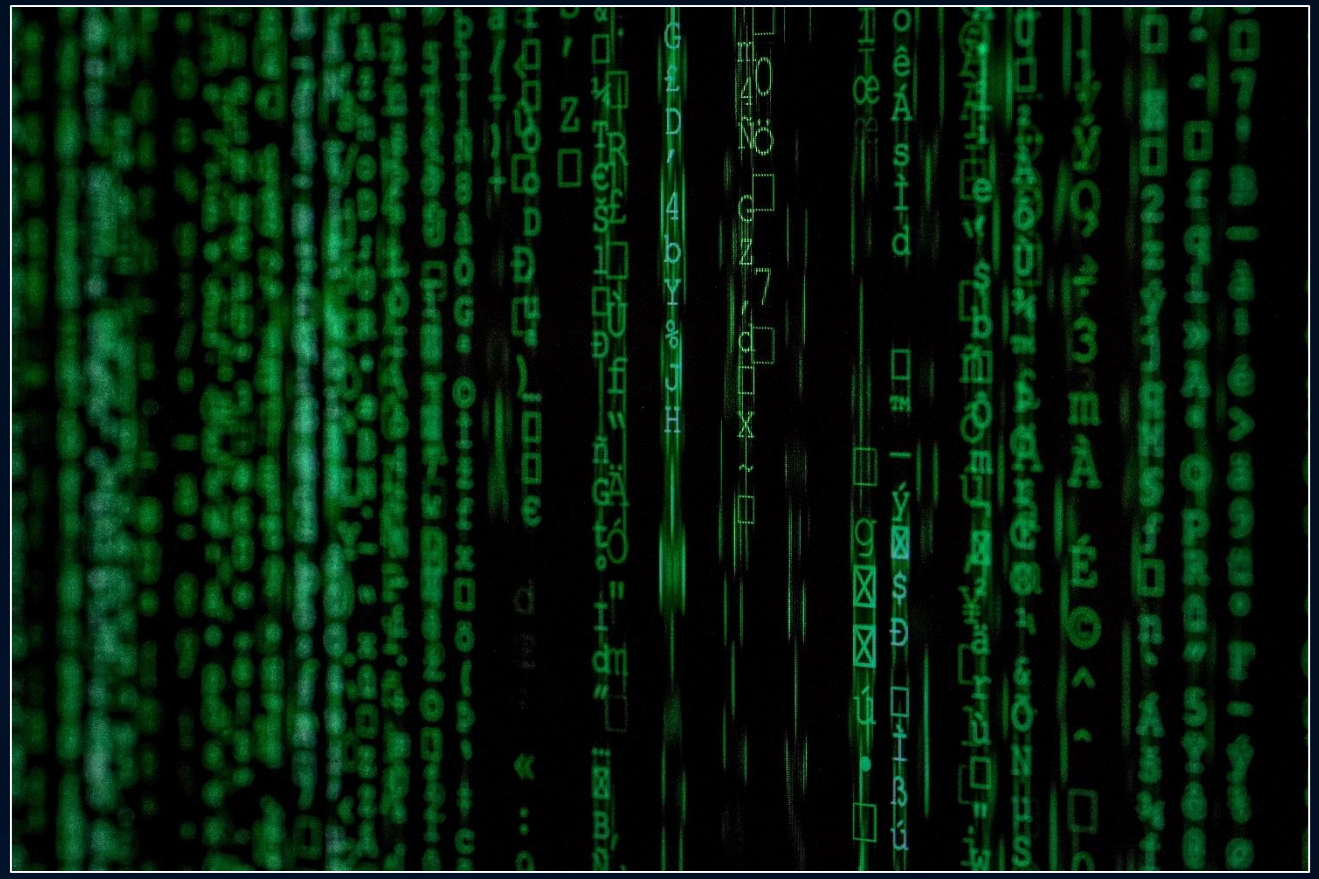
WordPress-Sicherheit
Ein kleiner Überblick

FRANK SCHMITTLEIN

WORDPRESS-MEETUP NÜRNBERG
MAI 2019

Warum geht uns Sicherheit was an?



Was ist Sicherheit?

- Sicherheit ist nicht absolut, es ist ein kontinuierlicher Prozess und sollte als solcher verwaltet werden. Bei Sicherheit geht es um Risikominderung, nicht um die Beseitigung von Risiken, und das Risiko wird niemals Null sein. Es geht darum, die geeigneten Sicherheitskontrollen einzusetzen, um die Risiken und Bedrohungen für die Website am besten zu bekämpfen.

Was ist Sicherheit?

- Sicherheit geht auch über die WordPress-Anwendung hinaus. Es ist genauso wichtig, deine lokale Umgebung, dein Online-Verhalten und deine internen Prozesse zu sichern und abzusichern. Die Sicherheit besteht aus drei Bereichen: Menschen, Prozesse und Technologien. Jeder arbeitet in synchroner Harmonie miteinander, ohne die Menschen und ihre Prozesse wäre die jedoch Technologie selbst nutzlos.

