüfen
- ggf. *.htaccess* anpassen

Keine Sicherungen im Website-Root

- Immer außerhalb des Installationsverzeichnisses
- Zugriff von außen verhindern (.htaccess)

Berechtigungen von Dateien und Ordnern

- Niemals Schreibzugriff für öffentliche Benutzer erlauben (777)
- Dateirechte auf Server mit äußerster Vorsicht verändern

02

VERSCHLÜSSELTE ÜBERTRAGUNG

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > contao-academy.de > 116.203.135.87

SSL Report: contao-academy.de (116.203.135.87)

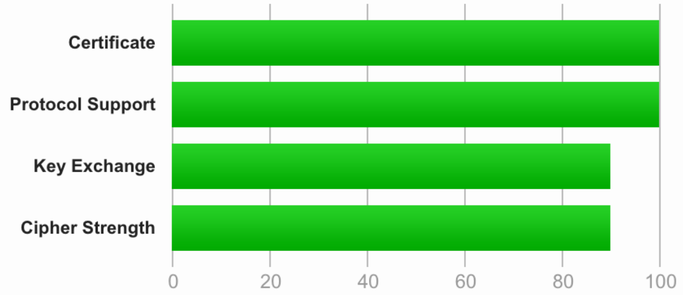
Assessed on: Thu, 12 Oct 2023 12:46:57 UTC | HIDDEN | Clear cache

Scan Another »

Summary

Overall Rating

A+



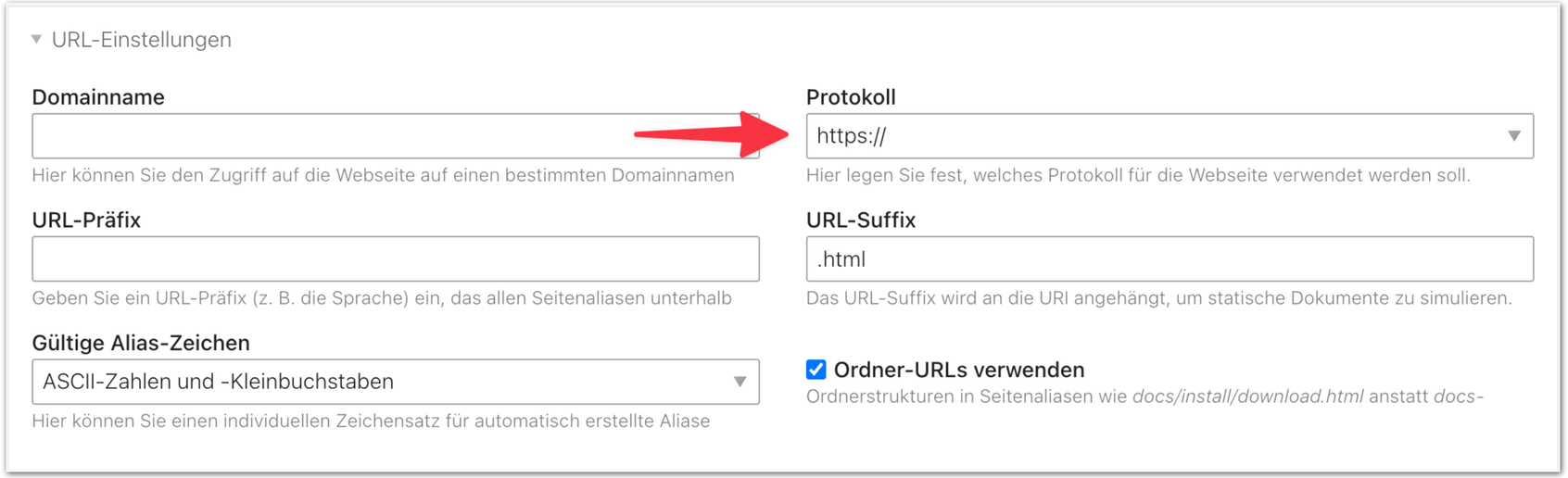
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

This server supports TLS 1.3.

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

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




```
RewriteCond %{HTTPS} !=on
RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
```

HTTP STRICT-TRANSPORT-SECURITY (HSTS)

```
Strict-Transport-Security: max-age=<expire-time>; includeSubDomains; preload
```

`max-age=<expire-time>`

The time, in seconds, that the browser should remember that a site is only to be accessed using HTTPS.

`includeSubDomains` Optional

If this optional parameter is specified, this rule applies to all of the site's subdomains as well.

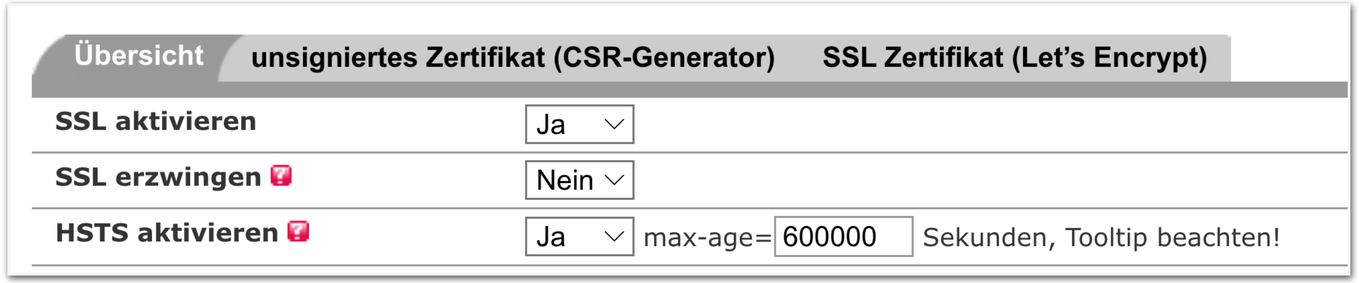
`preload` Optional ⚠

See Preloading Strict Transport Security for details. When using `preload`, the `max-age` directive must be at least `31536000` (1 year), and the `includeSubDomains` directive must be present. Not part of the specification.

VORTEILE HSTS

- Zugriff auf die Website soll nur noch über HTTPS erfolgen
- Kein 301 Redirect von HTTP zu HTTPS mehr nötig
- Information wird für längere Zeit zwischengespeichert
- HSTS Perload List aufnehmen (https://hstspreload.org/)

Control Panel des Hosters (z. B. all-inkl.)



