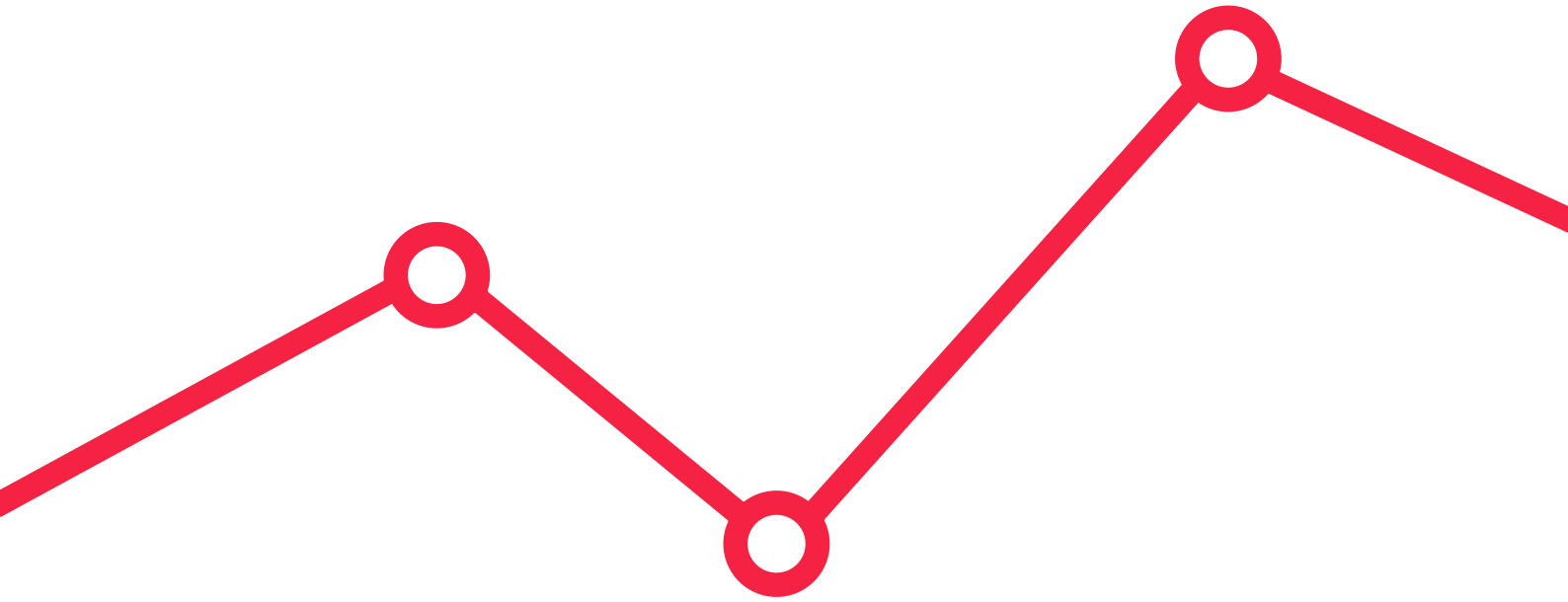
byteReport

byteReport | Ihr persönlicher Webseitencheck

www.bytepark.de

Report erstellt am:
20. August 2019 um 09:55 Uhr



Wie geht es meiner Webseite?

Als bytepark entwickeln wir seit 2001 sichere und skalierbare Webanwendungen. Mit dem byteReport stellen wir nun unseren Webseitencheck zur Verfügung. Sie erhalten innerhalb von 24 Stunden einen Report, der wichtige Schwachstellen aus den Bereichen Leistung, Barrierefreiheit, Best Practices, SEO, Progressive Web App und Sicherheit & Setup in einem verständlichen Dokument zusammenfasst. Mit dem byteReport erhalten Sie hilfreiche Verbesserungsvorschläge.

Messungen im byteReport für Nutzer mit Mobilgeräten

bytepark GmbH Schützenstraße 8 10117 Berlin +49 30 2000521-0 bytereport@bytepark.de https://byteReport.me

byteReport | Ihr Ergebnis (Zusammenfassung)

Der nachfolgende byteReport für www.bytepark.de wurde am 20. August 2019 um 09:55 Uhr erstellt und ergab in den einzelnen Bereichen folgende Ergebnisse:

Leistung

90

Diese Prüfungen stellen sicher, dass eine Webseite im Hinblick auf das Ladeverhalten für ein maximales Nutzererlebnis optimiert wurde.

Barrierefreiheit

92

Mit diesen Prüfungen erfahren Sie, wie Sie die Barrierefreiheit Ihrer Web-App verbessern. Nur bestimmte Probleme mit der Barrierefreiheit können durch automatisierte Tests erkannt werden, weshalb es empfehlenswert ist, zusätzlich manuelle Tests durchzuführen.

Best Practices

100

Diese Prüfungen zeigen Möglichkeiten auf, die allgemeine Qualität der Web-App anhand gängiger Best Practices zu verbesseren.

SEO

98

Mit diesen Prüfungen ist gewährleistet, dass Ihre Seite für das Ergebnis-Ranking von Suchmaschinen optimiert ist. Darüber hinaus gibt es aber auch noch andere Faktoren, die sich auf das Such-Ranking Ihrer Seite auswirken können und die dieser Report nicht berücksichtigt.

Progressive Web App

59

Mit diesen Prüfungen wird untersucht, ob und wie Ihre Seite als Progressive Web App funktioniert.