Schwachstellen für WordPress

- Betriebssystem
- Web-Server
- Datenbank-Server

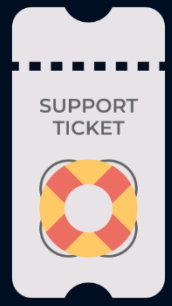
Hoster

- PHP
- WordPress Kern
- Plugins
- Themes

Benutzer

Ist meine Website unsicher?

- WPScan (https://wpscan.org/)
  - Docker: docker run -it --rm wpscanteam/wpscan --url https://wpmeetup-nuernberg.de/ --enumerate
- WPCheck (https://github.com/sergejmueller/wpcheck)



Allgemeine Grundsätze

- Ein SSL-Zertifikat sollte für jede Website, spätestens mit der DS-GVO Pflicht sein
- Verwendung intelligenter Benutzernamen und Passwörter
- Verwende (nach Möglichkeit) die neueste Version von WordPress, Plugins und Themes
- Generelle Verzeichnis- und Dateirechte: Dateirechte auf 644 und die Verzeichnisrechte auf 755

Härtung der wp-config.php

- wp-config.php eine Ebene höher verschieben
  - Beispiel: von htdocs/wordpress/wp-config.php nach htdocs/wp-config.php
- Sicherheitsschlüssel aktualisieren
  - Link: https://api.wordpress.org/secret-key/1.1/salt/
  - Beispiel:

```
/* Authentication Unique Keys and Salts. */
define( 'AUTH_KEY',         'put your unique phrase here' );
define( 'SECURE_AUTH_KEY',  'put your unique phrase here' );
define( 'LOGGED_IN_KEY',    'put your unique phrase here' );
define( 'NONCE_KEY',        'put your unique phrase here' );
define( 'AUTH_SALT',        'put your unique phrase here' );
define( 'SECURE_AUTH_SALT', 'put your unique phrase here' );
define( 'LOGGED_IN_SALT',   'put your unique phrase here' );
define( 'NONCE_SALT',       'put your unique phrase here' );
```

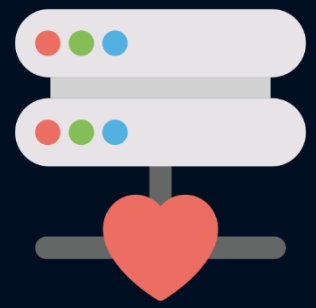
- Änderung der Berechtigungen (400)
- Schutz über die .htaccess

Absicherung deines WordPress Admin-Bereiches

- Anzahl der Anmeldeversuche begrenzen (Plugin: Limit Login Attempts Reloaded)
- Zwei-Faktoren-Authentifizierung (2FA) einsetzten (Plugin: Two-Factor oder Google Authenticator)
- Login-URL ändern (Plugin: Move Login)
- HTTP-Basic-Authentifizierung hinzufügen (htpasswd-Schutz)

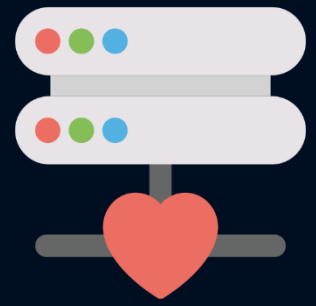
Kleine Schritte für mehr Sicherheit

- Tabellenpräfix ändern (schon bei der Installation)
- wp-content Ordner umbenennen (am besten gleich nach der Installation)
  - wp-config.php:
    ```
    define('WP_CONTENT_DIR', ' /htdocs/wordpress/wpc');
    define('WP_CONTENT_URL', 'https://www.domain.tld/wpc');
    ```
- XML-RPC-Schnittstelle deaktivieren (Plugin: Disable XML-RPC) oder .htaccess
- REST-API schützen (Plugin: REST API Toolbox)
- WordPress-Version verstecken
  - functions.php:
    ```
    function no_generator() { return ‘’; }
    add_filter( 'the_generator', 'no_generator' );
    ```
- Umsetzung der neuesten HTTP-Security-Header (.htaccess)



Kleine Schritte für mehr Sicherheit

- Emoji's deaktivieren (Plugin: Disable Emojis)
- .htaccess auf 644 oder (wenn Möglich) 444
- Dateibearbeitung im Dashboard ausschalten
  - wp-config.php:
    ```
    define('DISALLOW_FILE_EDIT', true);
    ```
- Starke Passwörter (Plugin: Force Strong Passwords)
- Hotlinking verhindern (http://www.htaccesstools.com/hotlink-protection/)
- 6G Firewall 2019 (https://perishablepress.com/6g/) oder 7G (Beta)
- Erstelle immer Backups und Teste diese
- Server-Signatur deaktivieren
  - `.htaccess:`
    ```
    ServerSignature Off
    ```