.htaccess ()

```
# 5 Minuten zum Testen
Header set Strict-Transport-Security "max-age=300" env=HTTPS

# 1 Jahr inkl. Subdomains und preload
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload" env=HTTPS
```

Contao per config.yml

```
nelmio_security:
    forced_ssl:
        hsts_max_age: 31536000 # 1 year
        hsts_subdomains: false / true
```

ACHTUNG

- HTTPS muss fehlerfrei funktionieren (Mixed Content)
- Unbedingt auch alle Subdomain prüfen
- Wert für *`max-age`* schrittweise erhöhen (z. B. `max-age=300`)
- Fehlkonfiguration + langes Caching macht Website unerreichbar

VERSCHLÜSSELTE DATENÜBERTRAGUNG

- **Kein veraltetes FTP verwenden!**
  Unbedingt gesicherter Übertragung per FTPS oder SFTP / SSH
- SSH-Keys statt Passwörter nutzen
- SMTPS für verschlüsselte E-Mails

03
PASSWÖRTER

TOP 10 PASSWÖRTER 2022

1. 123456	6. qwertz
2. 123456789	7. ficken
3. 1Qaz2wsx3edc	8. 12345678
4. 12345	9. passwort
5. password	10. Ebels123

Quelle: https://hpi.de/

Time It Takes Using AI to Crack Your Password [2023]

# OF CHARACTER	Numbers Only	Lowercase Letters	Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	4 Seconds
7	Instantly	Instantly	22 Seconds	42 Seconds	6 Minutes
8	Instantly	3 Seconds	19 Minutes	48 Minutes	7 Hours
9	Instantly	1 Minutes	11 Hours	2 Days	2 Weeks
10	Instantly	1 Hours	4 Weeks	6 Months	5 Years
11	Instantly	23 Hours	4 Years	38 Years	356 Years
12	25 Seconds	3 Weeks	289 Years	2K Years	30K Years
13	3 Minutes	11 Months	16K Years	91K Years	2M Years
14	36 Minutes	49 Years	827K Years	9M Years	187M Years
15	5 Hours	890 Years	47M Years	615M Years	14Bn Years
16	2 Days	23K Years	2Bn Years	26Bn Years	1Tn Years
17	3 Weeks	812K Years	539.72M Years	2Tn Years	95Tn Years
18	10 Months	22M Years	7.23Bn Years	96Tn Years	6Qn Years

(Bild: Home Security Heroes)

Managen statt merken!

1Password

LastPass

DASHLANE

Sticky Password

KeePass

bitwarden

Enpass

KEEPER
Cybersecurity Starts Here®

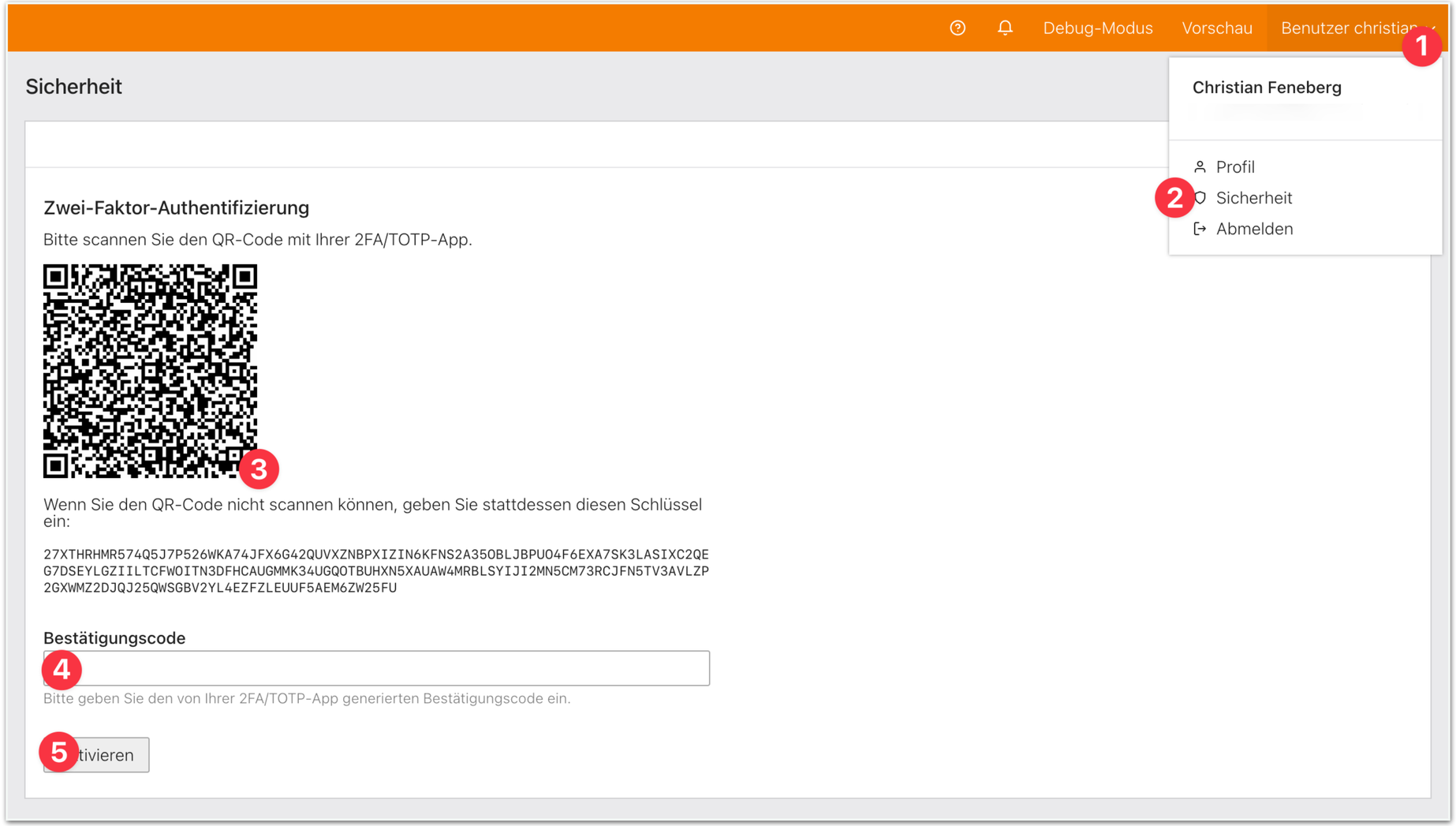
RoboForm

NordPass®

VORTEIL PASSWORTMANAGER

- Nur ein sicheres **Master-Passwort** merken
- Verwahren von Passwörtern und Benutzernamen mittels Verschlüsselung
- Passwortgenerator
- Warnung vor gefährdeten Websites und möglichen Phishing-Attacken (Watchtower, haveibeenpwned, …)
- Synchronisieren zwischen verschiedenen Geräte möglich
- Anmeldedaten automatisch ausfüllen (Autofill)

