cehler.dev
DEV, SEO & CLOUD

WordPress Sicherheit.

Analyse der WP-Core-Software

Stand 2022

Überblick

Quelle: https://de.wordpress.org/about/security/

Dieses Dokument ist eine Analyse und Erläuterung der WordPress-Core-Software und der damit verbundenen Sicherheitsprozesse sowie eine Untersuchung der inhärenten Sicherheit, die direkt in die Software eingebaut ist.

Entscheidungsträger, die WordPress als Content-Management-System oder Web-Anwendungs-Framework bewerten, sollten dieses Dokument in ihrer Analyse und Entscheidungsfindung verwenden und sich mit den Sicherheitskomponenten und bewährten Vorgehensweisen der Software vertraut machen.

https://de.wordpress.org/about/security/1/15
12/18/21, 11:15 AM Sicherheit | WordPress.org Deutsch

Die Informationen in diesem Dokument sind aktuell für die neueste stabile Version der Software, WordPress 4.7 zum Zeitpunkt der Veröffentlichung, sollten aber auch für die neuesten Versionen der Software als relevant angesehen werden, da die Rückwärtskompatibilität ein starker Fokus für das WordPress-Entwicklungsteam ist.

Spezifische Sicherheitsmaßnahmen und Änderungen werden vermerkt, da sie in bestimmten Releases der Core-Software hinzugefügt wurden. **Es wird dringend empfohlen, immer die neueste stabile Version von WordPress zu verwenden, um die bestmögliche Sicherheit zu gewährleisten.**

Zusammenfassende Darstellung

WordPress ist ein dynamisches Open-Source-Content-Management-System, mit dem Millionen von Websites, Webanwendungen und Blogs betrieben werden. Es versorgt derzeit mehr als **43 % der Top 10 Millionen Websites** im Internet.

Die Benutzerfreundlichkeit, Erweiterbarkeit und ausgereifte Entwicklungs-Community von WordPress machen es zu einer beliebten und sicheren Wahl für Websites jeder Größe.

Seit seiner Gründung im Jahr 2003 hat WordPress eine kontinuierliche Weiterentwicklung erfahren, so dass seine Core-Software gemeinsame Sicherheitsbedrohungen adressieren und entschärfen kann, einschließlich der Top-10-Liste, die vom **Open-Web-Access-Security Projekt („OWASP“)** als gemeinsame Sicherheitslücken identifiziert wurden und in diesem Dokument diskutiert wird.

Das WordPress-Sicherheitsteam arbeitet in Zusammenarbeit mit dem WordPress-Core Führungsteam und mit Unterstützung der weltweiten WordPress-Community daran, Sicherheitsprobleme in der Core-Software zu identifizieren und zu lösen, die für die Verteilung und die Installation auf WordPress.org verfügbar ist, und empfiehlt und dokumentiert bewährte Sicherheitsverfahren für Plugin- und Theme-Autoren von Drittanbietern.

Website-Entwickler und -Administratoren sollten besonderes Augenmerk auf die korrekte Verwendung der Core-APIs und der zugrunde liegenden Serverkonfiguration legen, die die Ursache für häufige Schwachstellen waren, und sicherstellen, dass alle Benutzer starke Passwörter für den Zugriff auf WordPress verwenden.

Ein Überblick über WordPress

WordPress ist ein kostenloses und Open-Source- Content-Management-System (CMS). Es ist die am weitesten verbreitete CMS-Software der Welt und mehr als 43 % der Top 10 Millionen Websites werden damit betrieben, was einem geschätzten Marktanteil von 62 % aller Websites, die ein CMS einsetzen, entspricht.

WordPress wurde unter der General Public License (GPLv2 oder neuer) veröffentlicht, die vier Grundfreiheiten gibt und als so etwas wie die „Verfassung“ von WordPress betrachtet werden kann:

1. Die Freiheit, das Programm für jeden Zweck auszuführen.
2. Die Freiheit, zu verstehen, wie das Programm funktioniert, und es so zu verändern, dass es das tut, was du willst.
3. Die Freiheit zur Weitergabe.
4. Die Freiheit, Kopien deiner modifizierten Versionen an andere weiterzugeben.