Die perfekte .htaccess für WordPress – PageSpeed und Sicherheit

1. HTTP zu HTTPS Umleitung
2. CORS aktivieren für bestimmte Dateitypen
3. Block Nuisance Requests (lästige Anfragen blocken)
4. Dateien komprimieren und cachen
5. 7G-Firewall gegen die Einschleusung von Schadcode (Beta)
6. WordPress-Dateien gegen Zugriff blocken (ggf. um die wp-cron.php [Umstellung auf cronjob] und maintenance.php erweitern)
7. Hotlink Protection gegen Bildklau
8. Schutz gegen den »ReallyLongRequest« Banditen
9. Schütze Deinen Adminbereich mittels HTTP-Veriegelung
10. Die XML-RPC Datei sperren
11. Der Referrer Header für mehr Datenschutz
12. Die HTTP-Security-Header – Update 2019
13. Die WordPress Standard Regeln

Quelle: https://andreas-hecht.com/blog/4183/

WordPress überwachen

- Suchen nach geänderten Dateien (in den letzten 24 Stunden):

```
find /htdocs/wordpress -mtime -1 -name "*.php" -printf
'%TY-%Tm-%Td %TT\t%p\n‘
```

  - Das Gleiche macht man auch mit anderen Dateien (.js und evtl. auch mit .pl)

- Suche nach verdächtigem Code in PHP Dateien:

```
find /htdocs/wordpress -mtime -7 -name "*.php" | xargs grep
-l -i
"eval\|base64_decode\|iframe\|pharma\|viagra\|file_get_cont
ents„
```

- Den Upload Ordner von WordPress nach PHP Dateien durchsuchen

```
find /htdocs/wordpress/wp-content/uploads -name "*.php" -
print
```

Linux/Unix-Dateirechte

	Eigentümer			Gruppe			Sonstige		
Leserecht (4)	r	-	-	r	-	-	r	-	-
Schreibrecht (2)	-	w	-	-	w	-	-	w	-
Ausführungsrecht (1)	-	-	x	-	-	x	-	-	x

- Beispiel 1 – Dateirecht 755
  - Typische Dateirechte für eine ausführbare Datei (ein Programm oder ein Script). Nur der Eigentümer kann die Datei ändern. Alle anderen können sie lediglich lesen und ausführen.
- Beispiel 2 – Dateirecht 664
  - Mögliche Dateirechte für eine nicht ausführbare Datei (beispielsweise ein Textdokument), welche von Eigentümer und Gruppe bearbeitet, vom Rest allerdings nur gelesen werden kann.

Quelle: https://de.wikipedia.org/wiki/Unix-Dateirechte

Plugin-Liste

- Limit Login Attempts Reloaded (https://de.wordpress.org/plugins/limit-login-attempts-reloaded/)
- REST API Toolbox (https://de.wordpress.org/plugins/rest-api-toolbox/)
- Disable XML-RPC (https://de.wordpress.org/plugins/disable-xml-rpc/)
- Two-Factor (https://wordpress.org/plugins/two-factor/)
- Google Authenticator (https://wordpress.org/plugins/google-authenticator/)
- Force Strong Passwords (https://wordpress.org/plugins/force-strong-passwords/)
- Move Login (https://wordpress.org/plugins/sf-move-login/)
- Stop User Enumeration (https://de.wordpress.org/plugins/stop-user-enumeration/)
- Disable Emojis (GDPR friendly) (https://wordpress.org/plugins/disable-emojis/)

Plugin-Liste

- Username Changer (https://wordpress.org/plugins/username-changer/)
- Snitch (https://de.wordpress.org/plugins/snitch/)
- AntiVirus (https://wordpress.org/plugins/antivirus/)
- Antispam Bee (https://wordpress.org/plugins/antispam-bee/)
- Checksum Verifier (https://wordpress.org/plugins/checksum-verifier/)
- Duplicator (https://de.wordpress.org/plugins/duplicator/)
- BackWPup (https://de.wordpress.org/plugins/backwpup/)
- WPScan (https://de.wordpress.org/plugins/wpscan/)
- Really Simple SSL (https://wordpress.org/plugins/really-simple-ssl/)
- Inactive Logout (https://de.wordpress.org/plugins/inactive-logout/)

Wissenswertes

- WPScan (https://wpscan.org/)
- WPScan Vulnerability Database (https://wpvulndb.com/)
- Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers (https://www.exploit-db.com/)
- Zugriffsrechte auf Dateien von Linux (https://wiki.ubuntuusers.de/Rechte/)
- .htaccess Tools (http://www.htaccesstools.com/)
- GenerateWP (https://generatewp.com)
- Apache HTTP server boilerplate configs (https://github.com/h5bp/server-configs-apache)
- Security Headers (https://securityheaders.com)
- Report URI: Tools (https://report-uri.com/home/tools)
- KeyCDN Tools (https://tools.keycdn.com/)

Vielen Dank!

E-MAIL: MAIL@FRANK-SCHMITTLEIN.DE · TWITTER: @SCHMITTLEIN77

WEB: HTTPS://FRANK-SCHMITTLEIN.DE · BLOG: HTTPS://FRANK-SCHMITTLEIN.DE/BLOG