WACON Internet GmbH

TYPO3 Sicherheit

TYPO3 Websites sicher betreiben

Letzte Änderung: 30.11.2021

Über den Autor

Oliver Wassenaar

Geschäftsführer, WACON Internet GmbH

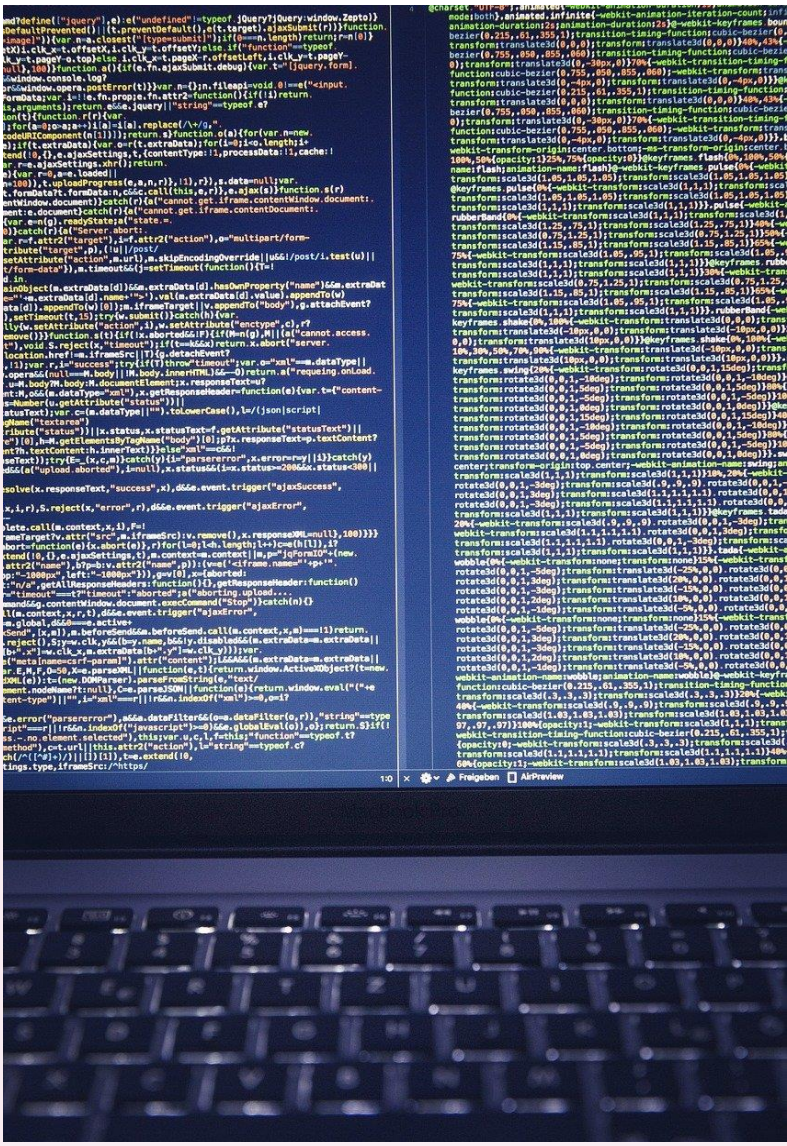
Die Die WACON Internet GmbH ist eine Internetagentur, die sich auf die Entwicklung, Optimierung und Wartung von Websites auf Basis des Content Management Systems TYPO3 spezialisiert hat.

TYPO3 CMS Certified Consultant

@wacon1999

linkedin.com/in/oliver-wassenaar

Inhalt



Einführung

In den Zeiten der digitalen Transformation gewinnen Websites als Informations-, Transaktions- und Präsentationsmedium immer größere Bedeutung. Gleichzeitig hat der Gesetzgeber in den letzten Jahren strenge Regeln für den Umgang mit pesönlichen Daten erstellt.