Das WordPress-Core-Führungsteam

Das WordPress-Projekt ist eine Meritokratie, die von einem zentralen Führungsteam betrieben und von seinem Co-Gründer und leitenden Entwickler, Matt Mullenweg, geleitet wird. Das Team steuert alle Aspekte des Projekts, einschließlich der Core-Entwicklung, WordPress.org und Community-Initiativen.

Das Core-Führungsteam besteht aus Matt Mullenweg, fünf Lead-Entwicklern und mehr als einem Dutzend Core-Entwicklern mit permanentem Commit-Zugriff. Diese Entwickler haben die endgültige Autorität über technische Entscheidungen und leiten Architektur-diskussionen und Implementierungs-bemühungen.

WordPress hat eine Reihe von mitwirkenden Entwicklern. Einige von ihnen sind ehemalige oder aktuelle Committer, andere sind wahrscheinlich zukünftige Committer. Diese beitragenden Entwickler sind vertrauenswürdige und erfahrene Mitwirkende von WordPress, die viel Respekt unter ihren Kollegen verdient haben. Bei Bedarf hat WordPress auch Gast-Committer, Personen, denen der Commit-Zugriff, manchmal für eine bestimmte Komponente, auf temporärer oder Testbasis gewährt wird.

Der Core und die beitragenden Entwickler leiten in erster Linie die Entwicklung von WordPress. In jeder Version tragen Hunderte von Entwicklern zu WordPress bei. Diese Core Mitwirkenden sind Freiwillige, die in irgendeiner Weise zur Core-Codebasis beitragen.

Der Release-Zyklus von WordPress

Jeder WordPress-Release-Zyklus wird von einem oder mehreren der wichtigsten WordPress Entwickler geleitet. Ein Release-Zyklus dauert in der Regel etwa 4 Monate vom ersten Beratungsgespräch bis zum Start der Version.

Ein Release-Zyklus erfolgt nach dem folgenden Muster:

1. **Phase 1: Planung und Sicherung der Teamleitung**
   Dies geschieht im #core-Chatraum auf Slack. Der Release-Lead diskutiert Funktionen für die nächste Version von WordPress. WordPress-Mitarbeiter beteiligen sich an dieser Diskussion. Der Release-Lead bestimmt die Team-Leads für jede der Funktionen.
2. **Phase 2: Beginn der Entwicklungsarbeiten**
   Teamleiter stellen Teams zusammen und arbeiten an den ihnen zugewiesenen Funktionen. Regelmäßige Chats sind geplant, um die Entwicklung voranzutreiben.
3. **Phase 3: Beta**
   Betas werden veröffentlicht, und Beta-Tester werden gebeten, Fehler zu melden. Ab dieser Phase werden keine Änderungen für neue Erweiterungen oder Funktions-Wünsche mehr durchgeführt. Plugin- und Theme-Autoren von Drittanbietern werden ermutigt, ihren Code gegen die bevorstehenden Änderungen zu testen.
4. **Phase 4: Release-Kandidat**
   Ab diesem Zeitpunkt gibt es einen String-Freeze für übersetzbare Strings. Es wird nur an Regressionen und Hindernissen gearbeitet.
5. **Phase 5: Start**
   WordPress-Version wird gestartet und im WordPress-Admin für Updates zur Verfügung gestellt.

Versionsnummerierung und Sicherheits-Releases

Eine WordPress-Hauptversion wird von den ersten beiden Sequenzen bestimmt. Beispielsweise ist 3.5 eine Hauptversion, ebenso wie 3.6, 3.7 oder 4.0. Es gibt kein „WordPress 3“ oder „WordPress 4“ und jede Hauptversion wird durch ihre Nummerierung bezeichnet, z. B. „WordPress 3.9“.

Hauptversionen können neue Benutzerfunktionen und Entwickler-APIs hinzufügen. Obwohl eine „major“-Version in der Softwarewelt typischerweise bedeutet, dass man mit der Abwärtskompatibilität brechen kann, strebt WordPress danach, niemals mit der Abwärtskompatibilität zu brechen. Abwärtskompatibilität ist eine der wichtigsten Philosophien des Projekts, mit dem Ziel, Updates für Anwender und Entwickler gleichermaßen stark zu vereinfachen.

Eine kleine WordPress-Version wird durch die dritte Sequenz festgelegt. Version 3.5.1 ist 3 eine Minor-Version, ebenso wie 3.4.2 . Eine Minor-Version ist für die Behebung von Sicherheitslücken und die Behebung kritischer Fehler reserviert. Da neue Versionen von WordPress so häufig veröffentlicht werden – ist das Ziel alle 4–5 Monate eine Hauptversion, und kleinere Versionen nach Bedarf – es gibt nur Bedarf an Haupt- und Nebenversionen.