Sicherheit & Setup

100

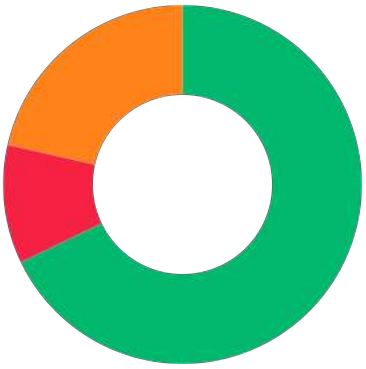
Mit diesen Prüfungen werden wichtige Sicherheitseinstellungen getestet. Hierbei werden sowohl die Webinhalte als auch das Setup des Servers und die DNS-Einstellungen der Domain untersucht.

- 90-100 Punkte: Sehr gut, hier besteht vorerst kein Handlungsbedarf.
- 50-89 Punkte: Es gibt kleinere und mittelgroße Probleme, lesen Sie auf den folgenden Seiten, was getan werden kann.
- 0-49 Punkte: Wichtig: byteReport hat einige gravierende Schwachstellen gefunden. Mehr dazu erfahren Sie in diesem Bericht.

Welcher Handlungsbedarf besteht?

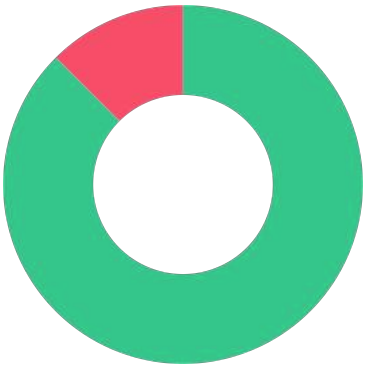
Die folgende Kurzübersicht zeigt die Verteilung der Analyseergebnisse auf.

