KLUGE & SCHLAAK

Kluge & Schlaak Ratgeber

Die größten Sicherheitsrisiken in WordPress: Ein Leitfaden für Start-up-CEOs

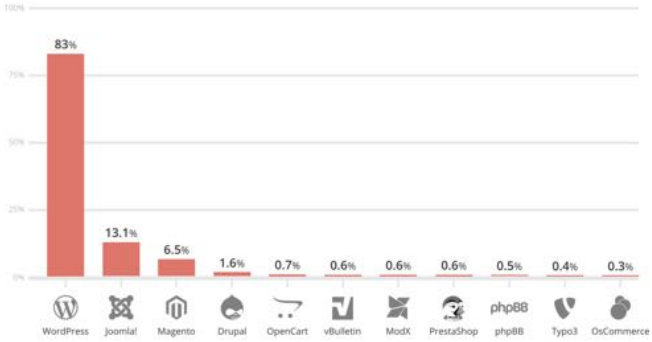
Inhaltsverzeichnis

01. Einleitung

WordPress ist das beliebteste Content Management System (CMS) der Welt. Der Marktanteil von WordPress liegt bei erstaunlichen 43% aller Webseiten. Allerdings zieht diese Beliebtheit auch Angreifer an.

Als Geschäftsführer eines Start-ups tragen Sie eine besondere Verantwortung: Sie müssen diese Risiken minimieren. **Eine Vernachlässigung dieser Pflicht kann zu zivil- und strafrechtlichen Konsequenzen führen.**

In diesem Ratgeber möchten wir Ihnen einen Überblick über die wichtigsten Sicherheitsrisiken in WordPress geben und wie wir Ihnen helfen können, Ihre Website zu schützen.



Über 80% aller Angriffe auf Open-Source-Plattformen im Jahr 2018 betrafen WordPress-Webseiten.

02. Brute-Force-Passwortangriffe

Brute-Force-Passwortangriffe sind eine häufige Angriffsmethode, bei der Angreifer versuchen, sich Zugriff auf ein Benutzerkonto zu verschaffen, indem sie systematisch tausende verschiedene Passwörter ausprobieren. Dank Tools wie WPScan können hunderte Kombination pro Sekunde durchgetestet werden.

Dieser Angriff zielt auf schwache oder wiederverwendeter Passwörter ab und kann zu einer erfolgreichen Übernahme Ihrer WordPress-Website führen.

Lösungen

In unseren Workshops zeigen wir Ihnen, wie Angreifer bei Brute-Force-Angriffen vorgehen und welche Methoden sie verwenden, um Passwortlisten zu erstellen. Wir vermitteln Ihnen praktische Techniken zur Benutzer-Identifikation, mit denen Sie potenziell gefährdete Benutzerkonten identifizieren können.

Darüber hinaus zeigen wir Ihnen, wie Angreifer geleakte Passwortlisten einsetzen oder soziale Daten wie Namen, Geburtsdaten oder Informationen über Familienmitglieder und Haustiere kombinieren, um Passwortlisten zu erstellen.

CUPP unterstützt beim Sammeln von Informationen über ein Opfer, um Benutzer-Passwort-Kombinationen zu generieren

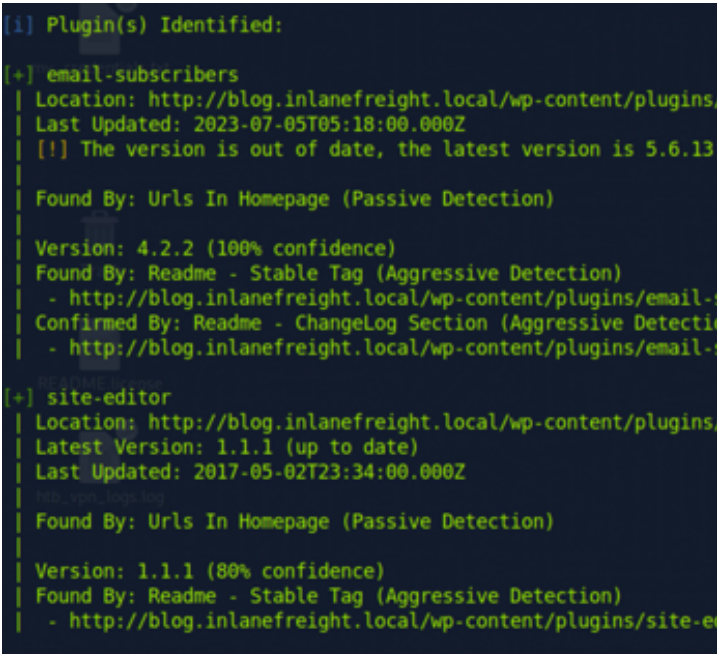
03. Plugins & Themes

Plugins und Themes bieten Ihnen die Möglichkeit, Ihre WordPress-Website mit zusätzlichen Funktionen und einem ansprechenden Design zu erweitern.