Version-Rückwärtskompatibilität

https://de.wordpress.org/about/security/4/15
12/18/21, 11:15 AM Sicherheit | WordPress.org Deutsch

Das WordPress-Projekt hat eine starke Verpflichtung zur Rückwärtskompatibilität. Diese Verpflichtung bedeutet, dass Themen, Plugins und benutzerdefinierter Code weiterhin funktionieren, wenn WordPress-Core-Software aktualisiert wird. Zudem werden Website Besitzer aufgefordert, ihre WordPress-Version auf die neueste sichere Version zu aktualisieren.

WordPress-Sicherheitsrisiken, Prozesse und Geschichte

Das WordPress-Sicherheitsteam glaubt an eine verantwortungsvolle Offenlegung, indem es das Sicherheitsteam sofort über mögliche Schwachstellen informiert.

Mögliche Sicherheitslücken können dem Sicherheitsteam über den WordPress HackerOne gemeldet werden. Das Sicherheitsteam kommuniziert untereinander über einen privaten Slack-Kanal und arbeitet an einem abgeschotteten, privaten Trac, um Fehler und Sicherheitsprobleme zu erkennen, zu testen und zu beheben.

Jeder Sicherheitsbericht wird nach Erhalt bestätigt, und das Team arbeitet daran, die Schwachstelle zu überprüfen und ihre Schwere zu bestimmen. Wenn dies bestätigt wird, plant das Sicherheitsteam dann einen Patch, um das Problem zu beheben, der für eine kommende Version der WordPress-Software festgelegt werden kann, oder es kann als

sofortige Sicherheitsveröffentlichung verwendet werden, abhängig von der Schwere des Problems.

Für eine sofortige Sicherheitsveröffentlichung wird vom Sicherheitsteam ein Hinweis auf der News-Seite von WordPress.org veröffentlicht, der die Veröffentlichung ankündigt und die Änderungen detailliert beschreibt. Die verantwortungsvolle Offenlegung einer Schwachstelle wird in der Beratung gewürdigt, um auch in Zukunft eine verantwortungsvolle Berichterstattung zu fördern und zu intensivieren.

Administratoren der WordPress-Software sehen eine Benachrichtigung im Admin-Dashboard ihre Website zu aktualisieren, wenn eine neue Version verfügbar ist, und nach dem manuellen Upgrade werden die Benutzer auf die Seite „Über WordPress“ umgeleitet, die die Änderungen im Detail beschreibt. Wenn Administratoren automatische Hintergrund Updates aktiviert haben, erhalten sie nach Abschluss eines Upgrades eine E-Mail.

Automatische Hintergrund-Updates für Sicherheits Releases

Mit der Version 3.7 führte WordPress automatische Hintergrundupdates für alle kleineren Versionen ein, wie z. B. 3.7.1 und 3.7.2. Das WordPress-Sicherheitsteam kann automatisierte Sicherheitsverbesserungen für WordPress identifizieren, beheben und verteilen, ohne dass der Website-Besitzer irgendetwas auf seiner Seite tun muss, und das Sicherheitsupdate wird automatisch installiert.

Wenn ein Sicherheitsupdate für die aktuelle stabile Version von WordPress veröffentlicht wird, wird das Core-Team auch Sicherheitsupdates für alle Versionen, die zu Hintergrundupdates fähig sind (seit WordPress 3.7) veröffentlichen, so dass diese älteren, aber immer noch aktuellen Versionen von WordPress Sicherheitsverbesserungen erhalten.

Einzelne Website-Besitzer können sich dafür entscheiden, automatische Hintergrund Updates durch eine einfache Änderung in der Konfigurationsdatei zu entfernen, aber das Aufrechterhalten dieser Funktionalität wird vom Core-Team dringend empfohlen, ebenso der Einsatz der neuesten stabilen Version von WordPress.

2013-OWASP-Top-10

Das Open-Web-Application-Security-Projekt („OWASP“) ist eine Online-Community, die sich der Sicherheit von Web-Anwendungen widmet.