Leistung



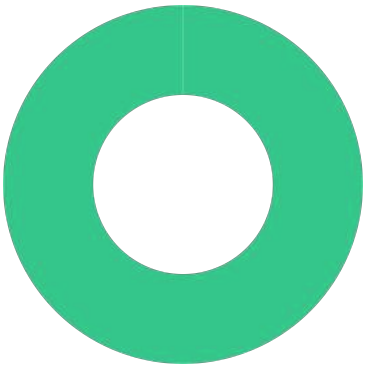
19 6 3

Barrierefreiheit



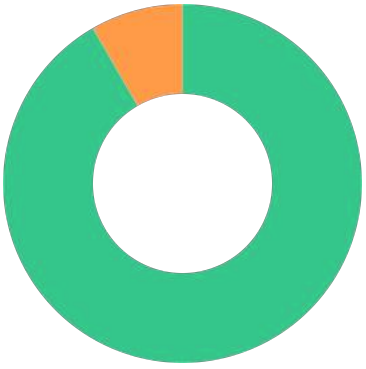
7 0 1

Best Practices



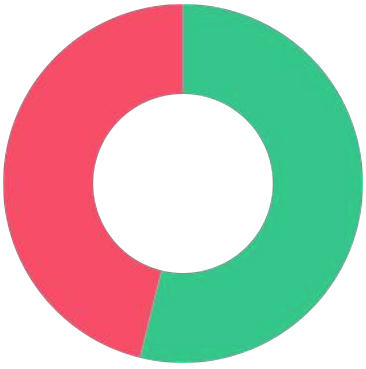
15 0 0

SEO



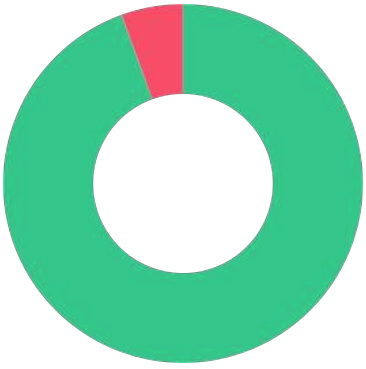
11 1 0

Progressive Web App



7 0 6

Sicherheit & Setup



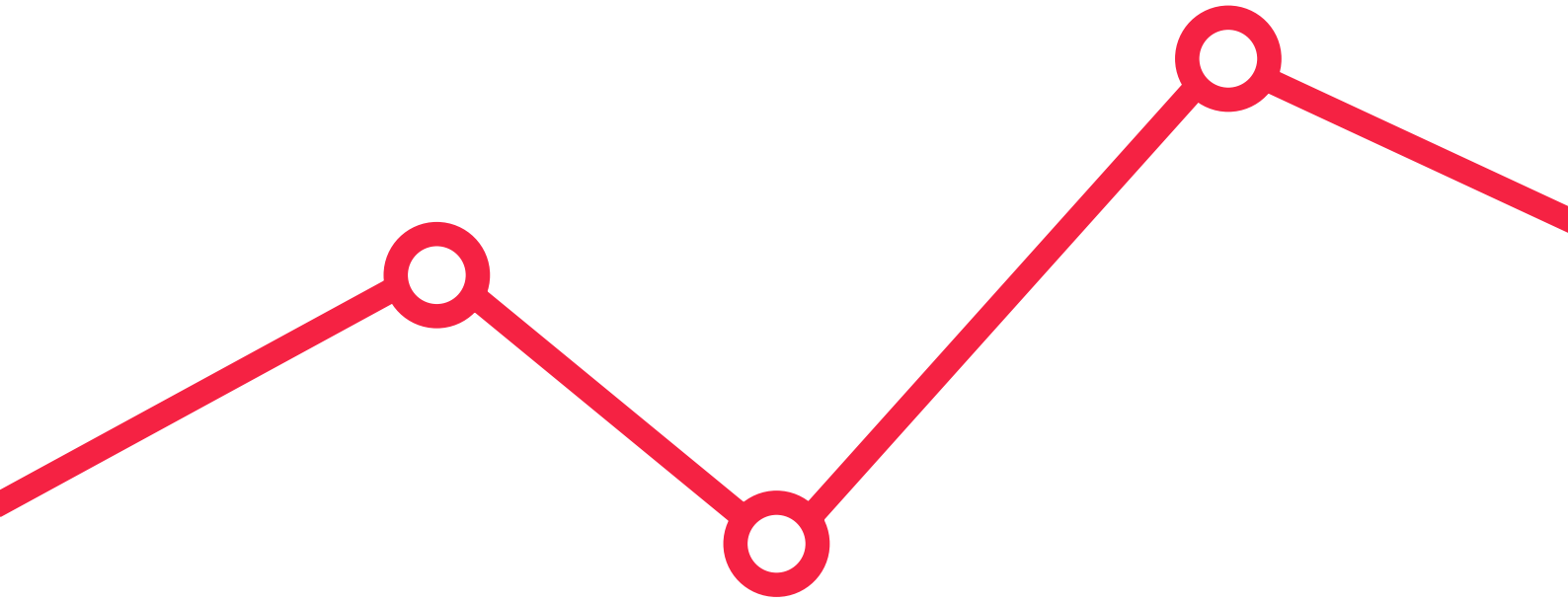
17 0 1

Erfolgreiche Analysen (kein Handlungsbedarf)

Analyse mit Warnung

Fehlgeschlagene Analyse

Ihre Ergebnisse im Detail



Was bedeuten die Ergebnisse?

Die Prüfergebnisse auf den nachfolgenden Seiten richten sich inhaltlich vor allem an den verantwortlichen Entwickler der geprüften Webseite, da sie technisch aufzeigen, welche Verbesserungen vorgenommen werden sollten bzw. welche spezifischen Werte in den Prüfungen gemessen wurden.

Leistung

Diese Prüfungen stellen sicher, dass eine Webseite im Hinblick auf das Ladeverhalten für ein maximales Nutzererlebnis optimiert wurde.

90

von 100

Hier besteht Handlungsbedarf (nach Dringlichkeit sortiert): Ergebnis:

Bilder in modernen Formaten bereitstellen — Mögliche Einsparung von 3.995 ms

Bildformate wie JPEG 2000, JPEG XR und WebP bieten oft eine bessere Komprimierung als PNG oder JPEG, was schnellere Downloads und einen geringeren Datenverbrauch ermöglicht.

Statische Inhalte mit einer effizienten Cache-Richtlinie bereitstellen — 28 Ressourcen gefunden

Eine lange Lebensdauer des Cache kann wiederholte Besuche Ihrer Seite beschleunigen.

URL	Cache-TTL (s)	Größe (KB)
...mobile-web-app/thumbnail_bc.png	0.000	2,150.59
...-app-flutter/thumbnail_roth.png	0.000	1,503.45
...bseite-drupal/thumbnail_cih.jpg	0.000	182.27
...arbeiten-bei-bytepark-title.jpg	0.000	175.29
...sets/img/agency/header/home.jpg	0.000	161.22
...mobile-web-app/thumbnail_bc.png	0.000	159.86
...-app-flutter/thumbnail_roth.png	0.000	126.43
...ets/img/video-previews/jobs.jpg	0.000	92.39
...scg-corporate/thumbnail_scg.png	0.000	84.58
...artsys-verify/thumbnail_gvl.png	0.000	64.2
...park.de/assets/js/main.2-3-0.js	0.000	36.74
...e/assets/img/customers/audi.png	0.000	35.87
...park.de/assets/js/libs.2-3-0.js	0.000	32.59
...rk.de/assets/css/main.2-3-0.css	0.000	30.12
https://bytestat.de/matomo.js	0.000	22.96
...-iot-button/thumbnail_igepa.png	0.000	21.43
...bseite-drupal/thumbnail_cih.jpg	0.000	17.74
...assets/img/customers/lekker.png	0.000	17.14
...uktur-hosting/thumbnail_scc.jpg	0.000	13.69
.../audi-moments/audimoments01.jpg	0.000	12.64
....de/assets/img/customers/bm.png	0.000	10.89
...tal-dekkel-online/header-bg.jpg	0.000	10.18
...e/assets/img/customers/immo.png	0.000	9.44
...tbot-howie/thumbnail_saturn.png	0.000	9.31
.../easy-locker/easy-locker-bg.jpg	0.000	7.05
...assets/img/customers/adidas.png	0.000	6.27
...g/bytepark_logotype_primary.svg	0.000	2.82
...k.de/assets/css/print.2-3-0.css	0.000	1.7

Sehr große Netzwerknutzlasten vermeiden — Die Gesamtgröße war 5.006 KB

Große Netzwerknutzlasten kosten Nutzer bares Geld und hängen eng mit langen Ladezeiten zusammen.

URL	Größe (KB)
...rlin-cuisine-mobile-web-app/thumbnail_bc.png	2,150.59
...-werke-native-app-flutter/thumbnail_roth.png	1,503.45
...bundeswehr-webseite-drupal/thumbnail_cih.jpg	182.27
...blog/2016/06/arbeiten-bei-bytepark-title.jpg	175.29
...ytepark.de/assets/img/agency/header/home.jpg	161.22
...rlin-cuisine-mobile-web-app/thumbnail_bc.png	159.86
...-werke-native-app-flutter/thumbnail_roth.png	126.43
...epark.de/assets/css/webfonts-woff2.2-3-0.css	121.63
...tepark.de/assets/img/video-previews/jobs.jpg	92.39
...00w/projects/scg-corporate/thumbnail_scg.png	84.58

Maximale potenzielle erste Eingabelatenz — 180 ms

Die erste Eingabelatenz, die bei Ihren Nutzern auftreten kann, entspricht der Dauer der längsten Aufgabe in Millisekunden.

Vorverbindung zu erforderlichen Ursprüngen aufbauen — Mögliche Einsparung von 310 ms

Versuchen Sie, Hinweise auf Ressourcen für eine Vorverbindung oder einen DNS-Vorabruf hinzuzufügen, damit möglichst frühzeitig eine Verbindung zu wichtigen Drittanbieterursprüngen hergestellt wird.