ZWEI-FAKTOR-AUTHENTIFIZIERUNG (2FA)



Anmelden

christian

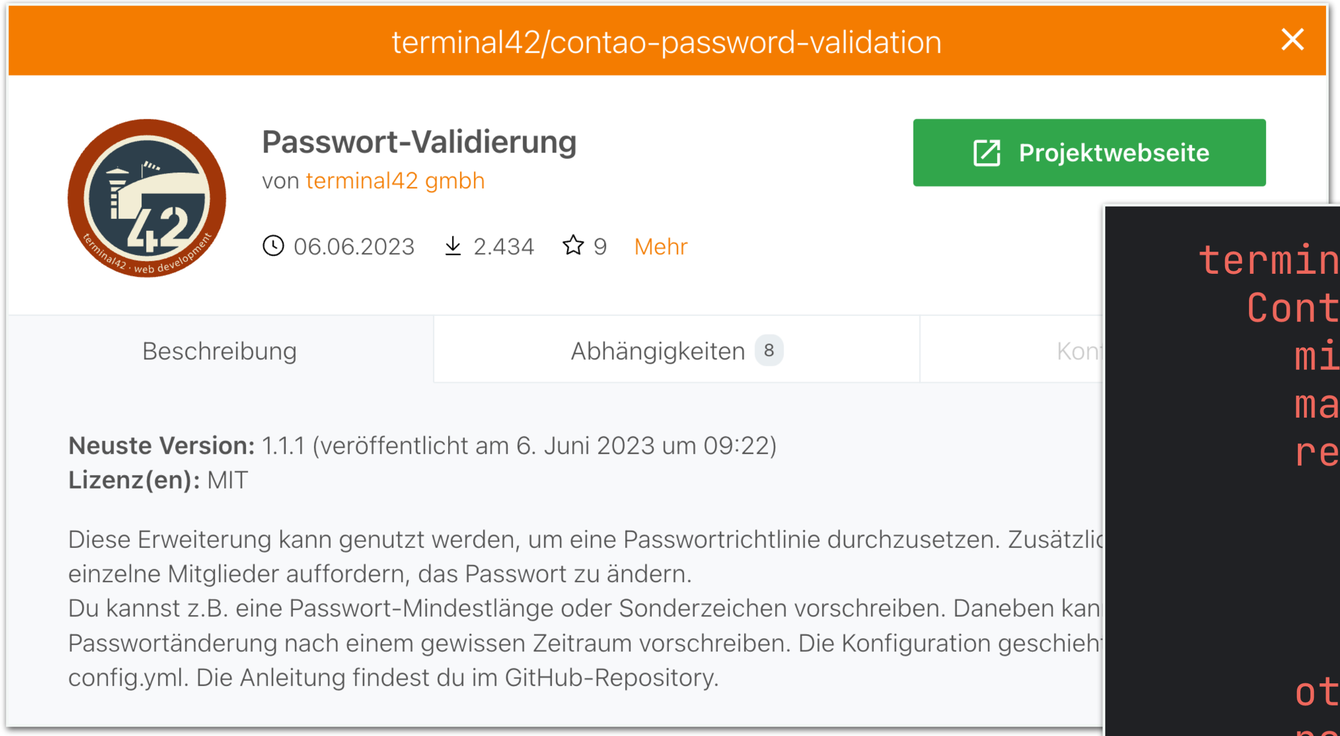
Weiter

Zum Frontend ›

2FA FÜR ALLE BACKEND-BENUTZER ERZWINGEN

```yaml
# config/config.yml
contao:
    security:
        two_factor:
            enforce_backend: true
```