Demzufolge birgen Website-Ausfälle und Hacker-Angriffe nicht nur hohe wirtschaftliche sondern auch rechtliche Risiken:

- **Datenmissbrauch**: *Der Missbrauch von Daten durch Dritte verursacht Imageschäden und kann im Rahmen der Datenschutzgrundverordnung(DSGVO) sehr hohe Geldstrafen nach sich ziehen.*

- **Servermissbrauch**: *Von Viren befallene Websites werden häufig zu Fremdzwecken mißbraucht (z.B. Suchmaschinenspaming, "Cryptojacking", DDoS-Attacken, usw.). Sie können Haftungsschäden verursachen sowie Rankingverluste bis hin zum Blacklisting bei Suchmaschinen.*

- **Datenverlust/Dysfunktionalität**: *In der Regel schützen Backups vor dem versehentlichen oder absichtlichen Verlust von Daten. Da sich ein Virenbefall in der Regel aber immer erst viel später bemerkbar macht, kann es sein, dass auch zurück liegende Datensicherungen keine Abhilfe mehr leisten. Im schlimmsten Fall muss die Website nocheinmal komplett neu entwickelt werden.*

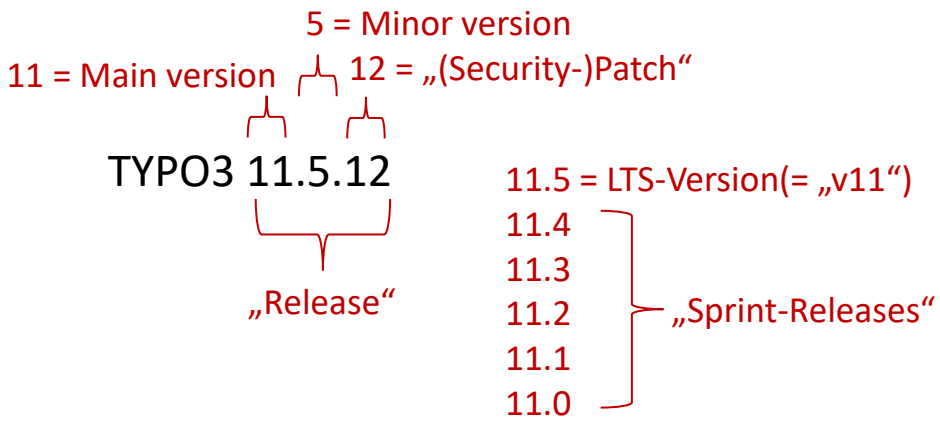
Dieses Dokument stellt einen Leitfaden für Betreiber von TYPO3 Websites bereit, der helfen soll, die oben genannten Risiken zu minimieren.

Ergänzend zu diesem Dokument empfehlen wir unser eBook https://www.wacon.de/internetagentur/downloads/dsgvo_typo3.pdf, das sich speziell mit dem Thema Datenschutz beschäftigt.

Versionslogik

Eine der wichtigsten Maßnahmen zum Betrieb einer sicheren TYPO3-Installation ist die Verwendung einer sicheren TYPO3 Version. Die TYPO3 Association hat eine verbindliche Releasepolitik entwickelt, die wir nachfolgend kurz vorstellen.

TYPO3 Release
Ein TYPO3 Release besteht immer aus drei durch einen Punkt getrennte Zahlen: <Main version>.<Minor version>.<Patch> (Bsp. 11.5.12).