Aufwand für Hauptthread minimieren — 2,8 s

Versuchen Sie, die Zeit für das Parsen, Kompilieren und Ausführen von JS zu reduzieren. Die Bereitstellung kleinerer JS-Nutzlasten kann dabei helfen.

Kategorie	Zeitaufwand (s)
Other	1.281
Style & Layout	0.596
Script Evaluation	0.507
Rendering	0.258
Parse HTML & CSS	0.112
Script Parsing & Compilation	0.031

Zeit bis Interaktivität — 4,3 s

Die Zeit bis Interaktivität entspricht der Zeit, die vergeht, bis die Seite vollständig interaktiv ist.

Ressourcen beseitigen, die das Rendering blockieren — Mögliche Einsparung von 150 ms

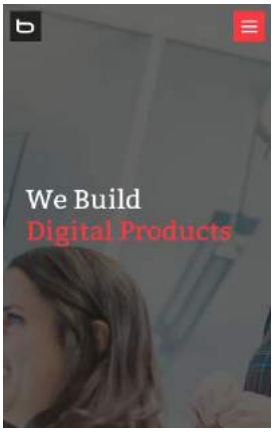
Ressourcen blockieren das erste Zeichnen Ihrer Seite. Versuchen Sie, wichtiges JS und wichtige CSS inline bereitzustellen und alle nicht kritischen JS und Stile aufzuschieben.

Nicht verwendete CSS entfernen — Mögliche Einsparung von 56 ms

Sie können ungültige Regeln aus Stylesheets entfernen und das Laden von CSS aufschieben, die nicht für ohne Scrollen sichtbare Inhalte verwendet werden, um unnötigen Datenverbrauch durch Netzwerkaktivität zu vermeiden.

Final Screenshot

Der letzte Screenshot des Seitenaufbaus.



Erfolgreiche Analysen (kein Handlungsbedarf): Ergebnis:

Erste Inhalte gezeichnet 2,2 s

"Erste Inhalte gezeichnet" gibt an, wann der erste Text oder das erste Bild gezeichnet wird.

Inhalte weitgehend gezeichnet 2,2 s

"Inhalte weitgehend gezeichnet" gibt an, wann die Hauptinhalte einer Seite sichtbar sind.

Geschwindigkeitsindex 3,1 s

Der Geschwindigkeitsindex zeigt an, wie schnell die Inhalte einer Seite sichtbar dargestellt werden.

Erster CPU-Leerlauf 3,4 s

"Erster CPU-Leerlauf" gibt den Zeitpunkt an, an dem die Aktivität des Hauptthreads der Seite das erste Mal gering genug ist, um Eingaben zu verarbeiten.

Geschätzte Eingabelatenz 20 ms

Bei der geschätzten Eingabelatenz handelt es sich um eine Schätzung dessen, wie viele Millisekunden Ihre App benötigt, um während des 5-s-Fensters mit der stärksten Auslastung beim Seitenaufbau auf Nutzereingaben zu reagieren. Wenn die Latenz bei Ihnen über 50 ms liegt, empfinden Nutzer Ihre App möglicherweise als langsam.

Gesamtzeit Blockierung der Webseite 140 ms

Summe aller Zeiträume zwischen FCP und Time to Interactive, wenn die Aufgabenlänge 50 ms überschreitet, ausgedrückt in Millisekunden.

Bilder richtig dimensionieren

Stellen Sie Bilder bereit, die eine angemessene Größe haben, um mobile Daten zu sparen und die Ladezeit zu verbessern.

Nicht sichtbare Bilder aufschieben

Versuchen Sie, nicht sichtbare und versteckte Bilder erst laden zu lassen, nachdem wichtige Ressourcen geladen wurden, um die Zeit bis zur Interaktivität zu reduzieren.

CSS komprimieren

Durch die Komprimierung von CSS-Dateien kann die Größe von Netzwerknutzlasten reduziert werden.

JavaScript komprimieren

Durch die Komprimierung von JavaScript-Dateien können Nutzlastgrößen und die Zeit zum Parsen von Skripts reduziert werden.

Bilder effizient codieren

Optimierte Bilder werden schneller geladen und verbrauchen weniger mobile Daten.

Textkomprimierung aktivieren

Textbasierte Ressourcen sollten mit Komprimierung (gzip, Deflate oder Brotli) bereitgestellt werden, um die Datenmenge im Netzwerk insgesamt zu minimieren.

Serverantwortzeiten sind niedrig (TTFB) — Stammdokument brauchte 0 ms

TTFB (Time To First Byte) erkennt den Zeitpunkt, an dem Ihr Server eine Antwort sendet.

Mehrere Weiterleitungen auf die Seite vermeiden

Weiterleitungen führen zu zusätzlichen Verzögerungen, bevor die Seite geladen werden kann.

Wichtige Anforderungen vorab laden

Mit <link rel=preload> können Sie das Abrufen von Ressourcen priorisieren, die aktuell später beim Seitenaufbau angefordert werden.

Videoformate für animierte Inhalte verwenden

Große GIF-Dateien sind nur bedingt für die Bereitstellung animierter Inhalte geeignet. Sie können statt GIF MPEG4- oder WebM-Videos für Animationen und PNG oder WebP für statische Bilder verwenden und so die Netzwerk-Datenmenge reduzieren.

Vermeidung einer exzessiven DOM Größe — 242 elements

Browserhersteller empfehlen, dass Seiten weniger als ~1.500 DOM-Elemente enthalten. Der Sweet Spot ist eine Baumtiefe von < 32 Elementen und weniger als 60 Kinder/Eltern-Elementen. Ein großer DOM kann den Speicherverbrauch erhöhen, längere Style-Berechnungen verursachen und teure Layout-Reflows erzeugen.

