Unser Spezialgebiet? Die Sicherheit deiner Webseite!

Website: www.riffbird.com

Zeitpunkt des Scans: 24.04.2023 17:42

Risikobewertung

D	26	40	✓
Risiko-Score	Externe Dienste gefunden	Cookies gefunden	Datenschutzerklärung gefunden

Die Website läuft im Netzwerk von **Hetzner Online GmbH**. Der Serverstandort ist Deutschland.

Bei der Prüfung der Server-Sicherheit sind eine oder mehrere mögliche Sicherheitsrisiken gefunden worden. Wenn nicht schon geschehen, so sollten Sie dies durch Ihre Agentur oder einen Sicherheitsexperten prüfen lassen.

Sie setzen auf Ihrer Website die Consent Management Software **legalweb.io** ein, um vom Benutzer eine Einwilligung zum Setzen von Cookies zu einzuholen.

Ihr Consent Management Software ist nicht korrekt konfiguriert - Ihre Website setzt ohne Einwilligung des Users nicht notwendige Cookies und Dienste.

Ihre Website setzt ohne Einwilligung des Benutzers mindestens **9 nicht notwendige Cookies**. Dies ist nicht rechtssicher, da gemäß §25 des TTDSG für das Setzen derartiger Cookies eine aktive Einwilligung erforderlich ist.

Ihre Website lädt ohne Einwilligung des Benutzers mindestens **12 nicht notwendige Dienste**. Dies ist nicht rechtssicher, da sowohl der Europäische Gerichtshof 2019 als auch der Bundesgerichtshof 2020 geurteilt haben, dass dafür (analog zum Setzen von Cookies) eine aktive Einwilligung erforderlich ist.

Ihre Website lädt mindestens 13 Externe Dienste, die per IP-Adresse und Cookies personenbezogene Daten aus dem Rechtsraum der EU in Drittstaaten ausleiten, ohne dass eine Einwilligung des Benutzers vorliegt.

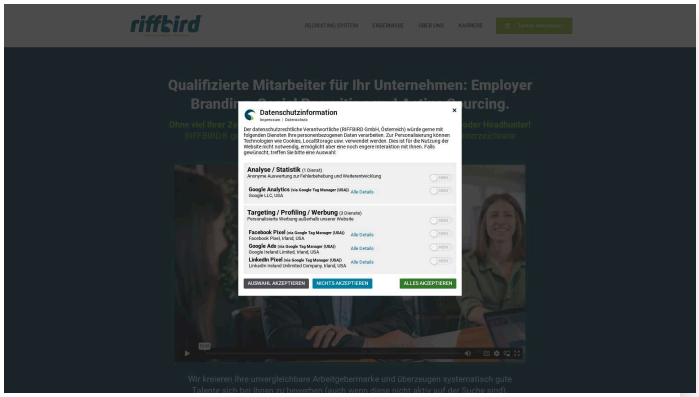
Sie verweisen in Ihrer Datenschutzerklärung auf das **Privacy-Shield** als Grundlage für eine Datenverarbeitung in den USA. Der Europäische Gerichtshof hat dieses jedoch in seinem "Schrems II"-Urteil für unwirksam erklärt.

Sie setzen Google Analytics mit aktivierter IP-Anonymisierung ein.

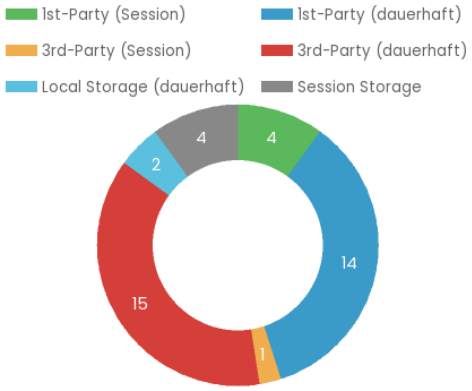
Sie binden **20 Externe Dienste** in Ihre Website ein, zu denen wir in der Datenschutzerklärung keinen Hinweis finden konnten. Damit verstoßen Sie gegen Ihre Informationspflicht nach Art. 13 der DSGVO.