Die OWASP-Top-10-Liste konzentriert sich auf die Identifizierung der schwerwiegendsten Anwendungssicherheitsrisiken für ein breites Spektrum von Unternehmen. Die Top-10-Positionen werden in Kombination mit Konsensus Schätzungen zur Ausnutzbarkeit, Erkennbarkeit und Auswirkung ausgewählt und priorisiert.

Die folgenden Abschnitte behandeln die APIs, Ressourcen und Richtlinien, die WordPress

verwendet, um die Kernsoftware, Plugins und Themes von Drittanbietern gegen potenzielle Risiken zu schützen.

A1 - Injection

Es gibt eine Reihe von Funktionen und APIs in WordPress, die Entwickler dabei unterstützen, sicherzustellen, dass nicht autorisierter Code nicht injiziert werden kann, und ihnen helfen, Daten zu validieren und zu bereinigen.

Bewährte Vorgehensweisen und Dokumentationen zur Verwendung dieser APIs zum Schutz, zur Validierung oder Bereinigung von Eingabe- und Ausgabedaten in HTML, URLs, HTTP-Headern und bei der Interaktion mit der Datenbank und dem Dateisystem sind verfügbar. Administratoren können auch die Dateitypen, die über Filter hochgeladen werden können, weiter einschränken.

A2 – Fehler in Authentifizierung und Session-Management

WordPress-Core-Software verwaltet Benutzerkonten und Authentifizierung. Details wie Benutzer-ID, Name und Passwort werden serverseitig verwaltet, ebenso wie die Authentifizierungs-Cookies. Die Passwörter werden in der Datenbank durch Standard Salting-und-Stretching-Techniken geschützt. Bestehende Sitzungen werden beim Abmelden für Versionen von WordPress ab 4.0 zerstört.

A3 - Cross Site Scripting (XSS)

WordPress bietet eine Reihe von Funktionen, die dazu beitragen können, dass die vom Benutzer bereitgestellten Daten sicher sind. Vertrauenswürdige Benutzer, d. h. Administratoren und Redakteure auf einer einzigen WordPress-Installation und Netzwerkadministratoren nur in WordPress-Multisite, können ungefiltertes HTML oder JavaScript posten, wie sie es benötigen, z. B. innerhalb eines Beitrags oder einer Seite.

Nicht vertrauenswürdige Benutzer und vom Benutzer übermittelte Inhalte werden standardmäßig gefiltert, um gefährliche Objekte zu entfernen, indem die KSES-Bibliothek über die Funktion wp_kses verwendet wird.

Zum Beispiel hat das WordPress-Core-Team vor der Veröffentlichung von WordPress 2.3 bemerkt, dass die Funktion `the_search_query()` von den meisten Theme-Autoren verkehrt genutzt wurde, da die Ausgabe der Funktion für die Verwendung in HTML nicht escaped wurde. In einem sehr seltenen Fall von leicht eingeschränkter Rückwärtskompatibilität wurde die Ausgabe der Funktion in WordPress 2.3 geändert, um sie vorab zu überarbeiten.

A4 - Unsichere direkte Objektreferenzen

WordPress bietet oft eine direkte Objektreferenz, wie z. B. eindeutige numerische Identifikatoren von Benutzerkonten oder Inhalte, die in den URL- oder Formularfeldern verfügbar sind. Während diese Kennungen direkte Systeminformationen preisgeben, verhindern die umfangreichen Berechtigungen und das Zugriffskontrollsystem von WordPress unautorisierte Anfragen.

A5 - Sicherheits-Fehlkonfiguration

Die Mehrheit der WordPress-Sicherheitskonfigurationen ist auf einen einzigen autorisierten Administrator beschränkt. Standardeinstellungen für WordPress werden kontinuierlich auf der Ebene des Core-Teams ausgewertet, und das Core-Team von WordPress bietet Dokumentationen und bewährte Verfahren, um die Sicherheit der Serverkonfiguration für den Betrieb einer WordPress-Website zu erhöhen.

A6 - Sensible Datenexposition

WordPress-Benutzerkonto-Passwörter werden auf der Grundlage des Portable-PHP Password-Hashing-Framework gesalzen und gehasht. Das Berechtigungssystem von WordPress wird verwendet, um den Zugriff auf private Informationen wie die PII registrierter Benutzer, E-Mail-Adressen von Kommentatoren, privat veröffentlichte Inhalte usw. zu kontrollieren.

