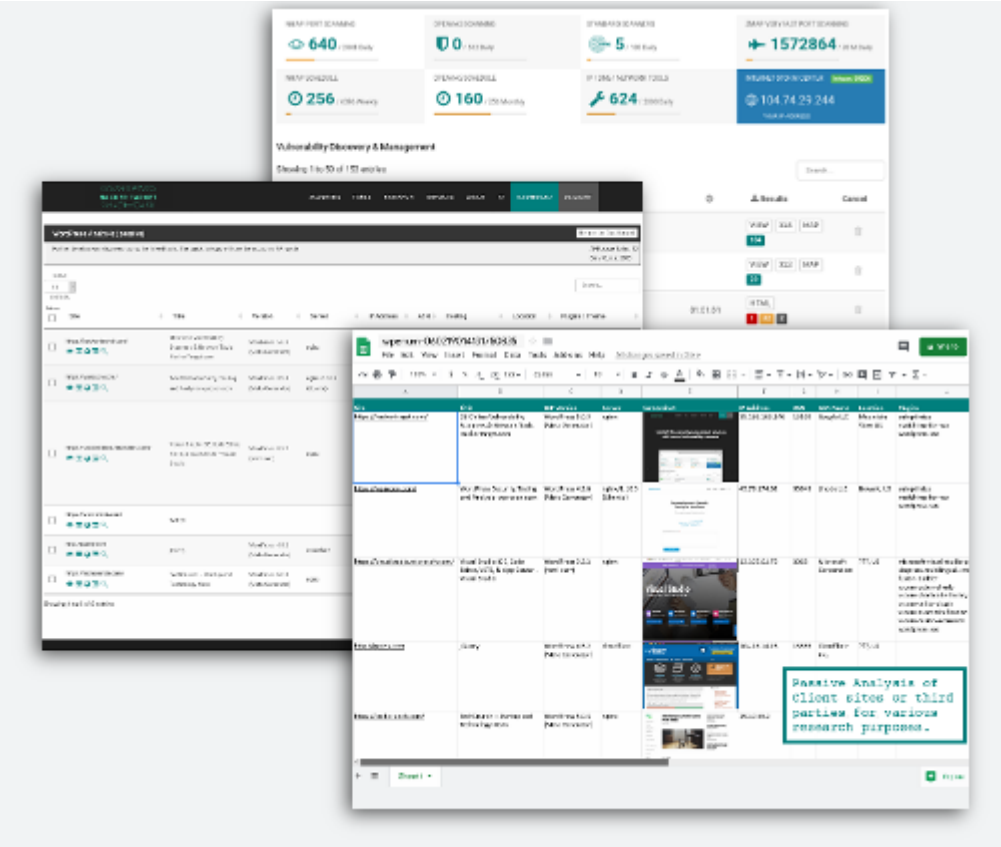
WordPress-Sicherheitsscan



WordPress Security Scan | HackerTarget.com

Perform an automated WordPress Security Scan, no installation required. WP is the worlds leading content management system making it a popular target.

WordPress-Sicherheitsscan

Online WordPress Security Scanner zum **Testen von Schwachstellen** einer WordPress-Installation. Zu den Prüfungen gehören Anwendungssicherheit, WordPress-Plugins, Hosting-Umgebung und Webserver.

Auf dieser WordPress-Sicherheitstestseite gibt es zwei Optionen. Die erste ist eine KOSTENLOSE **passive** Prüfung, die eine Handvoll Seiten von der Website herunterlädt und eine

Analyse des rohen HTML-Codes durchführt. Die zweite Option ist ein gründlicher **aktiver** Scan, der versucht, Plugins, Themes und Benutzer mit benutzerdefinierten WordPress-Audit-Skripten aufzulisten, die das Nmap NSE-Framework verwenden.

Brauchen Sie einen Experten? Wir identifizieren und validieren Möglichkeiten **zur Verbesserung Ihrer Sicherheit** WordPress-Analyse und Sicherheitsscan

Führen Sie einen **kostenlosen WordPress-Sicherheitsscan** mit einem Low-Impact-Test durch .