Bitte beachten Sie, dass trotz aller Sorgfalt bei der Untersuchung nicht ausgeschlossen werden kann, dass die Website Datenschutzschwachstellen aufweist, die in diesem Report nicht aufgezeigt werden. Wir können keine Haftung für die Vollständigkeit dieses Reports übernehmen.

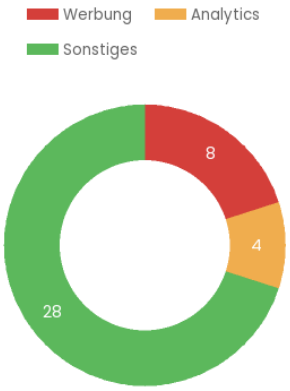
Ansicht Startseite



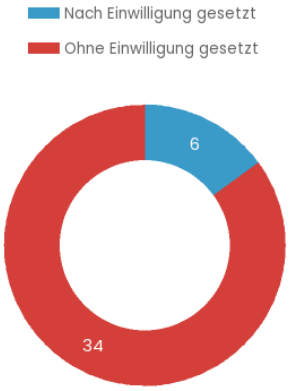
Cookies und Web-Speicher



Cookie-Typ



Verwendung



Einwilligung zum Setzen

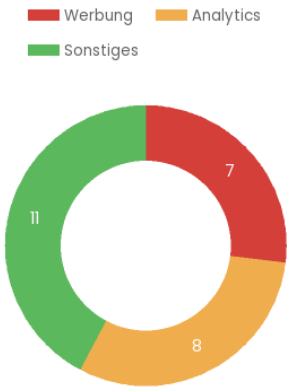
Cookies und Web-Speicher Übersicht

Name	Typ	Speicherdauer (Tage)	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt
__cf_bm	3rd-Party (dauerhaft)	1	vimeo.com	Unbekannt		Unbekannt	Nein
__cfruid Auf Unterseite gefunden (24.04.23 17:41)	3rd-Party (Session)	0	calendly.com	CloudFlare		Web-Speicher	Nein
_fbp	1st-Party (dauerhaft)	90	riffbird.com	Facebook Pixel	Ja (USA)	Werbung	Ja
_ga	1st-Party (dauerhaft)	400	riffbird.com	Google Analytics		Interaktion	Ja
_gat_UA-127965499-1	1st-Party (dauerhaft)	1	riffbird.com	Google Analytics		Interaktion	Ja
_gcl_au	1st-Party (dauerhaft)	90	riffbird.com	Unbekannt		Unbekannt	Nein