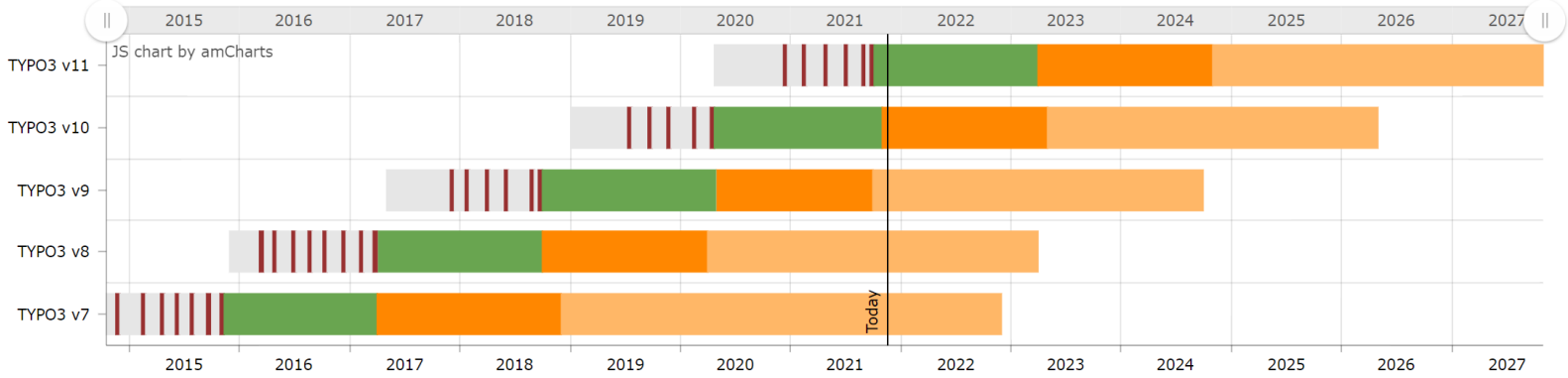
Long Term Support(LTS)
Zu jeder Main version gibt es immer eine sog. LTS Version. Sie hat die höchste Minor version. Im Falle von TYPO3 v11 ist es 11.5.. Es wird also niemals eine Version 11.6. geben. Die darunter liegenden Minor versions(11.0. – 11.4.) werden als **Sprint Releases** *bezeichnet und sind für den Produktiveinsatz nicht geeignet. LTS Versionen werden 1,5 Jahre mit Wartungs- und Sicherheitsupdates versorgt, was sich an der dritten Stelle bemerkbar macht (11.5.***0** *– 11.5.***xx***). Weitere 1,5 Jahre nur mit Sicherheitsupdates.*

Extended Long Term Support(ELTS)
Der Extended Long Term Support(ELTS) ist ein von der TYPO3 GmbH angebotener **kostenpflichtiger** *Support für TYPO3 Versionen, die (nach 3 Jahren) aus dem LTS fallen. In der Regel wird für zwei Main versions ein ELTS angeboten. Sind also die beiden Versionen v11 und v10 im LTS, wird für v9 und v8 ELTS angeboten. Im Rahmen dieses Services werden weiterhin Security-Updates ausgeliefert.*

Die TYPO3 Association aktualisiert regelmäßig Ihre TYPO3 Entwicklungsarbeit anhand einer Raodmap unter:

https://typo3.org/cms/roadmap

Support Times



PHP Version

Für den Betrieb von TYPO3 ist die serverseitige Programmiersprache PHP erforderlich. Auch für PHP gilt eine Sicherheitsstrategie, die sich an den Versionen orientiert. Und auch hier sollte man nur Versionen einsetzen, die mit Security-Updates versorgt werden(siehe: https://www.php.net/supported-versions.php).

Die folgende Matrix zeigt, welche TYPO3-Versionen mit welchen PHP-Versionen kompatibel sind:

	TYPO3 v11 10/2021-10/2024	**TYPO3 v10** 04/2020-04/2023	**TYPO3 v9** 10/2018-09/2021	**TYPO3 v8** 04/2017-03/2020
PHP 7.3 bis 6.12.2021	nein	ja	ja	ja
PHP 7.4 bis 28.11.2022	ja	ja	ja	ja
PHP 8.0 bis 26.11.2023	ja	nein	nein	nein

Hinweis: *Die Kompatibilität bezieht sich nur auf das TYPO3 Kernsystem nicht aber die eingesetzten Extensions. Die Änderung der PHP-Einstellung sollte daher vorher gründlich getestet werden.*

Organisatorisches

In der TYPO3 Association ist ein eigenes Security Team für die Überwachung und Steuerung von sicherheitsrelevanten Fragen und Problemen rund um TYPO3 zuständig(siehe https://typo3.org/community/teams/security).

Es ist auf jeden Fall empfehlenswert, die Veröffentlichungen des Teams über die Kanäle eMail-Verteiler(https://lists.typo3.org/cgi-bin/mailman/listinfo/typo3-announce), RSS News-Feed(https://typo3.org/?type=101) und Twitter(@typo3_security) zu verfolgen.

Unter https://typo3.org/help/security-advisories/ erhält man eine Liste aller bekannten Sichherheitslücken sowie entsprechende Handlungsempfehlungen, die jeweils als sog. "Security Bulletins" veröffentlicht werden. .