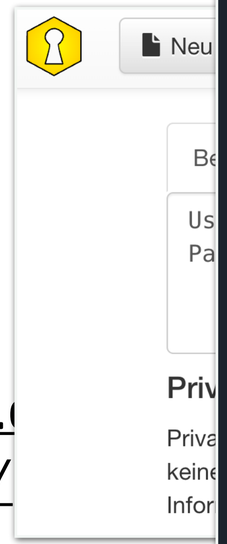
PASSWORTRICHTLINIEN DURCHSETZEN

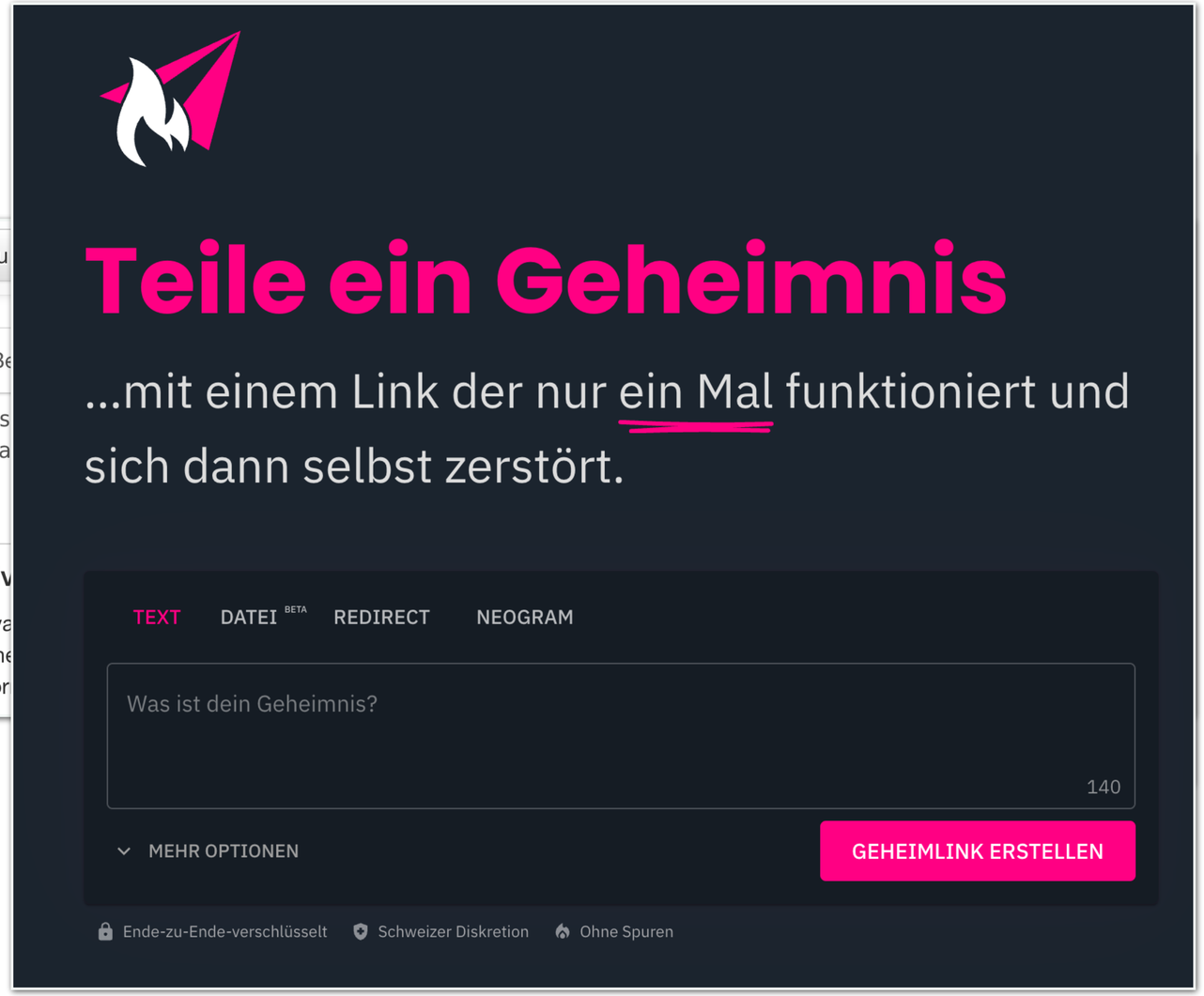



```yaml
terminal42_password_validation:
  Contao\FrontendUser:
    min_length: 10
    max_length: 20
    require:
      uppercase: 1
      lowercase: 1
      numbers: 1
      other: 1
    other_chars: "+*ç%&/()=?"
    password_history: 10
    change_days: 90
    haveibeenpwned: 1
  Contao\BackendUser:
    min_length: 10
    haveibeenpwned: 1
```

PASSWÖRTER SICHER TEILEN

- **Passwortmanager**
- **PrivateBin**
- **Online-Dienste**
  https://yopass.se/
  https://scrt.link/
  https://onetimesecret.
  https://password.link/
  https://pwpush.com/
  https://sicher-teilen.de/





PASSWÖRTER

- ✓ Lange Passwörter nutzen
- ✓ Nicht im Klartext speichern
- ✓ Passwortmanager verwenden
- ✓ Pro Installation ein einzigartiges und sicheres Passwort festlegen
- ✓ Zwei-Faktor-Authentifizierung aktivieren (Backup-Codes!)
- ✓ No-Go: Passwörter im Klartext versenden!