Statistik	Element	Wert
Anzahl an DOM Elementen	-	242
Maximale DOM Tiefe	-	9
Anzahl von Child Elementen	-	15

JavaScript-Ausführungszeit — 0,5 s

Versuchen Sie, die Zeit für das Parsen, Kompilieren und Ausführen von JS zu reduzieren. Die Bereitstellung kleinerer JS-Nutzlasten kann dabei helfen.

URL	CPU-Zeit insgesamt (s)	Skriptauswertung (s)	Parsen von Skripten (s)
Other	2.294	0.046	0.003
...at.de/matomo.js	0.166	0.160	0.006
...s/main.2-3-0.js	0.155	0.144	0.011

URL	CPU-Zeit insgesamt (s)	Skriptauswertung (s)	Parsen von Skripten (s)
...s/libs.2-3-0.js	0.096	0.085	0.009
...ww.bytepark.de/	0.074	0.072	0.002

Der gesamte Text bleibt während der Webfont-Ladevorgänge sichtbar

Sie können Gebrauch von der CSS-Funktion "font-display" machen, um sicherzugehen, dass der Text für Nutzer sichtbar ist, während Webfonts geladen werden.

Barrierefreiheit

92

von 100

Mit diesen Prüfungen erfahren Sie, wie Sie die Barrierefreiheit Ihrer Web-App verbessern. Nur bestimmte Probleme mit der Barrierefreiheit können durch automatisierte Tests erkannt werden, weshalb es empfehlenswert ist, zusätzlich manuelle Tests durchzuführen.

Hier besteht Handlungsbedarf (nach Dringlichkeit sortiert): Ergebnis:

Das Kontrastverhältnis von Hintergrund- und Vordergrundfarben ist nicht ausreichend.

Text mit geringem Kontrast ist für viele Nutzer schlecht oder gar nicht lesbar.

Fehlerhafte Elemente

.nav-main__logo
.db > .text-highlight
.btn--highlight
a[href$="impressum\/"]
a[href$="datenschutz\/"]
.phonenumber
a[href="mailto\:webpost\@bytepark\.de"]

Erfolgreiche Analysen (kein Handlungsbedarf): Ergebnis:

Die Seite enthält eine Überschrift, einen Link zum Überspringen oder einen Landmark-Bereich

Wenn Tastaturnutzer sich wiederholende Inhalte überspringen können, sorgt das für eine effizientere Navigation.

Dokument verfügt über ein <title>-Element

Anhand des Titels wissen Screenreader-Nutzer, worum es auf der Seite geht, während Nutzer von Suchmaschinen auf der Grundlage des Titels entscheiden, ob eine Seite für ihre Suche relevant ist.

Für das <html>-Element ist ein [lang]-Attribut angegeben

Wenn auf einer Seite kein "lang"-Attribut angegeben ist, nimmt ein Screenreader an, dass der Text darauf in der Standardsprache ist, die der Nutzer beim Einrichten des Screenreaders ausgewählt hat. Wenn die Sprache aber nicht der Standardsprache entspricht, gibt der Screenreader den Inhalt der Seite möglicherweise falsch aus.

Für das [lang]-Attribut des <html>-Elements ist ein gültiger Wert angegeben

Durch Angabe einer gültigen [Sprache gemäß BCP 47](https://www.w3.org/International/questions/qa-choosing-language-tags#question) kann der Text von einem Screenreader korrekt wiedergegeben werden.

Für Bildelemente sind [alt]-Attribute vorhanden

Informative Elemente sollten einen kurzen, beschreibenden alternativen Text haben. Dekorative Elemente können mit einem leeren ALT-Attribut ignoriert werden.

Links haben einen leicht erkennbaren Namen

Linktext, der leicht erkennbar, eindeutig und fokussierbar ist, verbessert die Navigation für Screenreader-Nutzer. Dies gilt auch für alternativen Text für Bilder, die als Links verwendet werden.

"[user-scalable="no"]" wird nicht im <meta name="viewport">-Element verwendet und das [maximum-scale]-Attribut ist nicht kleiner als 5.

Wenn Sie die Zoomfunktion deaktivieren, haben Nutzer mit eingeschränktem Sehvermögen, die auf die Bildschirmvergrößerung angewiesen sind, möglicherweise Probleme dabei, den Inhalt einer Webseite zu sehen.

Best Practices

Diese Prüfungen zeigen Möglichkeiten auf, die allgemeine Qualität der Web-App anhand gängiger Best Practices zu verbesseren.

100

von 100

Erfolgreiche Analysen (kein Handlungsbedarf): Ergebnis:

Vermeidet Anwendungs-Cache

Die Anwendungs-Cache API ist veraltet und sollte nicht mehr verwendet werden.

Benutzt HTTPS

Alle Webseiten sollten mit HTTPS geschützt werden, auch solche, die nicht mit sensiblen Daten umgehen. HTTPS verhindert, dass Angreifer die Kommunikation zwischen Ihrer App und Ihren Benutzern manipulieren oder passiv überwachen, und ist eine Voraussetzung für HTTP/2 und viele neue Webplattform-APIs.

Verwendet HTTP/2 für seine eigenen Ressourcen.

HTTP/2 bietet viele Vorteile gegenüber HTTP/1.1, einschließlich Binär-Header, Multiplexing und Server-Push. Idealerweise werden die eigenen Ressourcen über HTTP/2 ausgeliefert.

Nutzt passive Listener, um die Bildlaufleistung zu verbessern.

Erwägen Sie, Ihre Touch und Wheel Event Listeners als "passiv" zu kennzeichnen, um die Page Scroll Performance zu verbessern.

Vermeidet `document.write()`

Für Benutzer mit langsamen Verbindungen können externe Skripte, die dynamisch über `document.write()` injiziert werden, das Laden der Seite um viele Sekunden verzögern.