Security Bulletins

Es gibt drei Arten von Bekanntmachungen("Security Bulletins"), die mit einer eindeutigen Kennung veröffentlicht werden:

- *TYPO3-CORE-SA-yyyy-nnn für Bulletins, die den TYPO3 Core betreffen*
- *TYPO3-EXT-SA-yyyy-nnn für Bulletins, die für TYPO3-Extensions gelten*
- *TYPO3-PSA-yyyy-nnn für Public Service Announcements*

Wobei yyyy für das entsprechende Jahr der Veröffentlichung und nnn für eine fortlaufende Nummer steht.

Public Service Anouncements
Sichheitsrelevante Informationen, die nicht direkt den Source Code von TYPO3 oder Extensions betreffen, werden als sog. Public Service Announcements veröffentlicht. Darunter fallen unter anderem Probleme bei Dritt-Software wie Apache, PHP oder mySQL.

- Release Date: November 10, 2021
- Component Type: Third party extension. This extension is not a part of the TYPO3 default installation.
- Component: "Job Fair" (jobfair)
- Vulnerability Type: Sensitive Data Exposure.
- Affected Versions: 1.0.12 and below, 2.0.0 - 2.0.1
- Severity: Medium
- Suggested CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:U/RC:C
- References: CVE-2021-43564

Severity
Die Severity ist ein Indikator für die Dringlichkeit einer Sicherheitslücke:

Critical	*höchste Dringlichkeitsstufe, die ein sofortiges Handeln erfordert*
High	*zweithöchste Stufe, schnellstmöglicher Handlungsbedarf*
Medium	*Ihre Installation ist nicht zwingend betroffen, dennoch sollte Update erfolgen*
Low	*die Installation ist nur unter bestimmten – eher unwahrscheinlichen – Umständen betroffen. Auch in diesem Fall empfehlen wir ein Update.*

Warum ist es wichtig, immer das aktuellste Sicherheitsupdate zu installieren?

TYPO3 ist ein Quellcode offenes System. Durch den Vergleich von alter Version und neuer Version können Hacker sehr schnell erkennen, welche Änderungen durchgeführt wurden. Auf diese Weise wird dann auch die Schwachstelle der alten Version sichtbar.
Daher eine der wichtigsten Regeln in Sachen Sicherheit:

Halten Sie das System immer auf dem neuesten Sicherheitspatch.

Installation

Installieren Sie den Code direkt von **get.typo3.org**. *Vermeiden Sie vermeintlich einfachere Installationspakete von Drittanwendern. Vergleichen Sie den Hashwert der heruntergeladenen Datei mit dem auf der offiziellen Website veröffentlichten.*

Package Signatures - Verifying integrity of releases

TYPO3 Release Packages (the downloadable tarballs and zip files) as well as Git tags are signed using PGP signatures since TYPO3 v7 during the automated release process. Besides that, SHA1 and SHA2-256 hashes are being generated for these files. Find more details on verifying signatures and hashes in the infrastructure guide.

Checksums of TYPO3 11.5.3

SHA256

```
1592757da5f32b23e69b034a8c1dd5db99cbe3f55729801ab80a24ee4d67b544 typo3_src-11.5.3.tar.gz
e4dbcc902a9f50abd1e451e353fdd8dcac174ed2eb3eec7bf7937d505b1886ef typo3_src-11.5.3.zip
```

SHA1

```
d7328ef70495b22c07a971ae0b4b8e4a3dd0f628 typo3_src-11.5.3.tar.gz
db6ebf39f9f509bd2fb52c86322d33ecbe5f9821 typo3_src-11.5.3.zip
```

MD5

```
365c19403ff89f641c1b4362ed72a034 typo3_src-11.5.3.tar.gz
a450dffe4a19498eb140928ba5ae3f3b typo3_src-11.5.3.zip
```

Schreib- und Leserechte sollte nur der User (z.B. “apache”) haben, unter dem der Webserver läuft. Programmierer/Administratoren sollten durch eine Gruppenzuordnung entsprechende Rechte erhalten. Grundsätzlich reichen die Schreibrechte für die Verzeichnisse “fileadmin”, “typo3conf” und “typo3temp”.

