Ergebnisse für **padlet.com**

Wiederholen
2020-12-03 18:05:46 Etc/UTC

HTTPS als Voreinstellung: ✔ Ja
Content Security Policy: ✖ fehlt ⓘ Berichte wurden übermittelt
Referrer Policy: ⓘ Referrers werden teilweise übermittelt
Cookies: **11** (11 First-Party; 0 Third-Party)
Drittanfragen (Third-Party): **29** Anfragen an 7 einzigartige Hosts
Serverstandort: Vereinigte Staaten von Amerika — 2606:4700::6812:1e24 Nachschlagen

Überprüfte URL: http://padlet.com
Weitergeleitet: https://padlet.com/

✔ HTTPS als Voreinstellung

`padlet.com` verwendet HTTPS als Voreinstellung.

Chromium hat folgendes entdeckt:

Status	Titel	Ergebnis	Beschreibung
✔	Certificate	valid and trusted	The connection to this site is using a valid, trusted server certificate issued by Cloudflare Inc ECC CA-3.
✔	Connection	secure connection settings	The connection to this site is encrypted and authenticated using TLS 1.3, X25519, and AES_128_GCM.
✔	Resources	all served securely	All resources on this page are served securely.

Weitere Informationen zur TLS/SSL-Konfiguration dieser Website:

- Analysiere padlet.com bei SSL Labs
- Observatory by Mozilla
- Mozilla TLS Observatory
- testssl.sh

Anleitung

HTTPS verschlüsselt nahezu alle Informationen, die zwischen Client und Webservice ausgetauscht werden. Richtig konfiguriert, garantiert es drei Dinge:

- **Vertraulichkeit**. Eine Verbindung ist verschlüsselt und URLs, Cookies und andere sensible Metadaten sind geschützt.
- **Authentizität**. Ein Besucher befindet sich auf der "echten" Website und nicht auf irgendeiner, die etwas vorgibt zu sein oder auf der eines "Man-in-the-Middle".
- **Integrität**. Zwischen einem Besucher und dem Betreiber einer Website ausgetauschte Daten wurden nicht manipuliert oder verändert.

Einfache HTTP-Verbindungen können leicht überwacht, verändert oder nachgeahmt werden. Jede unverschlüsselte verschickte HTTP-Anfrage beinhaltet Meta-Informationen und ermöglicht Rückschlüsse auf das Verhalten. Das Mitlauschen und Nachverfolgen von unverschlüsseltem Surfen ist zur Selbstverständlichkeit geworden.

Ziel der Internet-Community ist es, die Verschlüsselung als Standard zu etablieren und die Verwendung unverschlüsselter Verbindungen auslaufen zu lassen.

🔨 DSGVO: Erwägungsgrund 83, Art. 5.1.f, Art. 25, Art. 32.1
Nach DSGVO Art. 25 ist ein Controller für die Durchsetzung des Datenschutzes bereits in der Entwicklung und in Standardeinstellungen auf dem aktuellen Stand der Technik verantwortlich. Verschlüsselte Verbindungen sind eine etablierte Technologie zum Schutz der Privatsphäre von Website-Besuchern vor Lauschangriffen.

✖ Strict Transport Security

Eine HTTP Strict Transport Security (HSTS) fehlt.

HTTP Strict Transport Security (HSTS) ist ein breit

Anleitung

unterstützter Standard zum Schutz eines Besuchers, indem es sicher stellt, daß der Webbrowser eine Seite immer nur über HTTPS öffnen kann. Mit HSTS entfällt die unsichere Notwendigkeit der Weiterleitung eines Besuchers von `http://` - zu `https://` -URLs.

Wird dem Browser mitgeteilt, dass eine Domain HSTS nutzt, so macht er zwei Dinge:

- Verwendet immer eine `https://` -Verbindung, selbst wenn auf einen `http://` -Link geklickt wird oder wenn eine Domäne in der Adressleiste ohne Protokoll eingegeben wurde.
- Entfernt die Möglichkeit für Benutzer, Warnungen vor ungültigen Zertifikaten zu ignorieren.