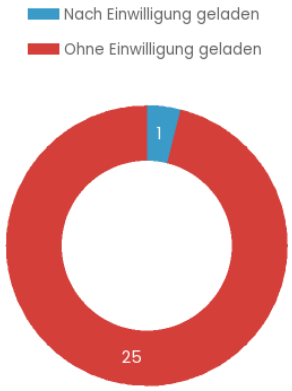
Name	Typ	Speicherdauer (Tage)	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt
_gid	1st-Party (dauerhaft)	1	riffbird.com	Google Analytics		Interaktion	Ja
_hjAbsoluteSessionInProgress Auf Unterseite gefunden (24.04.23 17:41)	1st-Party (dauerhaft)	1	riffbird.com	Hotjar		Analytics	Nein
_hjFirstSeen Auf Unterseite gefunden (24.04.23 17:41)	1st-Party (dauerhaft)	1	riffbird.com	Hotjar		Analytics	Nein
_hjIncludedInSessionSample_2881925 Auf Unterseite gefunden (24.04.23 17:41)	1st-Party (dauerhaft)	1	riffbird.com	Unbekannt		Unbekannt	Nein
_hjSessionUser_2881925 Auf Unterseite gefunden (24.04.23 17:41)	1st-Party (dauerhaft)	365	riffbird.com	Hotjar		Analytics	Nein
_tt_enable_cookie	1st-Party (dauerhaft)	390	riffbird.com	TikTok	Ja (China)	Soziale Medien	Nein
_ttp	3rd-Party (dauerhaft)	390	tiktok.com	TikTok	Ja (China)	Soziale Medien	Nein
_uetsid	1st-Party (dauerhaft)	1	riffbird.com	Bing Ads		Werbung	Nein
_uetsid_exp	Local Storage (dauerhaft)	unbegrenzt		Bing Ads		Werbung	Nein
_uetvid	1st-Party (dauerhaft)	390	riffbird.com	Bing Ads		Werbung	Nein
_uetvid_exp	Local Storage (dauerhaft)	unbegrenzt		Bing Ads		Werbung	Nein
AnalyticsSyncHistory	3rd-Party (dauerhaft)	30	linkedin.com	LinkedIn Widgets	Ja (USA)	Soziale Medien	Nein
attribution_user_id Auf Unterseite gefunden (24.04.23 17:41)	3rd-Party (dauerhaft)	365	typeform.com	Typeform		Interaktion	Nein
AWSALBTGCORS Auf Unterseite gefunden (24.04.23 17:41)	3rd-Party (dauerhaft)	7	typeform.com	Amazon Web Services	Ja (USA)	Hosting	Nein
bcookie	3rd-Party (dauerhaft)	365	linkedin.com	LinkedIn	Ja (USA)	Funktional	Nein
breakdance_last_session_id	1st-Party (Session)	0	riffbird.com	Unbekannt		Unbekannt	Nein
breakdance_session_count	1st-Party (Session)	0	riffbird.com	Unbekannt		Unbekannt	Nein
breakdance_view_count	1st-Party (Session)	0	riffbird.com	Unbekannt		Unbekannt	Nein
bscookie	3rd-Party (dauerhaft)	365	linkedin.com	LinkedIn	Ja (USA)	Funktional	Nein
IDE	3rd-Party (dauerhaft)	390	doubleclick.net	DoubleClick		Werbung	Ja
legalweb_cookie_settings	1st-Party (dauerhaft)	400	riffbird.com	legalweb.io		Consent Management	
li_gc	3rd-Party (dauerhaft)	180	linkedin.com	LinkedIn Widgets	Ja (USA)	Soziale Medien	Nein
lidc	3rd-Party (dauerhaft)	1	linkedin.com	LinkedIn	Ja (USA)	Funktional	Nein
ln_or	1st-Party (dauerhaft)	1	riffbird.com	LinkedIn Analytics	Ja (USA)	Analytics	Nein

Name	Typ	Speicherdauer (Tage)	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt
m Auf Unterseite gefunden (24.04.23 17:41)	3rd-Party (dauerhaft)	400	stripe.com	Stripe	Ja (USA)	Interaktion	Nein
MUID	3rd-Party (dauerhaft)	390	bing.com	Bing Ads		Werbung	Nein
PHPSESSID	1st-Party (Session)	0	riffbird.com	Webserver		Funktional	Nein
test_cookie Auf Unterseite gefunden (24.04.23 17:41)	3rd-Party (dauerhaft)	1	doubleclick.net	DoubleClick		Werbung	Nein
tf_respondent_cc Auf Unterseite gefunden (24.04.23 17:41)	3rd-Party (dauerhaft)	183	typeform.com	Typeform		Interaktion	Nein
tt_appInfo	Session Storage	0		TikTok	Ja (China)	Soziale Medien	Nein
tt_pageId	Session Storage	0		TikTok	Ja (China)	Soziale Medien	Nein
tt_pixel_session_index	Session Storage	0		TikTok	Ja (China)	Soziale Medien	Nein
tt_sessionId	Session Storage	0		TikTok	Ja (China)	Soziale Medien	Nein
UserMatchHistory	3rd-Party (dauerhaft)	30	linkedin.com	LinkedIn	Ja (USA)	Funktional	Nein