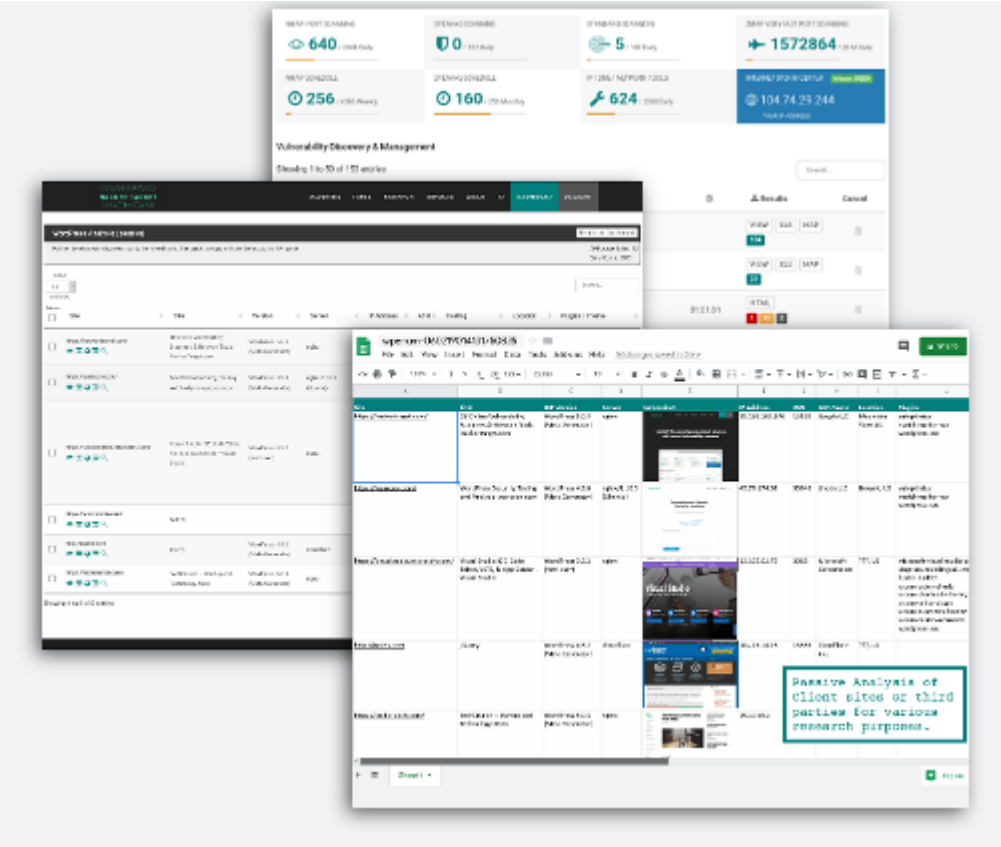
Überprüfen Sie jede WordPress-basierte Website und erhalten Sie einen umfassenden Überblick über die Sicherheitslage der Website. Sobald Sie sehen, wie einfach es ist, eine Mitgliedschaft zu erwerben und **WordPress** + Server-**Schwachstellen** mit Nmap WordPress NSE-Skripten, Nikto, OpenVAS und mehr zu testen.

Artikel, die im KOSTENLOSEN Scan überprüft wurden
Versuchen Sie, die Version von WordPress Core zu erkennen Finden Sie Plugins in der HTML-Antwort Identifizieren Sie das verwendete Thema Versuchen Sie, die ersten 2 WP-Benutzer aufzuzählen Listen Sie Seitenressourcen auf, einschließlich js und iframes Testen Sie, ob die Verzeichnisindizierung an Schlüsselpositionen aktiviert ist Überprüfen Sie die Reputation von Google Safe Browse Geben Sie die zu testende(n) WordPress-Site(s) ein *

WordPress-Aufzählungstyp

Gültige(s) Ziel(e)
www.example.com https://example.com/ 192.16.1.1

Login für WordPress Enumeration & Vulnerability Scanners
Aggressive Aufzählung von Plugins, Themen, Versionen und interessanten URLs.