Allerdings können diese auch Sicherheitslücken aufweisen. Da sie von unabhängigen Drittanbietern entwickelt werden, sind sie eigenständig für die Gewährleistung der Sicherheit und die regelmäßige Aktualisierung ihrer Erweiterungen verantwortlich.

Lösungen

In unseren Workshops zeigen wir Ihnen, wie Sie Plugins und Themes sicher verwenden können. Wir erklären, wie Sie gefährdete Plugins erkennen und wie Angreifer diese nutzen würden, um Kontrolle über die Webseite und die Infrastruktur zu erlangen.



WPScan unterstützt Informationen über gefährdete Plugin & Themes einer WordPress-Seite zu sammeln

04. Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS)-Schwachstellen gehören zu den häufigsten Angriffsvektoren von Webanwendungen. Eine XSS-Schwachstelle kann es einem Angreifer ermöglichen, beliebigen JavaScript-Code im Browser des Ziels auszuführen und zu einer vollständigen Kompromittierung der Webanwendung führen, wenn sie mit anderen Schwachstellen gekoppelt ist.

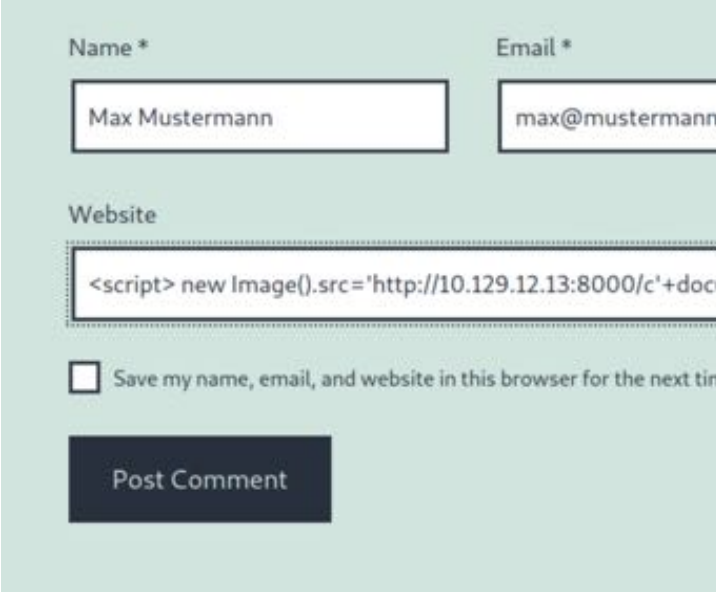
Das Ziel dieser Angriffe ist es, Code in ihre Website einschleusen, der dann von anderen Benutzern ausgeführt wird. Beispielsweise können Formulare genutzt werden, um bösartige Code in die Datenbank der Website einzufügen.

Dies bedeutet, dass bei jedem Aufruf der Website durch einen Benutzer der schadhaften Code als Teil der Antwort an den Browser des Benutzers gesendet wird.

XSS-Angriffe zielen darauf ab, vertrauliche Benutzerdaten zu stehlen oder bösartige Aktionen im Namen des Benutzers auszuführen.

Lösungen

In unseren hands-on Workshops zeigen wir Ihnen, wie Hacker XSS-Angriffe durchführen und wie Sie Ihre Website gegen diese Angriffe absichern können. Wir demonstrieren bewährte Sicherheitspraktiken und geben Ihnen praktische Anleitungen zur Überprüfung und Absicherung.



Simpler XSS-Angriff der es erlaubt den Cookie und somit die Identität anderer Benutzer zu stehlen

05. Über den Autor

Sebastian Schlaak ist Mitbegründer renommierter Startups und Absolvent der Stanford-Universität mit Abschlüssen sowohl in Informatik als auch in Management.

Mit einer Erfahrung von über 10 Jahren in der Entwicklung von Apps und Webanwendungen und dem Aufbau von IT-Organisationen ist er ein erfahrener Ausbilder im Bereich Cybersecurity.

In seiner Karriere hat er maßgeblich zur Sicherheit und dem Wachstum namhafter Berliner Startups beigetragen, indem er sie als Interim-CTO unterstützte. Dabei legte er immer großen Wert auf die Entwicklung und Umsetzung effektiver Sicherheitsstrategien.

Sebastian Schlaak bei LinkedIn

Kontaktieren Sie uns

Unsere hands-on Workshops bieten Ihnen umfassende Unterstützung, um Ihre WordPress-Website vor den wichtigsten Sicherheitsrisiken zu schützen.

Kontaktieren Sie uns noch heute, um weitere Informationen zu unseren maßgeschneiderten Schulungen und Sicherheitsdiensten zu erhalten.

info@klugeundschlaak.de

+49 (0)30 754 378 77