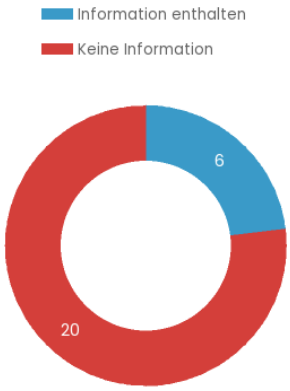
Externe Dienste



Verwendung



Einwilligung zum Laden



Information in Datenschutzerklärung

Externe Dienste Übersicht

Name	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt	Information in Datenschutzerklärung
Airbrake Auf Unterseite gefunden (24.04.23 17:41)	airbrake.io	Airbrake	Ja (USA)	Werbung	Nein	Nein
Amazon CloudFront Auf Unterseite gefunden (24.04.23 17:41)	cloudfront.net	Amazon	Ja (USA)	Web-Speicher	Nein	Nein
Bing Ads Auf allen Seiten gefunden (24.04.23 17:41)	bing.com	Microsoft		Werbung	Nein	Nein
Braze Auf Unterseite gefunden (24.04.23 17:41)	appboycdn.com	Braze	Ja (USA)	Analytics	Nein	Nein
Calendly Auf Unterseite gefunden (24.04.23 17:41)	calendly.com	Calendly LLC	Ja (USA)	Externer Inhalt	Nein	Nein

Name	Domain	Quelle	Datentransfer	Zweck	Einwilligung erteilt	Information in Datenschutzerklärung
DoubleClick Auf allen Seiten gefunden (24.04.23 17:41)	doubleclick.net	Google		Werbung	Nein	Nein
Facebook Pixel Auf allen Seiten gefunden (24.04.23 17:41)	connect.facebook.net/*/fbevents.js	Facebook	Ja (USA)	Werbung	Nein	Ja
Google AdServices Auf Unterseite gefunden (24.04.23 17:41)	googleadservices.com	Google		Werbung	Nein	Ja
Google AdWords Conversion Auf allen Seiten gefunden (24.04.23 17:41)	www.google.xxx/pagead	Google		Werbung	Nein	Ja
Google Analytics Auf allen Seiten gefunden (24.04.23 17:41)	google-analytics.com	Google		Interaktion	Nein	Ja
Google Recaptcha Auf Unterseite gefunden (24.04.23 17:41)	recaptcha.net	Google		Interaktion	Nein	Nein
Google Tag Manager Auf allen Seiten gefunden (24.04.23 17:41)	googletagmanager.com	Google		Funktional	Nein	Ja
Heap Auf Unterseite gefunden (24.04.23 17:41)	heapanalytics.com	Heap		Analytics	Nein	Nein
Hotjar Auf 3 Unterseiten gefunden (24.04.23 17:41)	hotjar.com	Hotjar		Analytics	Nein	Nein
legalweb.io	riffbird.com (*Lokaler Server*)	legal web GmbH		Consent Management		Ja
LinkedIn Ads Auf allen Seiten gefunden (24.04.23 17:41)	ads.linkedin.com	Microsoft	Ja (USA)	Werbung	Nein	Nein
LinkedIn Analytics Auf allen Seiten gefunden (24.04.23 17:41)	snap.licdn.com	Microsoft	Ja (USA)	Analytics	Nein	Nein
Oribi (LinkedIn) Auf allen Seiten gefunden (24.04.23 17:41)	oribi.io	Microsoft	Ja (USA)	Analytics	Nein	Nein
pendo Auf Unterseite gefunden (24.04.23 17:41)	pendo.io			Analytics	Nein	Nein
RudderStack Auf Unterseite gefunden (24.04.23 17:41)	rudderlabs.com	RudderStack Inc.	Ja (USA)	Analytics	Nein	Nein
Segment Auf Unterseite gefunden (24.04.23 17:41)	segment.io	Segment	Ja (USA)	Analytics	Nein	Nein
Stripe Auf Unterseite gefunden (24.04.23 17:41)	stripe.com	Stripe, Inc.	Ja (USA)	Interaktion	Nein	Nein
TikTok Auf allen Seiten gefunden (24.04.23 17:41)	tiktok.com	Beijing Bytedance Technology Ltd.	Ja (China)	Soziale Medien	Nein	Nein
Typeform Auf Unterseite gefunden (24.04.23 17:41)	typeform.com	Typeform		Interaktion	Nein	Nein
Usabilla Auf Unterseite gefunden (24.04.23 17:41)	usabilla.com	Usabilla		Interaktion	Nein	Nein
Vimeo Auf der Startseite gefunden (24.04.23 17:41)	vimeo.com	Vimeo	Ja (USA)	Audio/Video-Player	Nein	Nein