Links zu Cross-Origin Destinationen sind sicher

Fügen Sie `rel="noopener"` oder `rel="noreferrer"` zu jedem externen Link, um die Performance zu erhöhen und Sicherheit zu stärken.

Es wird vermieden, die Berechtigung für die Geolokalisierung beim Laden der Seite anzufordern.

Benutzer werden misstrauisch oder sind verwirrt von Websites, die ihren Standort ohne Kontext anfordern. Erwägen Sie stattdessen, die Anforderung an Benutzergesten zu binden.

Die Seite hat den HTML Doctype

Die Angabe eines Doctyps verhindert, dass der Browser in den Quirks-Mode wechselt.

Vermeidet Einsatz von Frontend-JavaScript-Bibliotheken mit bekannten Sicherheitsrisiken

Einige Skripte von Drittanbietern können bekannte Sicherheitsschwachstellen enthalten, die von Angreifern leicht identifiziert und ausgenutzt werden können.

Erkannte JavaScript-Bibliotheken

Alle Front-End-JavaScript-Bibliotheken, die auf der Seite erkannt werden.

Name	Version
jQuery	3.4.1

Vermeidet es, die Benachrichtigungsberechtigung beim Laden der Seite anzufordern.

Benutzer werden misstrauisch oder sind verwirrt von Websites, welche die Berechtigung zum Senden von Benachrichtigungen ohne Kontext anfordern. Erwägen Sie stattdessen, die Anforderung an Benutzergesten zu binden.

Vermeidet veraltete APIs

Veraltete APIs werden unter Umständen aus dem Browser entfernt.

Erlaubt Nutzern das Einfügen von Passworten aus der Zwischenablage

Die Verhinderung des Einfügens von Passworten aus der Zwischenablage in Formularfelder widerspricht gängigen Sicherheitsempfehlungen.

Keine Browserfehler in der Konsole protokolliert.

In der Konsole protokollierte Fehler zeigen ungeklärte Probleme an. Sie können durch Fehler bei Netzwerkanfragen und andere Browserprobleme verursacht werden.

Zeigt Bilder mit korrektem Seitenverhältnis an.

Die Abmessungen der Bildanzeige sollten dem natürlichen Seitenverhältnis entsprechen.

SEO

98

von 100

Mit diesen Prüfungen ist gewährleistet, dass Ihre Seite für das Ergebnis-Ranking von Suchmaschinen optimiert ist. Darüber hinaus gibt es aber auch noch andere Faktoren, die sich auf das Such-Ranking Ihrer Seite auswirken können und die dieser Report nicht berücksichtigt.

Hier besteht Handlungsbedarf (nach Dringlichkeit sortiert): Ergebnis:

Größe von Tippzielen ist nicht richtig eingestellt 90 % der Tippziele haben eine passende Größe

Interaktive Elemente wie Schaltflächen und Links sollten groß genug sein (48 x 48 px) und genügend Platz um sich herum haben, um einfach angetippt werden zu können. Dabei sollten sie sich aber nicht mit anderen Elementen überschneiden.

Tippziel	Größe (KB)	Sich überschneidendes Ziel
...a.phonenumber	129x18	...l-1of2--xsl > p.footer__section-text > a

Erfolgreiche Analysen (kein Handlungsbedarf): Ergebnis:

Hat ein `<meta name="viewport">` -Tag mit `Width` oder `Initial-Scale`.

Fügen Sie einen Viewport-Meta-Tag hinzu, um Ihre Anwendung für mobile Bildschirme zu optimieren.

Dokument verfügt über ein <title>-Element

Anhand des Titels wissen Screenreader-Nutzer, worum es auf der Seite geht, während Nutzer von Suchmaschinen auf der Grundlage des Titels entscheiden, ob eine Seite für ihre Suche relevant ist.

Dokument enthält eine Meta-Beschreibung

Meta-Beschreibungen können in die Suchergebnisse aufgenommen werden, um die Seiteninhalte kurz zusammenzufassen.

Seite hat einen gültigen HTTP-Statuscode

Seiten mit ungültigen HTTP-Statuscodes werden möglicherweise nicht richtig indexiert.

Links haben beschreibenden Text

Mit beschreibendem Linktext können Suchmaschinen Ihre Inhalte besser verstehen.

Seite ist nicht von Indexierung ausgeschlossen

Suchmaschinen können Ihre Seiten nicht in die Suchergebnisse aufnehmen, wenn sie nicht dazu berechtigt sind, sie zu crawlen.

robots.txt ist gültig

Wenn Ihre robots.txt-Datei fehlerhaft ist, können Crawler möglicherweise nicht nachvollziehen, wie Ihre Website gecrawlt oder indexiert werden soll.

Für Bildelemente sind [alt]-Attribute vorhanden

Informative Elemente sollten einen kurzen, beschreibenden alternativen Text haben. Dekorative Elemente können mit einem leeren ALT-Attribut ignoriert werden.

Dokument enthält ein gültiges "hreflang"-Element

Anhand von "hreflang"-Links können Suchmaschinen ermitteln, welche Version einer Seite sie in den Suchergebnissen für eine bestimmte Sprache oder Region anzeigen sollen.

Dokument enthält gut lesbare Schriftgrößen — 100 % gut lesbarer Text

Schriftgrößen von weniger als 12 px sind zu klein und deshalb nicht gut lesbar, sodass Nutzer von Mobilgeräten den Text per Fingerbewegung heranzoomen müssen. Mindestens 60 % des Texts auf der Seite sollten deshalb eine Schriftgröße von mindestens 12 px haben.

Source	Selector	% of Page Text	Font Size
Legible text	-	100.00%	≥ 12px

Dokument verwendet keine Plug-ins

Suchmaschinen können keine Plug-in-Inhalte indexieren und auf vielen Geräten werden Plug-ins eingeschränkt oder nicht unterstützt.