Eine Domain teilt den Webbrowsern mit, dass sie HSTS aktiviert hat, indem sie einen HTTP-Header über eine HTTPS-Verbindung zurückgibt.

✖ Content Security Policy

Keine Content Security Policy (CSP) Header gefunden.

Anleitung

Die Tests für Content Security Richtlinen basieren auf dem Scanner des Mozilla HTTP Observatory Projektes (Mozilla Public License 2.0) von April King, von uns für Webbkoll implementiert. Die Beschreibungstexte sind von der Mozilla Observatory Website entnommen, CC-BY-SA 3.0. Für Fehler oder Ungenauigkeiten sind wir verantwortlich.

> Eine Content Security Policy (CSP) bildet eine zusätzliche Sicherheitsebene, die hilft Angriffe zu erkennen und zu entschärfen, einschließlich Cross Site Scripting (XSS) und Data-Injection-Angriffen. Solche Art von Angriffen sind geeignet, eine Website zu verunstalten, und reichen bis hin zum Datendiebstahl und Verbreitung von Malware.
>
> Ein Hauptziel von CSP ist es, XSS-Angriffe zu minimieren und zu melden. XSS-Angriffe nutzen das Vertrauen des Browsers in die vom Server empfangenen Inhalte aus. Bösartige Skripte werden vom Browser des Opfers ausgeführt, weil der Browser der Quelle des Inhalts vertraut, auch wenn er nicht von dort kommt, wo er herzukommen scheint.
>
> Die CSP ermöglicht es Serveradministratoren, Angriffsvektoren durch XSS-Angriffe zu reduzieren oder zu eliminieren, indem dem Browser bestimmte Domains als gültige Quellen u.a. für ausführbare Skripte mitgeteilt werden. Ein CSP-kompatibler Browser führt dann nur noch Skripte aus, die von diesen Whitelist-Domänen empfangen wurde und ignoriert alle anderen Skripte (einschließlich Inline-Skripte und HTML-Attribute zur Ereignisbehandlung).
>
> — *MDN: Content Security Policy (CSP), Mozilla Contributors, CC BY-SA 2.5*

🔨 DSGVO: Erwägungsgrund 83, Art. 5.1.f, Art. 25, Art. 32.2
DSGVO Art. 32.2 stellt klar, daß Maßnahmen gegen unbefugte Weitergabe oder Zugriffe auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten zu ergreifen sind. Eine CSP ist ein relativ einfacher Weg, um sicherzustellen, dass Webbesucher nicht unerwartet mit Dritten in Kontakt kommen.

ⓘ Referrer Policy

Referrer Richtline auf `strict-origin-when-cross-origin` im

Wenn Du auf einen Link klickst, sendet Dein Browser in

`Referrer-Policy` HTTP Header gesetzt.

Anleitung

der Regel den HTTP-Referer - also die Adresse, von der Du kommst - an den Webserver, auf dem sich die Ziel-Website befindet. Auf diese Weise können Websites sehen, woher ihre Besucher kommen. Der Header wird auch gesendet, wenn externe Ressourcen (wie Bilder, Schriften, JS und CSS) geladen werden.

Referrer-Header sind ein Alptraum für die Privatsphäre, da er es Webseiten und Diensten ermöglicht, Dich im gesamten Web zu verfolgen und Deine Surfgewohnheiten (und damit möglicherweise private, sensible Informationen) preiszugeben, insbesondere wenn dies in Kombination mit Cookies erfolgt.

Durch die Festlegung einer Referrer-Richtlinie ist es für Websites möglich, Browsern mitzuteilen, dass sie keine Referrer verlieren. Mit der Referrer-Richtlinie können Sie eine Richtlinie festlegen, die auf alle angeklickten Links sowie auf alle anderen von der Seite erzeugten Anfragen (Bilder, JS etc.) angewendet wird.

🔨 DSGVO: Erwägungsgrund 83, Art. 5.1.c, Art. 25, Art. 32.2
Das Setzen einer Referer Richtlinie ist ein schneller und einfacher Weg zur Datenminimierung (Art. 5.1.c) und stellt sicher, dass Daten nicht unnötigerweise oder unzulässigerweise übermittelt werden (Art. 32.2).