TLS/SSL-Verschlüsselung und Sicherheit des Webservers

Das Zertifikat enthält korrekte und vollständige Informationen [1]

✅ Das Zertifikat ist zeitlich gültig bis 08.07.2023
✅ Das Zertifikat wird akzeptiert auf allen gängigen Plattformen (Apple, Android, Oracle/Java, Microsoft/Windows, Mozilla/Firefox) [2]
✅ Der Server ist geschützt gegen die verbreitetsten TLS/SSL-Angriffe [3]
✅ Der Webserver akzeptiert keine veralteten und unsicheren TLS/SSL-Protokolle. [4]
✅ Die aktuellen Protokolle TLS 1.2 bzw. TLS 1.3 werden akzeptiert [5]
⚠ Der Webserver setzt zwar HTTP-Header für Content-Security-Policy, diese ist aber nicht ausreichend sicher konfiguriert [6]
✅ Für den Webserver ist HTTP Strict Transport Security ausreichend sicher konfiguriert [7]
✅ Für den Webserver sind Umleitungen von HTTP zu HTTPS korrekt konfiguriert [8]
⚠ Der Webserver setzt keine Header für eine Referrer-Policy [9]
✅ Der Webserver setzt einen *X-Content-Type-Options*-Header [10]
✅ Der Webserver nutzt eine Content-Security-Policy für *X-Frame-Options* [11]
Zur Ermittlung der Sicherheit des Webservers verwenden wir Mozilla Observatory, für das komplette Scan-Ergebnis klicken Sie bitte hier.

Erläuterungen und Handlungsempfehlungen

[1] Wir untersuchen das TLS/SSL-Zertifikat darauf, ob der Server-Name im Zertifikat mit dem tatsächlichen Servernamen übereinstimmt, und ob das Zertifikat von einer vertrauenswürdigen Quelle stammt. Wenn eins von beiden nicht gegeben ist, zeigt ein Web-Browser normalerweise an, dass die Verbindung nicht sicher ist, weil in diesen Fällen sog. "Man-in-the-middle-Angriffe" möglich sind. Außerdem prüfen wir, ob die "Intermediate-Zertifikate" auf dem Server enthalten sind, die die Vertrauenswürdigkeit des Ausstellers nachweisen. Wenn diese fehlen, dann zeigen ältere Web-Browser möglicherweise Fehler an. Die Prüfungen zeigten keine Probleme.

[2] Die Zertifizierungsstelle, über die das Zertifikat des Webservers erworben wurden, muss von den großen Plattformen (Apple, Android, Oracle/Java, Microsoft/Windows, Mozilla/Firefox) als vertrauenswürdig eingestuft und in deren "Trust Store" aufgenommen worden sein. Wenn das nicht der Fall ist, dann stufen die Geräte dieser Plattformen das Zertifikat als nicht gültig ein. Im Fall dieses Webservers wird das Zertifikat von allen Plattformen als vertrauenswürdig eingestuft.