VORTEILE DER MITGLIEDSCHAFT

- Erkennen Sie WP-Plugin-Versionen, Themen und Benutzer mit **Nmap NSE-Skripten**
- Identifizieren Sie die **Angriffsfläche** durch Plugin- und Themenaufzählung
- Passiver Analysebericht für bis zu 1000 Websites mit einem Klick
- Testen Sie WordPress mit **OpenVAS** und **Nikto** Scanners
- Zugriff auf **27 Schwachstellen-Scanner** und **OSINT-** Tools
- **Vertrauenswürdige** Open-Source-Tools

Über die WordPress-Sicherheitsscans

Der grundlegende Sicherheitscheck überprüft eine WordPress-Installation auf häufige sicherheitsrelevante Fehlkonfigurationen. Beim Testen mit der **Basisprüfungsoption** werden normale Webanfragen verwendet. Das System lädt eine

Handvoll Seiten von der Zielseite herunter und führt dann eine Analyse der resultierenden HTML-Quelle durch.

Die **aggressivere** Aufzählungsoption versucht, alle Plugins/Designs zu finden, die in der WordPress-Installation verwendet werden, und versucht, Benutzer der Website aufzuzählen. Diese Tests generieren **HTTP 404-Fehler** in den Webserverprotokollen der Zielseite. Seien Sie gewarnt Wenn Sie alle Plugins testen, werden mehr als 18000 Protokolleinträge generiert und möglicherweise Intrusion Prevention-Maßnahmen ausgelöst.

Indem Sie alle Plugins, Themen und Benutzer der Website identifizieren, beginnen Sie, die Angriffsfläche zu verstehen. Mit diesen Informationen können Sie gezielt weitere Tests mit den entdeckten Ressourcen durchführen.

2554
veröffentlichte CVE's (Schwachstellen) für
WordPress und seine Komponenten

Vergleich der Optionen

Kostenloser WordPress-Sicherheitscheck

- **Testen Sie bis zu 20 Websites** gleichzeitig mit dem passiven WordPress-Analysetool
- WordPress-Versionsprüfung
- Website-Reputation von Google
- Standard-Administratorkonto aktiviert
- Verzeichnisindizierung auf Plugins
- Websites, die von der Hauptseite extern verlinkt sind (Reputationsprüfungen)
- Listen Sie WordPress-Plugins auf, die durch grundlegende HTML-Analyse erkannt wurden (versuchen Sie die aktive Aufzählungsoption für eine aggressivere Erkennung von Plugins).
- Javascript verlinkt

- iframes vorhanden
- Hosting-Reputations- und Geolokalisierungsinformationen

Zusätzliche Vorteile (mit Mitgliedschaft)

- **Testen Sie bis zu 1000 Websites** gleichzeitig mit dem passiven WordPress-Analysetool
- Verwenden Sie Nmap NSE-Skripte für die WordPress-Prüfung
- Plugins identifizieren in /wp-content/plugins/aus einer Datenbank von über 18000
- Identifizieren Sie Themen in /wp-content/themes/aus einer Datenbank von über 2600
- Fingerabdruck der Version der entdeckten Plugins und Designs, um bekannte Schwachstellen zu identifizieren
- Zählen Sie bis zu 50 Benutzernamen auf
- Benutzerdefinierter OpenVAS-WordPress-Scan zum Testen von WordPress- und Server-Schwachstellen.

- Mit der Mitgliedschaft haben Sie **vollen Zugriff auf alle Sicherheitstest-Tools,** einschließlich Port-Scanner, Webserver-Tests und System-Schwachstellen-Scanner.

7 Tage Geld-zurück-Garantie

WordPress ist das weltweit führende Content-Management-System . Das macht sie zu einem beliebten Ziel für Angreifer.

Die Analyse kompromittierter WordPress-Installationen zeigt, dass die Ausnutzung am häufigsten aufgrund einfacher Konfigurationsfehler oder durch Plugins und Themes erfolgt, auf die keine Sicherheitsfixes angewendet wurden.

Die von unserem WordPress-Sicherheitsscan durchgeführten Prüfungen weisen auf offensichtliche Sicherheitsmängel in der WordPress-Installation hin. Außerdem werden empfohlene sicherheitsbezogene Konfigurationsverbesserungen

bereitgestellt, um die Sicherheit der Website vor zukünftigen Angriffen zu erhöhen.