✖ Subresource Integrity (SRI)

Subresource Integrity (SRI) wurden nicht eingebunden. Externe Ressourcen werden über HTTP oder mit relativen URLs geladen src="//...".

Die folgenden Drittanbieter-Ressourcen werden ohne SRI geladen:

Typ	URL
css	`https://padlet.net/packs/css/home-d22e7576.chunk.css`
script	`https://padlet.net/packs/js/home-e857c3a07da29de7e42f.chunk.js`
script	`https://padlet.net/packs/js/1-1727e29571712b7c3af1.chunk.js`
script	`https://padlet.net/packs/js/0-4b44b1fdaf2855cbe4cb.chunk.js`
script	`https://padlet.net/packs/js/runtime~home-1617b4d7ad6087b673ba.js`
script	`https://www.googletagmanager.com/gtag/js?id=G-4M6WGE55N0`

> Subresource Integrity (SRI) ist ein Sicherheitsmerkmal, mit dem Browser überprüfen können, ob Ressourcen, die sie abrufen (z.B. von einem CDN), ohne unerwartete Manipulationen geliefert werden. Es funktioniert, indem es Ihnen erlaubt, einen kryptographischen Hash bereitzustellen, mit dem eine geholte Ressource übereinstimmen muss.
>
> Die Verwendung von Content Delivery Networks (CDNs) zum Hosten von Dateien wie Skripten oder Stilvorlagen kann die Leistung einer Website verbessern und die Bandbreite reduzieren. Die Verwendung von CDNs birgt jedoch auch das Risiko, dass wenn ein Angreifer die Kontrolle über ein CDN erlangt, er beliebige bösartige Inhalte in eine Website injizieren kann.
>
> Subresource Integrity minimiert das Risko solcher Angriffe. Es stellt sicher, dass Dateien einer Webanwendung, die von CDN oder sonstigen Quellen stammen, auch ohne Manipulationen geladen werden können.
>
> *— MDN, Subresource Integrity, Mozilla Contributors, CC BY-SA 2.5*

DSGVO: Erwägungsgrund 83, Art. 5.1.f, Art. 25, Art. 32.2
Dies ist eine einfache Maßnahme gegen unbefugte Offenlegung oder Zugriff auf personenbezogene Daten, welche übertragen, gespeichert oder anderweitig verarbeitet werden könnten.

Typ	URL
script	`//cdn.indicative.com/js/Indicative.min.js`
script	`https://padlet.net/libraries/alexa-20200924.js`

Anleitung

Der Subresource Integrity Test basiert auf dem Mozilla HTTP Observatory Scanner (Mozilla Public License 2.0) von April King, von uns für Webkoll implementiert.

HTTP-Kopfzeilen

Status	Kopfzeile	Wert	Ergebnis
✔	X-Content-Type-Options	nosniff	X-Content-Type-Options Header gesetzt auf "nosniff"
✘	X-Frame-Options		X-Frame-Options (XFO) Header fehlt
✘	X-XSS-Protection	0	X-XSS-Protection Header gesetzt auf "0" (inaktiv)

Anleitung

Der Header-Test basiert auf dem Mozilla HTTP Observatory Scanner (Mozilla Public License 2.0) von April King, von uns für Webbkoll implementiert. Die Beschreibungstexte sind von der Mozilla Observatory Website entnommen, CC-BY-SA 3.0.

Ein **`X-Content-Type-Options`** HTTP Header eines Servers gibt an, dass der jeweils gesendete MIME Content-Type einer Datei nicht verändert werden kann. Das Verhindert ein Ausspähen durch manipulierten MIME-Types oder in anderen Worten: Der Webmaster weiß, was sein Server genau macht.

Ein **`X-Frame-Options`** HTTP Antwort-Header wird verwendet, um einem Browser mitzuteilen, ob eine Seite in einem `<frame>`, `<iframe>` oder `<object>` angezeigt werden darf. Websites können dieses nutzen, um Clickjacking-Angriffe zu verhindern.