In WordPress 3.7 wurde eine Funktion zur Messung der Passwort-Stärke in die Core-Software integriert, die den Benutzern zusätzliche Informationen zur Einstellung ihrer Passwörter und Hinweise zur Erhöhung der Stärke liefert. **WordPress hat auch eine optionale Konfigurationseinstellung für die Anforderung von HTTPS.**

A7 - Fehlende Funktionsebenen-Zugriffskontrolle

WordPress prüft vor der Ausführung der Aktion, ob für alle Zugriffsanforderungen auf Funktionsebene die richtigen Berechtigungen vorhanden sind. Der Zugriff oder die Visualisierung von administrativen URLs, Menüs und Seiten ohne ordnungsgemäße Authentifizierung ist eng mit dem Authentifizierungssystem integriert, um den Zugriff durch nicht autorisierte Benutzer zu verhindern.

A8 - Cross Site Request Forgery (CSRF)

WordPress verwendet kryptographische Token, genannt nonces, um die Absicht von Handlungsanfragen autorisierter Benutzer zu validieren, um sich vor potenziellen CSRF Bedrohungen zu schützen. WordPress bietet eine API für die Generierung dieser Token, um eindeutige und temporäre Token zu erstellen und zu verifizieren, und das Token ist auf einen bestimmten Benutzer, eine bestimmte Aktion, ein bestimmtes Objekt und einen

einen bestimmten Benutzer, eine bestimmte Aktion, ein bestimmtes Objekt und einen bestimmten Zeitraum beschränkt, die bei Bedarf zu Formularen und URLs hinzugefügt werden können. Zusätzlich werden alle Nonces beim Ausloggen ungültig.

A9 - Verwendung von Komponenten mit bekannten Schwachstellen

Das Core-Team von WordPress überwacht die wenigen Bibliotheken und Frameworks, die in WordPress integriert sind. In der Vergangenheit hat das Core-Team Beiträge zu verschiedenen Komponenten von Drittanbietern geleistet, um diese sicherer zu machen, wie zum Beispiel das Update zur Behebung einer standortübergreifenden Sicherheitslücke in TinyMCE in WordPress 3.5.2.

Wenn nötig, kann das Core-Team entscheiden, kritische externe Komponenten zu spalten oder zu ersetzen, z. B. als in 3.5.2 die SWFUpload-Bibliothek offiziell durch die Plupload 15 Bibliothek ersetzt wurde und eine sichere Sparte von SWFUpload vom Sicherheitsteam für diejenigen Plugins zur Verfügung gestellt wurde, die SWFUpload kurzfristig weiter verwenden.

A10 - Nicht validierte Um- und Weiterleitungen

Das interne Zugriffskontroll- und Authentifizierungs-System von WordPress schützt vor Versuchen, Benutzer zu unerwünschten Zielen oder automatischen Weiterleitungen zu leiten. Diese Funktionalität wird auch Plugin-Entwicklern über eine API zur Verfügung gestellt, `wp_safe_redirect()`.

Weitere Sicherheitsrisiken und Bedenken

XML-eXternal-Entity(XXE)-Angriffe

Bei der Verarbeitung von XML deaktiviert WordPress das Laden von benutzerdefinierten XML-Entitäten, um Angriffe sowohl auf externe Entitäten als auch auf Entitätserweiterungen zu verhindern. **Über die Kernfunktionalität von PHP hinaus bietet WordPress keine zusätzliche sichere XML-Verarbeitungs-API für Plugin-Autoren.**

Side-Request-Forgery(SSRF)-Angriffe

Von WordPress ausgegebene HTTP-Anfragen werden gefiltert, um den Zugriff auf Loopback und private IP-Adressen zu verhindern. Zusätzlich ist der Zugriff nur auf bestimmte Standard-HTTP-Ports erlaubt.

WordPress-Plugin und -Theme-Sicherheit

Das Standard-Theme

WordPress benötigt ein Theme, um Inhalte im Frontend sichtbar zu machen. Das Standard Theme, das mit WordPress ausgeliefert wird (derzeit „Twenty Twenty-One“), wurde aus Sicherheitsgründen sowohl vom Team der Theme-Entwickler als auch vom Core Entwicklungsteam intensiv überprüft und getestet.