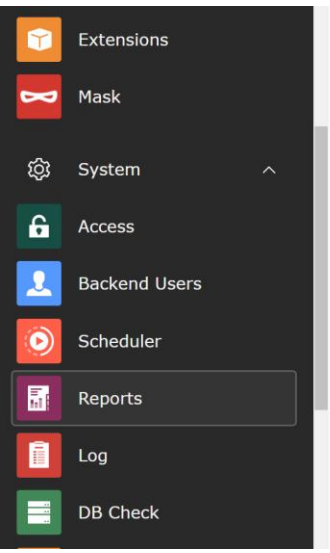
Die Datei **typo3conf/LocalConfiguration.php** *ist die wichtigste Konfigurationsdatei in TYPO3. Sie sollte nicht von Unbefugten les-(weil hier Datenbankzugangsdaten im Klartext enthalten sind) oder schreibbar(weil eine Änderung des Installtool-Passwortes und damit die Erstellung eines Admin-Accounts möglich ist) sein.*

Für die Benutzung des Installtools sollten nur ausgewählte Administratoren sog. “Maintainer-Rechte” haben.

Redakteure sollten grundsätzlich keinen ftp/ssh/scp-Zugang zum Webserver haben.

Reports & Logs

Unter dem Punkt "Reports" im TYPO3 Backend gibt es einen Bereich "Security", der komplett auf grün stehen sollte.



Security

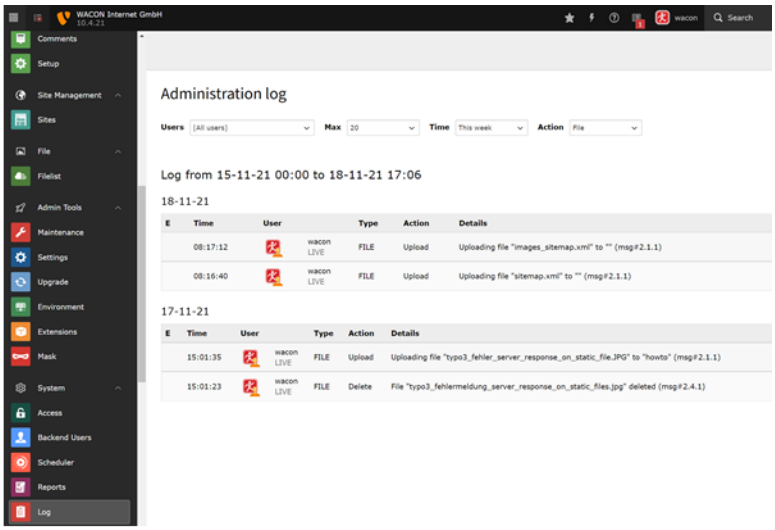
.htaccess Upload Protection	OK
Admin User Account	OK
Backend only accessible through HTTPS	OK
Encrypted backend connection (HTTPS)	OK
Exception Handler / Error Reporting	OK
File Deny Pattern	OK
Install Tool	Disabled
Install Tool Password	OK
Server Response on static files	OK • All 10 files processed correctly
Trusted Hosts Pattern	OK

Server Response on static files
Hierbei handelt es sich um eine häufige Warnmeldung, die nach einer Standard-Installation häufig angezeigt wird. Damit wird die Möglichkeit beschrieben, mit dem TYPO3 Filemanager Dateien mit der Syntax „maliciouscode.html.txt" (oder „maliciouscode.svg.txt") hochzuladen. Einige Webserver behandeln diese Dateien als HTML-Dateien, weil sie „.html" enthalten.
Da html- und svg-Dateien schadhaften Code enthalten können, besteht für Redakteure die Möglichkeit, das System auf diese Weise zu unterwandern. In unserem Artikel unter https://www.wacon.de/typo3-know-how/server-response-on-static-files.html beschreiben wir, wie Sie dieses Problem beheben können.

Server Response on static files	Warnings Please see documentation for further details... • https://www.wacon.de/typo3temp/assets/4f63578c.tmp/60cd7fd4.html.wrong unexpected content-type `text/html` • https://www.wacon.de/typo3temp/assets/4f63578c.tmp/60cd7fd4.1.svg.wrong unexpected content-type `image/svg+xml`

Unter "Logs" stehen umfangreiche Informationen zu Systemfehlern, Login-Versuchen, Benutzeraktionen, Datei-Uploads und Löschungen u.v.m. zur Verfügung.