Der HTTP **`X-XSS-Protection`** Antwort-Header ist ein Feature des Internet Explorers, Chrome und Safari, das ein Nachladen bei einer entdeckten Cross-Site Scripting (XSS) Attacke verhindert. Gleichwohl ist dieser Header huetzutage in modernen Browswern weniger wichtig, wenn Weibseiten eine strenge `Content-Security-Policy` implementiert haben, die Inline JavaScripts (`'unsafe-inline'`) verhindert. Es kann aber weiterhin einen gewissen Schutz für ältere Browser darstellen, die keine CSP unterstützen.

— MDN, Content Security Policy (CSP), Mozilla Contributors, CC BY-SA 2.5

DSGVO: Art. 5.1.c, Art. 5.1.f, Art. 25, Art. 32.1-2. Diese Header helfen dabei, das Risiko eines Datenmissbrauchs zu minimieren.

Cookies

First-Party-Cookies (11)

Domain	Name	Wert	Verfällt am	HttpOnly	Secure	SameSite
.padlet.com	__cf_bm	846731464b0d01dabd4a...	2020-12-03 18:35:36Z	✔	✔	✔ (None)
.padlet.com	ww_p	QjBWZm1pWE5nenJOa3VT...	2070-12-03 18:05:36Z	✔	✔	✔ (None)

Domain	Name	Wert	Verfällt am	HttpOnly	Secure	SameSite
.padlet.com	__auc	7581142f17629c7e76b8...	2021-12-04 18:05:35Z	✗	✗	✗
.padlet.com	__asc	7581142f17629c7e76b8...	2020-12-03 18:35:35Z	✗	✗	✗
.padlet.com	_ga	GA1.1.1737768961.160...	2022-12-03 18:05:35Z	✗	✗	✗
.padlet.com	_ga_4M6WGE55N0	GS1.1.1607018735.1.0...	2022-12-03 18:05:35Z	✗	✗	✗
.padlet.com	ww_s	52245b4a0d8b3d8e60f8...	2020-12-03 18:35:36Z	✗	✓	✓ (None)
.padlet.com	ww_d	f83ec4f5c0491e83c643...	2070-12-03 18:05:35Z	✗	✓	✓ (None)
.padlet.com	__cfduid	d97aff01fd9570bc5f53...	2021-01-02 18:05:35Z	✓	✗	✓ (Lax)
padlet.com	Indicative_e42b4377-...	"%7B%22defaultUnique...	2021-12-03 18:05:35Z	✗	✗	✗
padlet.com	ww_dpr	1	2042-08-19 21:56:52Z	✗	✗	✗

HttpOnly bedeutet, dass Cookies nur vom Server gelesen werden können und nicht durch JavaScript im Webbrowser. Das verhindert XSS (Cross-Site Scripting) Angriffe.

Secure bedeutet, dass ein Cookie nur über eine sichere (HTTPS) Verbindung gesendet wird. Das verhindert MITM (Man-in-the-Middle) Angriffe.

SameSite wird verwendet um dem Browser mitzuteilen, dass er nur dann Cookies senden darf, wenn die Anfrage von der gleichen Seite stammt. Das verhindert CSRF (Cross-Site Request Forgery) Angriffe.

🔨 GDPR: Erwägungsgrund 60, Erwägungsgrund 61, Erwägungsgrund 69, Erwägungsgrund 70, Erwägungsgrund 75, Erwägungsgrund 78, Art. 5.1.a, Art. 5.1.c, Art. 5.1.e, Art. 21, Art. 22, Art. 32.

e-PD (2002/58/EC). Rec. 24, 25, Art. 5.2.

e-PD revised (2009/136/EC). Rec. 65, 66.

Mehr Informationen

localStorage

Kein LocalStorage.

Wie Cookies speichern Web-Storage-Daten im Webbrowser eines Benutzers. Doch anders als Cookies wird ein Web Storage nicht über HTTP-Anfragen abgefragt, sondern immer nur direkt durch den Browser (mit JavaScript). Im Vergleich zu Cookies können deutlich mehr Daten gespeichert werden.