Das Standard-Theme kann als Ausgangspunkt für die Entwicklung eines benutzerdefinierten Themes dienen, und Website-Entwickler können ein untergeordnetes Theme erstellen, das einige Anpassungen enthält, aber für die meisten Funktionen und Sicherheit auf das Standard-Theme zurückgreift. Das Standard-Theme kann problemlos von einem Administrator entfernt werden, wenn es nicht benötigt wird.

Themes- und Plugin-Repositories auf WordPress.org

Ungefähr 50.000+ Plugins und 5.000+ Themes sind auf der WordPress.org-Website gelistet. Diese Themes und Plugins werden zur Aufnahme eingereicht und von Freiwilligen manuell geprüft, bevor sie im Repository verfügbar sind.

Die Aufnahme von Plugins und Themes in das Repository ist keine Garantie dafür, dass sie frei von Sicherheitslücken sind. Für Plugin-Autoren gibt es Richtlinien, die vor der Einreichung zur Aufnahme im Repository beachtet werden sollen. Außerdem gibt es auf der WordPress.org-Website eine ausführliche Dokumentation über die WordPress-Theme Entwicklung.

Jedes Plugin und Theme kann vom Plugin- oder Theme-Besitzer kontinuierlich weiterentwickelt werden, und alle nachfolgenden Korrekturen oder Funktions Entwicklungen können in das Repository hochgeladen und den Benutzern des Plugins oder Themes mit einer Beschreibung der Änderung zur Verfügung gestellt werden. Website Administratoren werden über Plugins informiert, die über ihr Administrations-Dashboard aktualisiert werden müssen.

Wenn eine Plugin-Schwachstelle vom WordPress-Security-Team entdeckt wird, kontaktieren sie den Plugin-Autor und arbeiten zusammen, um eine sichere Version des Plugins zu erstellen und zu veröffentlichen. Wenn der Autor des Plugins nicht reagiert oder die Sicherheitslücke schwerwiegend ist, wird das Plugin/Theme aus dem öffentlichen Verzeichnis entfernt und in einigen Fällen direkt vom Sicherheitsteam behoben und aktualisiert.

Das Review-Team für Themes

Das Theme-Review-Team ist eine Gruppe von Freiwilligen, geleitet von zentralen und etablierten Mitgliedern der WordPress-Community, die Themes prüfen und genehmigen, die zur Aufnahme in das offizielle WordPress-Theme-Verzeichnis eingereicht wurden.

Das Theme-Review-Team pflegt die offiziellen Theme-Review-Guidelines, die Theme-Unit-Test Datas und die Theme-Check -plugins und versucht, die Theme-Entwickler-Community von WordPress in Bezug auf bewährte Praktiken zu informieren. Die Einbindung in die Gruppe wird von Core-Committern des WordPress-Entwicklungsteams moderiert.

Die Rolle des Webhosting-Providers bei der WordPress-Sicherheit

WordPress kann auf einer Vielzahl von Plattformen installiert werden. Obwohl die WordPress-Core-Software viele Maßnahmen für den Betrieb einer sicheren Web Anwendung bereitstellt, die in diesem Dokument behandelt wurden, ist die Konfiguration des Betriebssystems und der zugrunde liegende Web-Server Hosting der Software ebenso wichtig, um die WordPress-Anwendungen sicher zu halten. Wir bieten sichere, performante Hostingoptionen in der Google Cloud, siehe unser Angebot WordPress in Google Cloud.

Hostingoptionen für WordPress

Wählen Sie aus einfachen Bereitstellungen oder vollständig anpassbaren Hostingoptionen für WordPress aus.

Hostingtyp	Google Cloud-Dienst	Optimal für
Virtuelle Maschine (empfohlen)	**WordPress in Compute Engine** Die einfachste und schnellste Bereitstellungsoption für WordPress in Google Cloud. Stellen Sie WordPress mit nur einem Klick auf einer einzigen Compute Engine-Instanz bereit.	• Wenig bis mittlerer Traffic • Grundlegende Skalierbarkeit • Blog und CMS
Vollständig verwaltete Infrastruktur	**WordPress in App Engine** Eine gute Option für WordPress-Installationen, die die Flexibilität von Anwendungscontainern erfordern – aber mit einer einfacheren Bereitstellung als WordPress in Google Kubernetes Engine.	• Variabler Traffic mit starken Spitzen • Hohe Skalierbarkeit • Einfachere Bereitstellung vor Flexibilität
Container	**WordPress in Kubernetes Engine** Eine gute und äußerst flexible Option für starken Traffic, die jedoch einen komplexeren Aufbau und eine komplexere Bereitstellung erfordert als bei App Engine.	• Starker Traffic • Autoscaling • Flexibilität vor einfacher Bereitstellung