Hier kann man übrigens auch ungewünschte Änderungen von Redakteuren rückgängig machen:



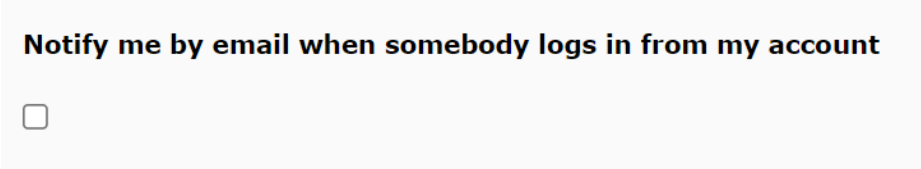
Systemeinstellungen automatisiert überwachen
Mit dem Scheduler-Task „System Status Update" können Sie die Systemumgebung automatisiert überwachen. Bei Fehler/Warnungen (oder wenn gewünscht grundsätzlich) wird eine Mail an die in der Taskdefinition hinterlegte Adresse geschickt.

Scheduled tasks

ID	Task	Type	Frequency	Parallel Execution	Last Execution	Next Execution
1	**System Status Update (reports)**	Recurring	0 9,15 * * 1-5	No	22-11-21 10:23 (Manual)	22-11-21 15:00

Mailbenachrichtigung
Lassen Sie sich per Mail informieren, wenn sich ein User(“1”) oder zumindest Administrator(“2”) einloggt:
`$GLOBALS['TYPO3_CONF_VARS']['BE']['warning_mode’]` *= 1 oder 2*
`$GLOBALS['TYPO3_CONF_VARS']['BE']['warning_email_addr’]` *= <MAILADRESSE>*
(Beide Werte können über das Installtool eingestellt werden)

Redakteure können sich über ihre Einstellungen ebenfalls informieren lassen, wenn sich jemand über ihren Account einloggt.



Fehlerhafte Loginversuche
Sie können fehlgeschlagene Loginversuche manuell nachvollziehen, indem Sie unter „Reports“ das Filterfeld „Action“ auf „Login“ setzen und den gewünschten Zeitraum angeben.

Log from 22-11-21 00:00 to 22-11-21 09:34

22-11-21

E	Time	User	Type	Action	Details	Actions
ⓘ	09:33:04	[0] [-99]	LOGIN	ATTEMPT	Login-attempt from 87.191.168.20, username 'wacon', password not accepted! (msg#255.3.1)	

Für die **automatisierte Überwachung** *fehlgeschlagener Loginversuche können Sie mit Hilfe eines einfachen Abfrage-Scripts die Tabelle sys_log direkt nach der Zeichenkette „Login-attempt“ abfragen und die relevanten Daten(Zeitstempel, IP-Adresse, Username) weiterverarbeiten.*

error	details	tstamp	type	details_nr	IP	log_data	e
3	Login-attempt from ###IP###, username '%s', passwo...	1637570736	255	1	87.191.168.20	a:1: {i:0;s:5:"wacon";}	

Weitere Maßnahmen

Im Folgenden weitere Maßnahmen, die den Schutz Ihres TYPO3-Systems weiter erhöht:

Passwortmanagement
Verwenden Sie nur ausreichend sichere Passwörter(mind. 9 Zeichenkombination aus Klein-/Großbuchstaben, Zahlen, Sonderzeichen). Verwenden Sie nicht die gleichen Passwörter für unterschiedliche Zugänge und ändern Sie Passwörter regelmäßig.

Multifaktor-Authentifizierung
Ab TYPO3 v11 besteht die Möglichkeit, Backend-User nur noch über eine Mehrfaktorauthentifizierung Zugang zum Backend zu ermöglichen.
Mehr Infos dazu:
https://www.wacon.de/typo3-know-how/multi-faktor-authentifizierung.html