Progressive Web App

59

von 100

Mit diesen Prüfungen wird untersucht, ob und wie Ihre Seite als Progressive Web App funktioniert.

Hier besteht Handlungsbedarf (nach Dringlichkeit sortiert): Ergebnis:

Die aktuelle Seite reagiert nicht mit einer 200er-Meldung, wenn sie offline ist.

Wenn Sie eine Progressive Web App erstellen, sollten Sie einen Service Worker einsetzen, damit Ihre App offline arbeiten kann.

start_url regiert nicht mit einem 200er wenn offline

Ein Service Worker ermöglicht es Ihrer Webanwendung, unter unvorhersehbaren Netzwerkbedingungen zuverlässig zu sein.

- No usable web app manifest found on page.

Es wird kein Service Worker registriert, der die Seite und start_url kontrolliert

Service Worker ist die Technologie, die es Ihrer Anwendung ermöglicht, viele Funktionen der Progressiv Web App (PWA) zu nutzen, wie z.B. Offline, Hinzufügen zum Homescreen und Push-Benachrichtigungen.

Das Web App Manifest erfüllt nicht die Anforderungen an die Installationsfähigkeit.

Browser können Benutzer proaktiv auffordern, Ihre App auf ihrem Homescreen hinzuzufügen, was zu einem höheren Engagement führen kann.

- Failures: No manifest was fetched.

Ist nicht für einen benutzerdefinierten Splash-Screen konfiguriert.

Ein thematischer Splash-Screen sorgt für ein hochwertiges Erlebnis, wenn Benutzer Ihre App von ihrem Homescreen aus starten.

- Failures: No manifest was fetched.

Setzt keinen Farbcode für das Theme des Adressbalken.

Die Adressleiste des Browsers kann thematisch an Ihre Website angepasst werden.

- Failures: No manifest was fetched,
  No `<meta name="theme-color">` tag found.

Erfolgreiche Analysen (kein Handlungsbedarf): Ergebnis:

Seitenaufbau in Mobilfunknetzen ist schnell genug

Ein schneller Seitenaufbau über ein Mobilfunknetz sorgt dafür, dass die Seite für Nutzer auf Mobilgeräten angenehm zu bedienen ist.

Benutzt HTTPS

Alle Webseiten sollten mit HTTPS geschützt werden, auch solche, die nicht mit sensiblen Daten umgehen. HTTPS verhindert, dass Angreifer die Kommunikation zwischen Ihrer App und Ihren Benutzern manipulieren oder passiv überwachen, und ist eine Voraussetzung für HTTP/2 und viele neue Webplattform-APIs.

HTTP-Aufrufe werden auf HTTPS umgeleitet

Wenn HTTPS bereits für den Server eingerichtet ist, sollten alle Aufrufe über unverschlüsselte Verbindungen (HTTP) automatisch zu HTTPS umgeleitet werden.

Der Inhalt ist für das Ansichtsfenster (Viewport) korrekt dimensioniert.

Wenn die Breite des Inhalts Ihrer Anwendung nicht mit der Breite des Ansichtsfensters (Viewport) übereinstimmt, ist Ihre Anwendung möglicherweise nicht für mobile Bildschirme optimiert.

Hat ein `<meta name="viewport">` -Tag mit `Width` oder `Initial-Scale`.

Fügen Sie einen Viewport-Meta-Tag hinzu, um Ihre Anwendung für mobile Bildschirme zu optimieren.

Enthält einige Inhalte, wenn JavaScript nicht verfügbar ist.

Ihre App sollte einige Inhalte anzeigen, wenn JavaScript deaktiviert ist, auch wenn es sich nur um eine Warnung an den Benutzer handelt, dass JavaScript für die Nutzung der App erforderlich ist.

Hat ein gültiges `apple-touch-icon`

Für ein ideales Erscheinungsbild unter iOS, wenn Benutzer den Startbildschirm erweitern, definieren Sie ein Apple-Touch-Icon. Es muss auf ein intransparentes 192px (oder 180px) quadratisches PNG verweisen.

Sicherheit & Setup

Mit diesen Prüfungen werden wichtige Sicherheitseinstellungen getestet. Hierbei werden sowohl die Webinhalte als auch das Setup des Servers und die DNS-Einstellungen der Domain untersucht.

100

von 100

Hier besteht Handlungsbedarf (nach Dringlichkeit sortiert):

Ergebnis:

Server sendet einen `Server` Header

nginx

Um Fingerprinting zu vermeiden, sollte kein `Server` Header vom Server gesendet werden. Ein solcher Header hilft einem Angreifer dabei, automatisiert nach Servern mit Sicherheitslücken zu suchen.

Erfolgreiche Analysen (kein Handlungsbedarf): Ergebnis:

Benutzt HTTPS

Alle Webseiten sollten mit HTTPS geschützt werden, auch solche, die nicht mit sensiblen Daten umgehen. HTTPS verhindert, dass Angreifer die Kommunikation zwischen Ihrer App und Ihren Benutzern manipulieren oder passiv überwachen, und ist eine Voraussetzung für HTTP/2 und viele neue Webplattform-APIs.

HTTP-Aufrufe werden auf HTTPS umgeleitet

Wenn HTTPS bereits für den Server eingerichtet ist, sollten alle Aufrufe über unverschlüsselte Verbindungen (HTTP) automatisch zu HTTPS umgeleitet werden.

Server sendet einen starken Strict-Transport-Security (HSTS) Header `max-age=31536000; includeSubDomains; preload`

HTTP Strict Transport Security (HSTS) ist eine Server-Einstellung, die eine sichere Verbindung erzwingt. Durch den Einsatz von HSTS wird der Browser prüfen, ob eine sichere Verbindung über HTTPS auf die besuchte Webseite erfolgt. Wenn dies nicht der Fall ist, werden die Besucher automatisch von http auf https und damit auf die sichere Version der Website umgeleitet.