Es gibt zwei Arten: `LocalStorage` mit dauerhaft gespeicherten Daten (auch wenn der Browser geschlossen wird) und `SessionStorage`, das gelöscht wird sobald die Session einer Website beendet wird (anders Verhalten wie Session Cookies). Eine SessionStorage Sitzung gilt immer *pro Fenster/Tab*.

Dies kann verwendet werden, um Benutzer zu verfolgen und Profile zu erstellen indem JavaScript-Code den Speicher ausliest und an einen Server sendet.

🔨 DSGVO: Gleiche Bestimmungen wie bei Cookies weiter oben.

Drittanfragen (Third Party)

29 Anfragen (29 sicher, 0 unsicher) an 7 einzigartige Hosts.

Eine "Third-Party-Anfrage" ist ein Abruf von Ressourcen von einer anderen Domain als `padlet.com` oder einer ihrer Subdomains.

Host	IP	Land	Einordnung	URLs
api.indicative.com	2600:1901:0:cdcd::	US		Zeigen (4)
cdn.indicative.com	146.88.138.69	US		Zeigen (1)
certify.alexametrics.com	13.33.243.109	US	Analytics (Amazon.com)	Zeigen (1)
padlet.net	91.189.179.2	NO		Zeigen (12)
v1.padlet.pics	151.101.246.137	FI		Zeigen (8)
www.google-analytics.com	2a00:1450:400f:807::200e	IE	Analytics (Google)	Zeigen (2)
www.googletagmanager.com	2a00:1450:400f:808::2008	IE		Zeigen (1)

Wir nutzen Mozillas Version der Open-Source-Tracker-Liste von Disconnect, um Hosts zu klassifizieren.

🔨 GDPR: Erwägungsgrund 69, Erwägungsgrund 70, Art. 5.1.b-c, Art. 25.

Serverstandort

Der Server **padlet.com** (2606:4700::6812:1e24) scheint sich während unseres Tests in **Vereinigte Staaten von Amerika** zu befinden.

Weitere Informationen (z.B. Provider) zu dieser IP über KeyCDN abrufen.

Einige Seiten nutzen ein CDN, Content Delivery Networks. In diesem Falle hängt der angezeigte Serverstandort vom Standort des Besuchers ab. Webbkoll als Tool ist auf einem Server in Finnland beheimatet.

🔨 Mit der DSGVO gelten alle EU/EWR-Länder als gleichermaßen vertrauenswürdig, so dass es keinen besonderen Grund gibt, ein EU-Land als mehr oder

weniger zuverlässig oder vertrauenswürdig zu betrachten. Die Bedeutung des Standorts eines Servers kommt nur im Rahmen der DSGVO Art. 23, Beschränkung zum Tragen, bei denen sich die Mitgliedstaaten auf eine Reihe von Gründen, insbesondere auf die nationale Sicherheit, berufen können, die es ihnen ermöglicht, den Schutz für Besucher oder Webseiten-Betreiber aufzuheben.

Für Nicht-EU/EWR-Gebiete hängt es von (DSGVO Art. 44) ab. Für eine Website sind Übertragungen wahrscheinlich auf Abwägungsentscheidungen nach (Art. 45) der Europäischen Kommission angewiesen, wenn in einem Drittland nach ihren Rechtsvorschriften angemessene Datenschutzmaßnahmen vorgesehen sind. Abwägungsentscheidungen können jedoch nicht immer heran gezogen werden wie der Europäische Gerichtshof 2015 (C-362/14) zeigt. Verbindliche Unternehmensregeln (Art. 47) oder Standardklauseln (Art. 46) können auch zur Datenübermittlung herangezogen werden. Das ist aber mangels ausreichender Gerichts- und Datenschutzurteile noch auf rechtlich wackeliger Basis.