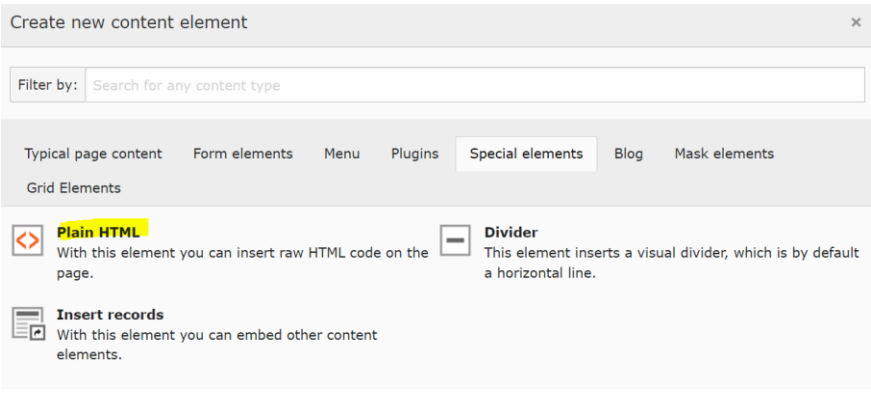
Logdaten anonymisieren
Anonymisieren Sie die Daten in der Tabelle sys_log über den Scheduler-Task „Anonymize IP addresses in database tables"

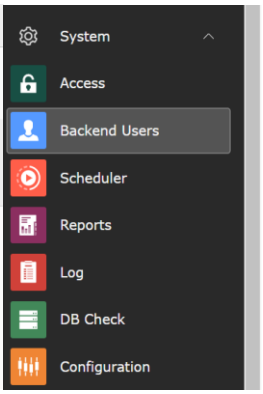
Verwendung des HTTP Security Headers
Die Verwendung von HTTP Security Headern ist eine weitere Möglichkeit, die eigene Website sicherer zu machen. Die Header weisen Browser z.B. an, Serveranfragen nur über "https" zu stellen("HTTP Strict-Transport-Security response header" oder kurz HSTS), verhindern und vermeiden u.a. Angriffe durch Cross Site Scripting, MIME Sniffing und Clickjacking.

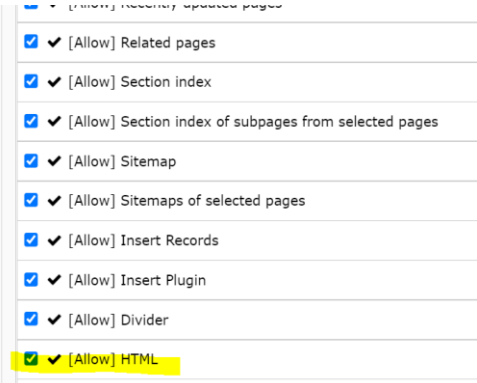
Ob Ihre Website mit diesen Headern ausreichend geschützt ist, können Sie unter https://securityheaders.com testen.

Eine einfache Lösung zum Setzen des HTTP Security Headers finden Sie in unserem DSGVO-Artikel: https://www.wacon.de/typo3-service/dsgvo.html

Inhaltselement "Plain HTML" deaktivieren
In TYPO3 gibt es die Möglichkeit, HTML(und damit auch svg/JavaScript)-Code als Inhaltselement auf einer Seite auszugeben. Diese Funktion sollten Sie zumindest für Redakteure über die „Access Lists" in den Einstellungen des Users(oder besser der Gruppe) deaktivieren.







Einbindung von HTML-Code

Deaktivierung dieser Möglichkeit

Hochladen von HTML, JavaScript- und SVG-Dateien unterbinden

HTML-, JavaScript- und SVG-Dateien können schadhaften Code enthalten. Die Möglichkeit des Hochladens solcher Dateien über den Filemanager sollte daher nach Möglichkeit unterbunden werden.