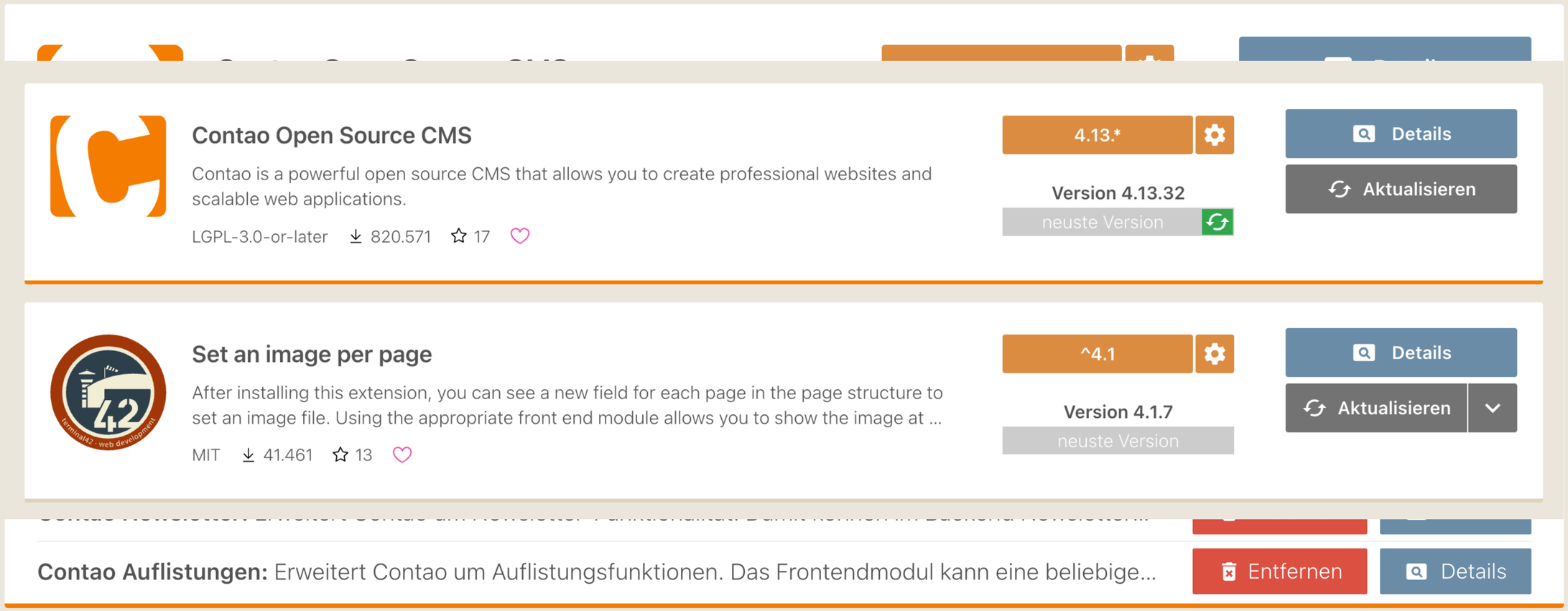
04
BENUTZER

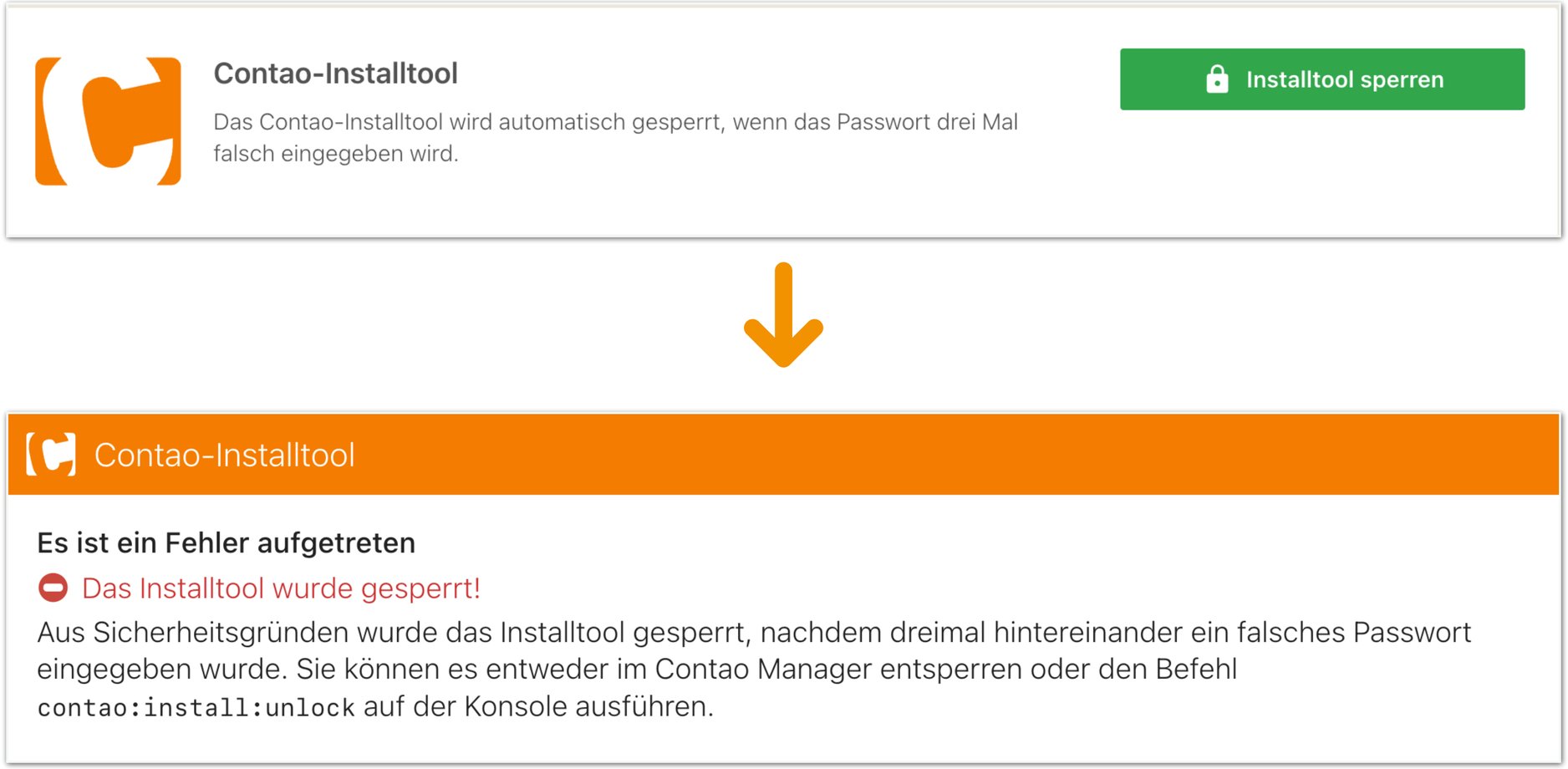
BENUTZER

- ✓ Eigene Benutzer pro Person anlegen (Contao, Hosting, SFTP)
- ✓ Keine Default-Benutzernamen (admin, administrator, …)
- ✓ So wenig Admins wie nötig
- ✓ Rechte für Anwender einschränken
- ✓ Inaktive Konten löschen
- ✓ Ablaufdatum für temporäre Benutzer festlegen
- ✓ Regelmäßig überprüfen!

05

KOMPONENTEN DEAKTIVIEREN


Contao Open Source CMS
Contao is a powerful open source CMS that allows you to create professional websites and scalable web applications.
LGPL-3.0-or-later
820.571
17
4.13.*
Version 4.13.32
neuste Version
Details
Aktualisieren
Set an image per page
After installing this extension, you can see a new field for each page in the page structure to set an image file. Using the appropriate front end module allows you to show the image at ...
MIT
41.461
13
^4.1
Version 4.1.7
neuste Version
Details
Aktualisieren
Contao Auflistungen: Erweitert Contao um Auflistungsfunktionen. Das Frontendmodul kann eine beliebige...
Entfernen
Details


Contao-Installtool
Das Contao-Installtool wird automatisch gesperrt, wenn das Passwort drei Mal falsch eingegeben wird.
Installtool sperren
Contao-Installtool
Es ist ein Fehler aufgetreten
Das Installtool wurde gesperrt!
Aus Sicherheitsgründen wurde das Installtool gesperrt, nachdem dreimal hintereinander ein falsches Passwort eingegeben wurde. Sie können es entweder im Contao Manager entsperren oder den Befehl contao:install:unlock auf der Konsole ausführen.

KOMPONENTEN DEAKTIVIEREN

- ✓ Ungenutzte **Core-Pakete entfernen** (News, Events, Newsletter, …)
- ✓ Ungenutzte **Erweiterungen entfernen**
- ✓ Ungenutzte **Bibliotheken deaktivieren / entfernen** (jQuery, jQuery-UI, Mootools, …)
- ✓ Installtool sperren (entfällt ab Contao 5)
- ✓ FTP-Zugang deaktivieren
- ✓ SSH-Zugang nur bei Bedarf aktivieren