Original Header

Kopfzeile	Wert
cache-control	max-age=0, private, must-revalidate
cf-cache-status	DYNAMIC
cf-ray	5fbf37753db9caf8-ARN
cf-request-id	06cb60fd420000caf8f3baf000000001
content-encoding	br
content-type	text/html; charset=utf-8
date	Thu, 03 Dec 2020 18:05:35 GMT
expect-ct	max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
p3p	CP="IDC DSP COR CURa ADMa OUR NOR ONL COM"
referrer-policy	strict-origin-when-cross-origin
server	cloudflare
set-cookie	ww_d=f83ec4f5c0491e83c643a60e4ac66ea9; domain=.padlet.com; path=/; expires=Wed, 03 Dec 2070 18:05:35 GMT; Secure; SameSite=None ww_s=52245b4a0d8b3d8e60f8fa3a5868e1bd; domain=.padlet.com; path=/; expires=Thu, 03 Dec 20

Kopfzeile	Wert
	20 18:35:35 GMT; Secure; SameSite=None ww_p=MHVOUDhmUGxnYlhCZmpOMGhFMFBiWndCMUpXaWxIWXdXTHIjaW1oWkJDTFJyanFoaWVBQUdvQWZrdWIITFFvZEVicmM3NzRNbG1OejVGQ0RvUUdSZU03b1lUM1ROdDBnelg2Vi9hZnBObUE2aG54NnI5a2kranpBQXdqOWVjanFlcW1WRFN3V0MzalBXTnVTQmhNZ0c4TEI0QVpsR0NrajRSM2dYYjhMbzl5SnNSL2xaTVV6OEVmS2xoY3c2eEZmLS02WFpVeVVZODduZldqdXkwVFNLMFZnPT0%3D--8ec4949b5182a82dc71ba50e7626d98e07322df9; domain=.padlet.com; path=/; expires=Wed, 03 Dec 2070 18:05:35 GMT; HttpOnly; Secure; SameSite=None __cf_bm=aea778a44cecf58306d208ac7d90c32137d6f29e-1607018735-1800-ARdJk8CRrkpX9jLd1xdTvB2V4+MvNABRt67i7wmBRJ2eOua7QMTZgMq/h0GgvAEnrkW17ZMy99O9JYbH/ggINaM=; path=/; expires=Thu, 03-Dec-20 18:35:35 GMT; domain=.padlet.com; HttpOnly; Secure; SameSite=None
status	200
vary	Accept-Encoding, Accept-Language
via	1.1 google
ww-app-version	v-2012030155-production
ww-box	mozart-web-us-central1-n2-l812
x-content-type-options	nosniff
x-download-options	noopen
x-permitted-cross-domain-policies	none
x-request-id	eed83b23-7a60-4ad8-9226-8017766d4773
x-runtime	0.027358
x-xss-protection	0

Was genau prüft das Tool (und was nicht)

Dieses Tool simuliert den Aufruf einer Website mit einem typischen Webbrowser. Der Browser hat keine Addons/Erweiterungen und die Do-Not-Track Einstellungen sind nicht aktiviert, da das die Standardeinstellung in den meisten Browsern ist.

Dateien wie Bilder, Skripte und CSS-Stilvorlagen werden zwar geladen, das Tool führt jedoch keine Interaktionen mit der Website aus — es werden keine Links angeklickt und keine Formulare abgeschickt.

Hinweis: Fehler können passieren. Die Ergebnisse erheben keinen Anspruch auf 100% Richtigkeit. Dieses Tool ist

auch nicht als Analyse gedacht sondern eher als Ausgangspunkt für Website-Betreiber zur weiteren Verbesserung.

Texte über HTTPS teilweise übernommen aus The HTTPS-Only Standard (Public Domain). MaxMind's GeoLite2 Länderdatenbank (CC-BY-SA 4.0) wird für die GeoIP Abfragen verwendet. Bitte hier klicken für weitere Informationen.

Testergebnisse werden auf unserem Servern für 24 Stunden im Arbeitsspeicher gehalten. Wir zeigen keine Liste von zuletzt getesteten URLs. Wir verwenden keine URLs oder Testergebnisse. Wir loggen keine IP Adressen. Wir verwenden keine Cookies.

Entwickelt von dataskydd.net.

Der Quellcode ist auf GitHub verfügbar.

Feedback? Fragen? info@dataskydd.net

Twitter: @dataskyddnet

Unterstütze uns

d1f6324 2020-11-18 22:33:48 +0100