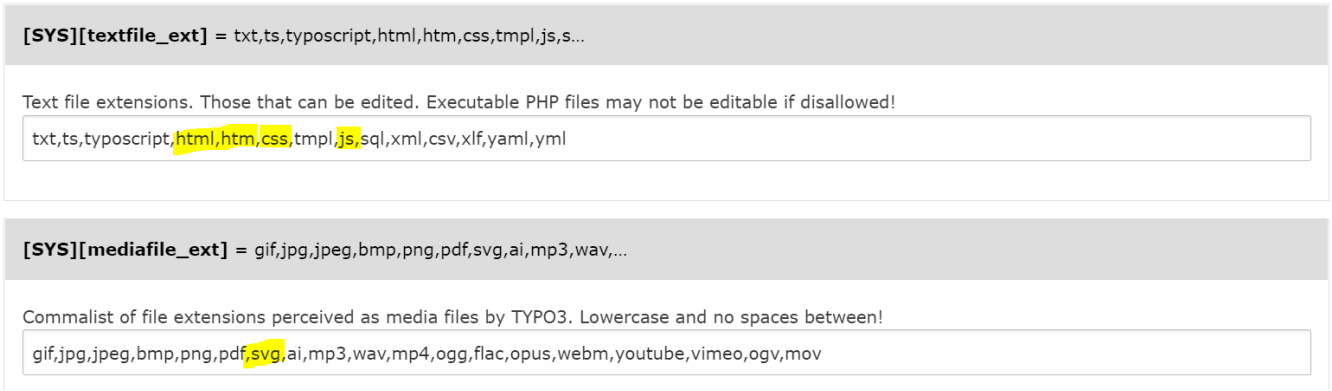
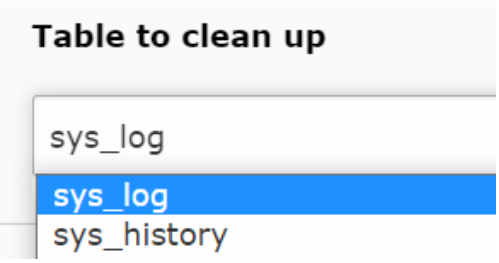


Table Garbage Collection

Löschen Sie regelmäßig über den scheduler-Task „Table Garbage Collection“ die Tabellen „syslog“ und „sys_history“. Wenn Sie – wie die meisten – die Extension powermail nutzen, löschen Sie auch die Tabellen „domain_model_mail“ und „domain_model_answer“



Backup-Strategie

Das Backup einer TYPO3 Installation umfasst zwei Komponenten:

1. Dateien
Ausschlaggebend sind i.d.R. die beiden Verzeichnisse:
<WEBROOT>/fileadmin
<WEBROOT>/typo3conf

Hierbei handelt es sich um Standardverzeichnisse, die in speziellen Fällen auch an anderer Stelle liegen können. „typo3conf" kann z.B. aus Sicherheitsgründen auch außerhalb des Webroot-Pfades liegen. „fileadmin" kann anders heißen bzw. kann es weitere Verzeichnisse(„File-Mounts") geben.

2. Datenbank
TYPO3 benötigt eine Datenbank, die selbstverständlich auch zu sichern ist.

Backup testen
Um sicher zu gehen, dass Backups vollständig sind und problemlos zurück gespielt werden können, sollten diese getestet werden. In der Praxis bietet es sich häufig an, ein Backup in einer zweiten Umgebung zurückzuspielen und diese dann gleichzeitig als Testumgebung für Aufgaben zu verwenden, die nicht sofort im Live-System durchgeführt werden sollen(wie z.B. Security-Update, Template-Änderungen usw.)

Remote Backups
Backups sollten nicht (nur) lokal gehalten werden. Wir haben ein eigenes Backup-Script entwickelt, das die Spiegelung von Backups auf andere Server ermöglicht:
https://www.wacon.de/typo3-service/eigene-extensions/wacon-typo3-backup.html

Bedenken Sie, dass Backups persönliche Daten im Sinne der DSGVO enthalten können und treffen Sie entsprechende Schutzmaßnahmen, wie z.B. die Verschlüsselung und einen Passwortschutz.

Backup Intervalle
Da mögliche Funktions-Fehler, Datenverlust und/oder schadhafter Code in den meisten Fällen erst spät erkannt werden, sollten Backups nicht nur vom Vortag sondern über einen längeren Zeitraum verfügbar sein.

Wir empfehlen die folgenden Backup-Intervalle:

- *Machen Sie ein tägliches Backup*
- *Behalten Sie ein Backup der letzten 7 Tage*
- *Behalten Sie ein Backup des letzten Monats*
- *Behalten Sie ein Backup des letzten halben Jahres*
- *Behalten Sie ein Backup der letzten 12 Monate*

Vielen Dank!

Wir hoffen, dass Ihnen dieses kostenlose eBook weitergeholfen hat. Für ein Feedback wären wir sehr dankbar.

Als Internetagentur sind wir auf die Entwicklung, Optimierung und den Support von Websites auf Basis von TYPO3 spezialisiert.

Gerne helfen wir Ihnen dabei, Ihre TYPO3 Website sicherer zu machen.

Nehmen Sie Kontakt mit uns auf

WACON Internet GmbH

www.wacon.de