06

PATCH-MANAGEMENT

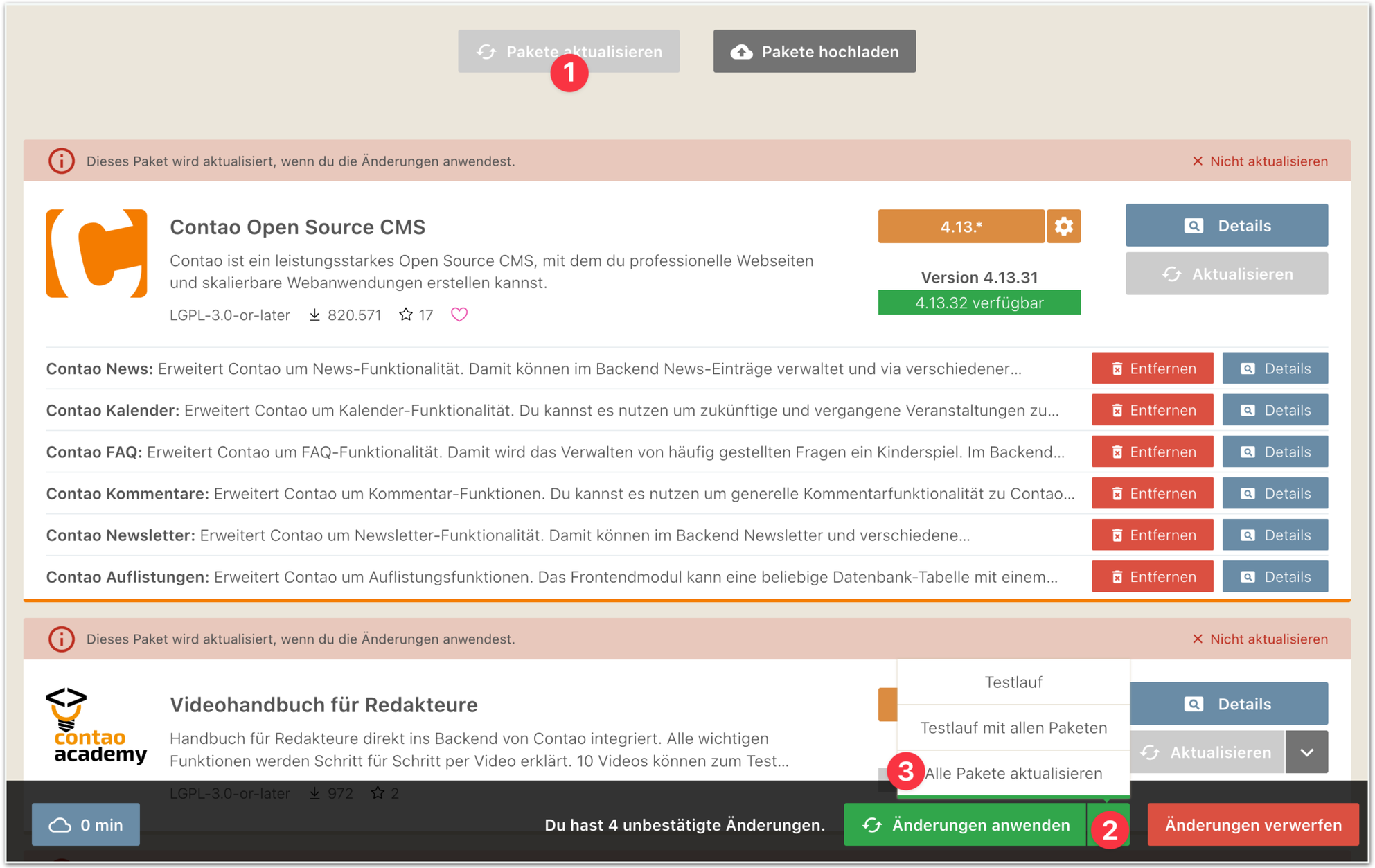
«CONTAO IST SICHER!»

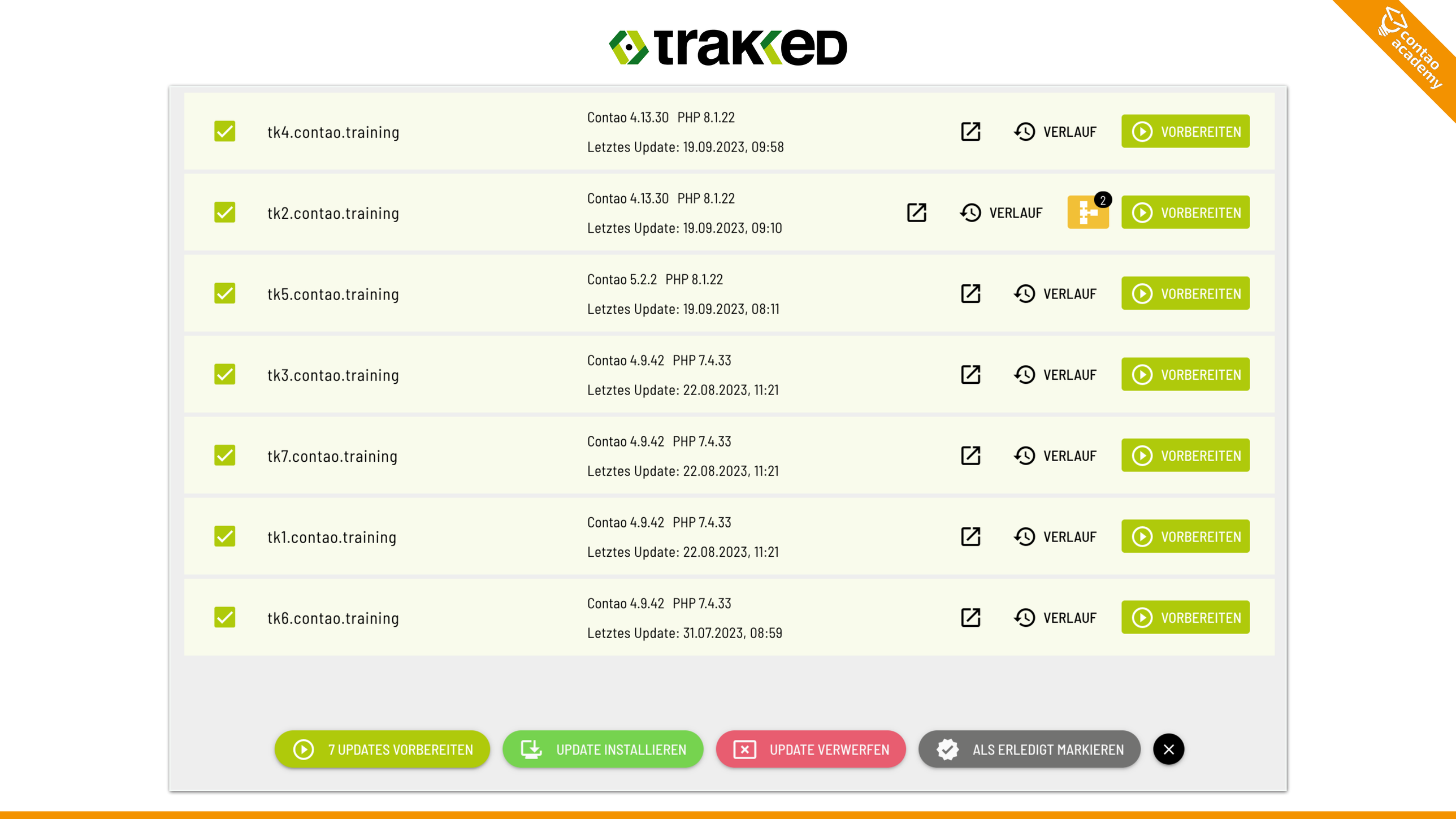
CONTAO UND SEINE ABHÄNGIGKEITEN

- mehr als 180 Pakte (symfony, doctrine, twig,)

```
composer.phar show contao/core-bundle --tree
```