Ein Hinweis zu WordPress.com und WordPress-Sicherheit

WordPress.com ist die größte WordPress-Installation der Welt und wird von Automattic, Inc. betrieben, die von Matt Mullenweg, dem Mitgestalter des WordPress-Projekts, gegründet wurde. WordPress.com läuft auf der Core-Software WordPress, und hat seine eigenen Sicherheitsprozesse, Risiken und Lösungen. Dieses Dokument bezieht sich auf die Sicherheit in Bezug auf die selbst gehostet, herunterladbare Open-Source-Software WordPress von WordPress.org, die auf jedem Server in der Welt installierbar ist.

Anhang

WordPress-Core-APIs

Das Application-Programming-Interface (API) des WordPress-Cores besteht aus mehreren einzelnen APIs , von denen jede die Funktionen abdeckt, die mit einem bestimmten Satz von Funktionen verbunden sind. Zusammen bilden sie die Projektschnittstelle, die es Plugins und Themes ermöglicht, mit den Core-Funktionen von WordPress sicher zu interagieren, sie zu ändern und zu erweitern.

Während jede WordPress-API die beste Methode und standardisierte Möglichkeiten zur Interaktion und Erweiterung der WordPress-Core-Software bietet, sind die folgenden WordPress-APIs für die Durchsetzung und Absicherung der WordPress-Sicherheit am wichtigsten:

Datenbank-API

Die in WordPress 0.71 hinzugefügte Datenbank-API wendet die korrekte Methode für den Zugriff auf Daten als benannte Werte an, die in der Datenbankschicht gespeichert sind.

Dateisystem-API

Die Dateisystem API, hinzugefügt in WordPress 2.6, wurde ursprünglich für die WordPress-eigene Funktion für automatische Updates erstellt. Die Dateisystem-API abstrahiert die Funktionalität, die zum sicheren Lesen und Schreiben von lokalen Dateien in das Dateisystem auf einer Vielzahl von Host-Typen benötigt wird.

Dies geschieht über die Klasse `WP_Filesystem_Base` und mehrere Unterklassen, die je nach individueller Host-Unterstützung unterschiedliche Möglichkeiten der Verbindung zum lokalen Dateisystem implementieren. Jedes Theme oder Plugin, das Dateien lokal schreiben muss, sollte dies mit der WP_Filesystem-Klassenfamilie tun.

HTTP-API

Die HTTP-API, die in WordPress 2.7 hinzugefügt und in WordPress 2.8 erweitert wurde, standardisiert die HTTP-Anfragen für WordPress. Die API verarbeitet Cookies, gzip-Kodierung und -Dekodierung, Chunk-Dekodierung (wenn HTTP 1.1) und verschiedene andere HTTP Protokoll-Implementierungen. Die API standardisiert Anfragen, testet jede Methode vor dem Senden und verwendet, basierend auf ihrer Serverkonfiguration, die entsprechende Methode, um die Anfrage zu stellen.

Berechtigungen und aktuelle Benutzer-API

Die Berechtigungen und die aktuelle Benutzer-API sind eine Reihe von Funktionen, die helfen, die Berechtigungen und Befugnisse des aktuellen Benutzers zu überprüfen, um eine angeforderte Aufgabe oder Operation auszuführen und können außerdem gegen unbefugte Benutzer schützen, die über ihre zulässigen Berechtigungen hinaus auf Funktionen zugreifen oder diese ausführen wollen.

Lizenz des Whitepaper-Inhalts

Mit einem besonderen Dank für das Sicherheits-Papier von Drupal, das die Mitglieder des WordPress-Core-Teams inspiriert hat.

Zusätzliche Informationen

- WordPress-News: https://wordpress.org/news/
- WordPress-Sicherheits-Releases: https://wordpress.org/news/category/security/
  WordPress-Entwicklungs-Ressourcen: https://developer.wordpress.org/

Verfasst von Sara Rosso
Mitgewirkt haben Barry Abrahamson, Michael Adams, Jon Cave, Helen Hou-Sandí, Dion Hulse, Mo Jangda, Paul Maiorana