Server benutzt nur aktuelle SSL-Protokolle

Über die Jahre wurden und werden verschiedenen Schwachstellen in SSL und den TLS-Protokollen entdeckt. Aus diesem Grund sollten SSLv2, SSLv3, TLS 1.0 und TLS 1.1 in der Serverkonfiguration abgeschaltet werden, so dass nur das TLS Protokoll 1.2 und 1.3 aktiviert ist.

Es wurde eine Content-Security-Policy definiert default-src 'self'; object-src 'self'; frame-src 'self' bytestat.de *.vimeo.com *.addtoany.com; script-src *.bytepark.de bytestat.de *.vimeo.com *.fastcdn.co *.addtoany.com *.instagram.com *.adobe.com maps.googleapis.com 'unsafe-inline' 'unsafe-eval'; style-src 'self' data: 'unsafe-inline' *.fastcdn.co fonts.googleapis.com; img-src 'self' data: bytestat.de maps.gstatic.com maps.google.com maps.googleapis.com *.fastcdn.co *.instapage.com; font-src data: 'self' fonts.googleapis.com fonts.gstatic.com *.fastcdn.co *.googleapis.com; manifest-src 'self'undefined

Eine Content-Security-Policy (CSP) ist eine effektive Maßnahme, um eine Webseite vor XSS-Angriffen, Clickjacking und anderen Code Injections zu schützen. CSP definiert Quellen mit vertrauenswürdigem Content als Whitelist, wodurch erreicht wird, dass ein Browser Inhalte aus anderen Quellen nicht lädt oder ausführt.

Server sendet einen `X-XSS-Protection` Header 1; mode=block

Der Verarbeitung des HTTP X-XSS-Protection Header ist ein Feature in verschiedenen Browsern, das Seiten vom Laden stoppt, wenn sie reflektierte Cross-Site-Scripting-(XSS-)Angriffe erkennen.

Server sendet einen `X-Content-Type-Options` Header — nosniff

Der HTTP-Header `X-Content-Type-Options` ist ein Header, der vom Server verwendet wird, um anzuzeigen, dass die in den Content-Type-Headern beworbenen MIME-Typen nicht geändert und befolgt werden sollten. Dies ermöglicht es,MIME-Sniffing zu unterbinden.

Server sendet einen `X-Frame-Options` Header — SAMEORIGIN

Der `X-Frame-Options' Header schützt die Besucher der Webseite gegen Clickjacking-Attacken, in dem es das Laden des Inhalts als IFrame auf einer Seite eines Angreifers verhindert.

Es wurde ein gültiger Referrer-Policy Header gesetzt. — same-origin

Referrer-Policy ist ein neuer Header, mit dem eine Seite kontrollieren kann, wie viele Informationen bei Verlassen einer Seite mit übermittelt werden.

Es wurde ein gültiger Feature-Policy Header gesetzt. — accelerometer 'none'; ambient-light-sensor 'none'; autoplay 'none'; camera 'none'; encrypted-media 'none'; fullscreen 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; microphone 'none'; midi 'none'; payment 'none'; picture-in-picture 'none'; speaker 'none'; sync-xhr 'none'; usb 'none'; vr 'none'

Feature-Policy ist ein neuer Header, mit dem eine Seite kontrollieren kann, welche Funktionen und APIs des Browsers genutzt werden sollen.

Links zu Cross-Origin Destinationen sind sicher

Fügen Sie `rel="noopener"` oder `rel="noreferrer"` zu jedem externen Link, um die Performance zu erhöhen und Sicherheit zu stärken.

Erlaubt Nutzern das Einfügen von Passworten aus der Zwischenablage

Die Verhinderung des Einfügens von Passworten aus der Zwischenablage in Formularfelder widerspricht gängigen Sicherheitsempfehlungen.

Eine Datei security.txt ist verfügbar

Die Datei security.txt definiert Kontaktinformationen und weitere Details, wie und wohin Sicherheitsprobleme gemeldet werden können.

Server sendet keinen `X-Generator` Header

Um Fingerprinting zu vermeiden, sollte kein `X-Generator` Header vom Server gesendet werden. Ein solcher Header hilft einem Angreifer dabei, automatisiert nach Servern und Webseiten mit Sicherheitslücken zu suchen.

Seite hat keinen `generator` Meta-Tag

Um Fingerprinting zu vermeiden, sollte der `generator` Meta-Tag nicht im Quelltext ausgegeben werden. Dieser Tag hilft dabei, automatisiert nach Servern und Webseiten mit Sicherheitslücken zu suchen.

Domain hat einen CAA DNS-Eintrag

Ein CAA DNS-Eintrag limitiert, wer ein SSL-Zertifikat für eine Domain ausstellen kann. Die Prüfung wird seit September 2017 von allen Zertifizierungsstellen bei der Neuausstellung und Verlängerung von Zertifikaten durchgeführt.

Domain hat einen AAAA DNS-Eintrag für IPv6 2a06:2380:0:1::34d

IPv6 ist die neueste Version des Internet Protocol (IP). Für eine Erreichbarkeit ist ein AAAA DNS-Eintrag notwendig. IPv6 bringt neben einem deutlich erweitertem Adressraum auch effizienteres Routing und einige andere Vorteile.

byteReport | Ihr Ansprechpartner

Sie wollen mehr erfahren zum vorliegenden Report und auch in Zukunft kontinulierlich an der Verbesserung Ihrer Webseite arbeiten? Der byteReport kann Ihnen dabei helfen und Sie regelmäßig auf dem Laufenden halten. Sprechen Sie uns einfach an - wir beraten Sie gern.

Kontakt:

Bogu Wojciechowska
Head of Business Development
E-Mail: bytereport@bytepark.de
Telefon: +49 30 2000 521-0