- jedes Paket kann Sicherheitslücken und Fehler enthalten
- Manuell hochgeladenen Erweiterungen


Pakete aktualisieren
1
Pakete hochladen
Dieses Paket wird aktualisiert, wenn du die Änderungen anwendest.
Nicht aktualisieren
Contao Open Source CMS
Contao ist ein leistungsstarkes Open Source CMS, mit dem du professionelle Webseiten und skalierbare Webanwendungen erstellen kannst.
LGPL-3.0-or-later
820.571
17
4.13.*
Version 4.13.31
4.13.32 verfügbar
Details
Aktualisieren
Contao News: Erweitert Contao um News-Funktionalität. Damit können im Backend News-Einträge verwaltet und via verschiedener...
Contao Kalender: Erweitert Contao um Kalender-Funktionalität. Du kannst es nutzen um zukünftige und vergangene Veranstaltungen zu...
Contao FAQ: Erweitert Contao um FAQ-Funktionalität. Damit wird das Verwalten von häufig gestellten Fragen ein Kinderspiel. Im Backend...
Contao Kommentare: Erweitert Contao um Kommentar-Funktionen. Du kannst es nutzen um generelle Kommentarfunktionalität zu Contao...
Contao Newsletter: Erweitert Contao um Newsletter-Funktionalität. Damit können im Backend Newsletter und verschiedene...
Contao Auflistungen: Erweitert Contao um Auflistungsfunktionen. Das Frontendmodul kann eine beliebige Datenbank-Tabelle mit einem...
Entfernen
Details
Dieses Paket wird aktualisiert, wenn du die Änderungen anwendest.
Nicht aktualisieren
Videohandbuch für Redakteure
Handbuch für Redakteure direkt ins Backend von Contao integriert. Alle wichtigen Funktionen werden Schritt für Schritt per Video erklärt. 10 Videos können zum Test...
LGPL-3.0-or-later
972
2
Testlauf
Testlauf mit allen Paketen
3
Alle Pakete aktualisieren
Details
Aktualisieren
0 min
Du hast 4 unbestätigte Änderungen.
Änderungen anwenden
2
Änderungen verwerfen


trakked
tk4.contao.training
Contao 4.13.30 PHP 8.1.22
Letztes Update: 19.09.2023, 09:58
VERLAUF
VORBEREITEN
tk2.contao.training
Contao 4.13.30 PHP 8.1.22
Letztes Update: 19.09.2023, 09:10
VERLAUF
2
VORBEREITEN
tk5.contao.training
Contao 5.2.2 PHP 8.1.22
Letztes Update: 19.09.2023, 08:11
VERLAUF
VORBEREITEN
tk3.contao.training
Contao 4.9.42 PHP 7.4.33
Letztes Update: 22.08.2023, 11:21
VERLAUF
VORBEREITEN
tk7.contao.training
Contao 4.9.42 PHP 7.4.33
Letztes Update: 22.08.2023, 11:21
VERLAUF
VORBEREITEN
tk1.contao.training
Contao 4.9.42 PHP 7.4.33
Letztes Update: 22.08.2023, 11:21
VERLAUF
VORBEREITEN
tk6.contao.training
Contao 4.9.42 PHP 7.4.33
Letztes Update: 31.07.2023, 08:59
VERLAUF
VORBEREITEN
7 UPDATES VORBEREITEN
UPDATE INSTALLIEREN
UPDATE VERWERFEN
ALS ERLEDIGT MARKIEREN
contao academy


Wer installiert
regelmäßig Updates?

CONTAO SECURITY POLICY

- Was bedeutet **Responsible Disclosure**?
- Muss ich jedes Sicherheitsupdate einspielen?
- Contao Security Policy
  https://github.com/contao/contao/security

PROZESS SICHERHEITSLÜCKE SCHLIESSEN

01

Meldung an security@contao.org

02

Lücke validieren + Bestätigung an Reporter senden

03

Patch für Lücke erstellen

04

CVE Nummer von mitre.org

05

Ankündigung auf contao.org

06

Patch zur Prüfung an Reporter

07

Patchen aller gepflegten Versionen

08

Neues Release veröffentlichen

09

Bekanntgabe auf contao.org

10

Update PHP Security Advisories Database

WIE ERFAHRE ICH VON UPDATES?

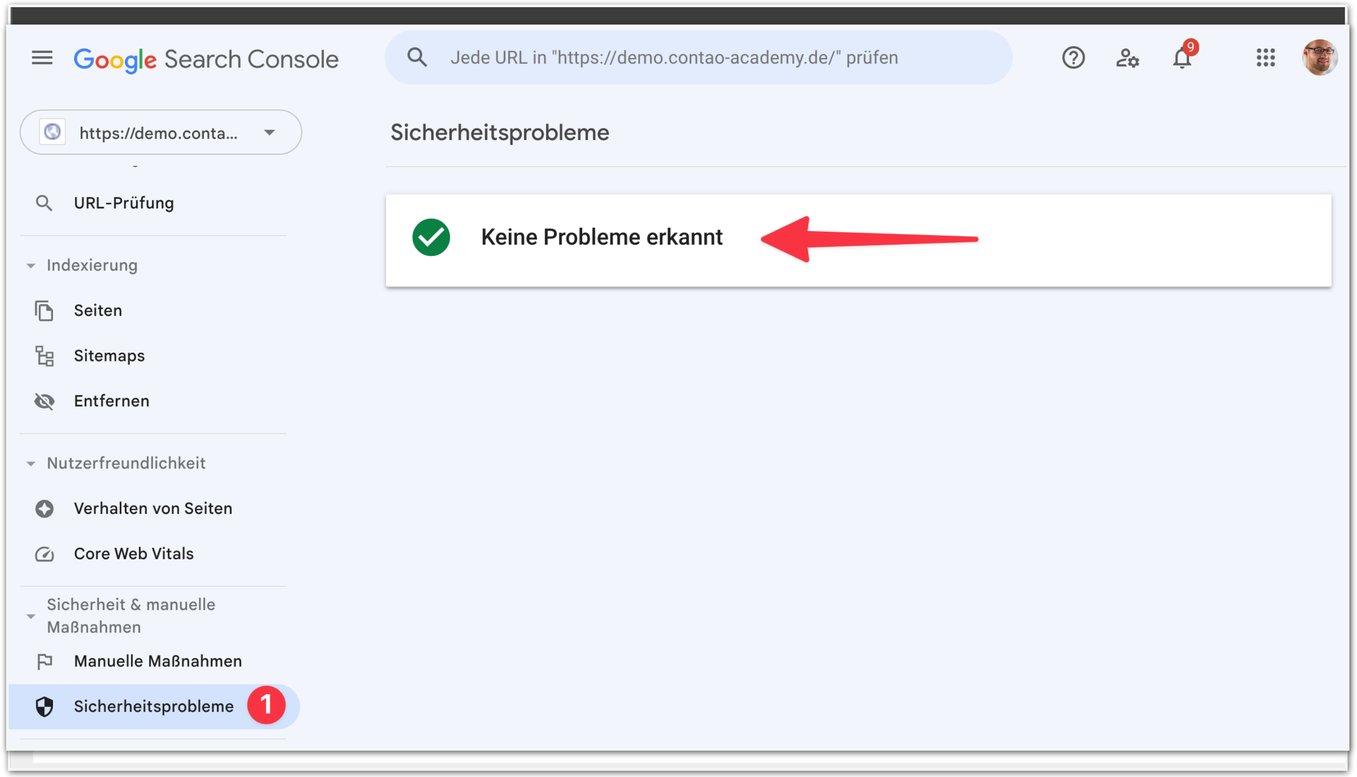
- contao.org (keine News für Bugfix-Releases)
- Social Media (Twitter / X)
- RSS-Feed (Packagist + IFTTT)
- trakked.io (Blog / Kunden direkt per E-Mail)

«Bitte vereinbart einen Update-Service mit Euren Kunden!»

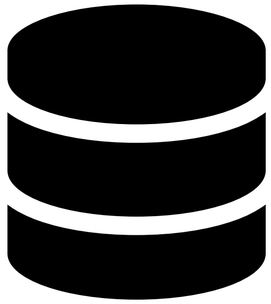
07
MONITORING

MONITORING TOOLS

- trakked 😉
- Google Search Console
- Sentry
- Uptime Robot
- …

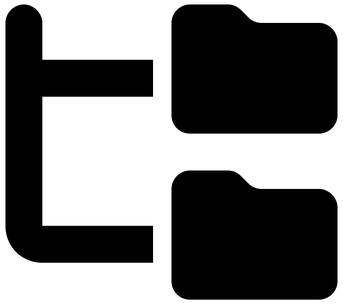


08
BACKUP



DATENBANK

+



DATEIEN

DATENBANK-BACKUP

- mysqldump -h localhost -u username -p -r databasename
- php vendor/bin/contao-console contao:backup:create
- Browser per *phpMyAdmin*
- Backup-Tools des Hosters

CONTAO DATEIEN

Datei / Verzeichnis	Erklärung
`config/`	Konfigurationsdateien der Applikation
`contao-manager/users.json`	User Contao Manager (optional)
`files/`	Dateien, die über den Dateimanager verwaltet werden
`system/config/localconfig`	Nötig für die Contao 3 Kompatibilität
`templates/`	Angepasste Contao Templates
`composer.json`	Projekt-Konfiguration, welche Pakete und Versionen zur Contao Installation gehören und installiert werden dürfen
`composer.lock`	Vollständige Liste aller Pakete und Abhängigkeiten
`.env.local`	Konfigurationsdatei der Applikation (Contao 5)

FALLS VORHANDEN

Datei / Verzeichnis	Erklärung
`contao/`	Anpassungen an Contao (z. B. DCA-Felder, Sprachdateien)
`src/`	Individuelle Programmierungen für Contao
`system/modules/*`	Alte Contao 3 Module
`public/*` bzw. `web/*`	Einzelne Dateien (z. B. .htaccess, Google Search Console File)

WEITERE MASSNAHMEN

01 Contao Manager umbenennen

02 Backend-URL umbenennen

03 Contao Manager sperren

04 Content Security Policy (CSP)

05 Passwortschutz per .htaccess

06 IP-Adressen einschränken

WEBSITE GEHACKT - WAS TUN?

1. **Keine Panik!** » überlegt und ruhig regieren!
2. Webseite umgehend in **Wartungsmodus versetzen** bzw. komplette Domain umleiten
   (NICHT löschen, Beweise sichern!)
3. **Webhoster informieren** und um Unterstützung bitten
4. Geräte auf **Viren und Malware prüfen** (eigene + Kunden)
5. **Alle Passwörter ändern** und neutrales Gerät verwenden
   Backend, Datenbank, (S)FTP, Hosting-Account, E-Mail, usw.)
6. **Analyse des Hacks** und die Lücke finden (Profi beauftragen)
7. Webseite aus **Backup vor dem Hack wiederherstellen**
8. **Lücke schließen** und alle **fehlenden Updates einspielen**
9. Website **online schalten**
10. Warnung bei **Google Search Console** beheben / Spam Blocklist prüfen
11. Einhalten erforderlicher Meldepflichten (DSGVO)

WORAUF DEN FOKUS LEGEN?

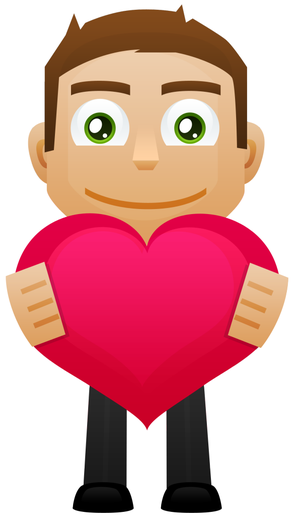
01 **REGELMÄSSIGE UPDATES**
Contao inkl. aller Abhängigkeiten

02 **PASSWÖRTER**
Passwortmanager + 2FA

03 **SICHERE DATENÜBERTRAGUNG**
SSL-Zertifikat und SFTP / SSH verwenden

https://fene.link/ck23

FRAGEN



DANKE!

Christian Feneberg
https://contao-academy.de
kontakt@contao-academy.de