[3] Wir untersuchen den Server auf die Schwachstellen "Heartbleed", "CRIME" und "Downgrade". Alle drei stehen in Zusammenhang mit veralteter Systemsoftware oder dem Akzeptieren veralteter Verschlüsselungsprotokolle. Wir konnten bei dem Server diese Schwachstellen nicht feststellen.

[4] Veraltete TLS/SSL-Protokolle bieten keine sichere Verschlüsselung mehr, so dass Daten für Angreifer sichtbar sein können. Insbesondere die sehr alten Protokolle SSL 2.0 und SSL 3.0 sollten auf keinen Fall mehr eingesetzt werden, aber auch TLS 1.0 und TLS 1.1 sind nicht mehr sicher genug. Der Webserver ist korrekt konfiguriert und akzeptiert diese Protokolle nicht.

[5] Der Webserver sollte für ausreichende Sicherheit die neuen TLS/SSL-Protokolle TLS 1.3 und ggfs. TLS 1.2 unterstützen. Der Webserver ist korrekt konfiguriert und unterstützt diese.

[6] Die Content Security Policy (CSP) ist nicht ausreichend restriktiv. Sie enthält die Direktiven *unsafe-eval* oder *data* innerhalb der Direktive *script-src*, zu weit gefasste Einschränkungen wie *https*: innerhalb der Direktive *object-src*, oder sie schränkt die Quellen für *object-src* or *script-src* nicht ein.
Hintergrund: Ein Content Security Policy (CSP)-HTTP-Header ist eine von mehreren möglichen Maßnahmen, um Websites gegen Angriffe durch Cross-Site-Scripting (XSS) zu schützen. Beim XSS injizieren Angreifer Javascript-Code in eine Seite (bspw. indem sie einen Blog-Kommentar schreiben, der Javascript-Code enthält). Wenn andere Besucher die Seite öffnen, wird das Javascript ausgeführt, was eine Vielzahl von Angriffsmöglichkeiten bietet, etwa das Auslesen und Versenden von Passwörtern während der Eingabe. Ein CSP-Header kann das verhindern, indem er das Ausführen von sog. "Inline-" Javascript grundsätzlich unterbindet, und nur Javascript von bestimmten Servern erlaubt, bzw. grundsätzlich das Laden von Ressourcen auf ausgewählte Server einschränkt. Bei der Einführung einer CSP muss möglicherweise der Anwendungscode angepasst werden, so ist u.A. der Einsatz des Google Tag Managers nicht mehr ohne Weiteres möglich. Die Herausforderungen bei der Einführung einer CSP beschreiben dieser und dieser Artikel.

[7] Der Parameter *max-age*, der angibt, wie lange per HSTS verschlüsselte Verbindungen erzwungen werde sollen, ist korrekt auf

mehr als 6 Monate konfiguriert. Ein Wert von ein bis zwei Jahren ist optimal.
Hintergrund: HTTP Strict Transport Security (HSTS) ist ein Sicherheitsmechanismus, bei dem der Server einem Browser mitteilt, dass für eine bestimmte Zeit ausschließlich verschlüsselte Verbindungen verwendet werden dürfen. Bei so genannten Man-in-the-Middle Angriffen versucht ein Angreifer, den Aufbau einer verschlüsselten Verbindung zu verhindern, ohne dass der Benutzer etwas davon merkt. Der Angreifer kann dann unbemerkt alle übermittelten Daten mitlesen. Mit HSTS soll bereits am Beginn der Verbindung eine HTTPS Verschlüsselung erzwungen und damit die Gefahr solcher Angriffe minimiert werden. Ein Webserver sollte für optimalen Schutz immer HSTS in Verbindung mit einer HTTPS-Umleitung verwenden.

[8] Alle Aufrufe zu unverschlüsselten URLs werden so umgeleitet, dass der Aufruf verschlüsselt erfolgt.
Hintergrund: Der Server sollte so konfiguriert sein, dass unverschlüsselte Aufrufe sofort auf die entsprechende HTTPS-URL umgeleitet werden. Andernfalls könnte ein Benutzer bspw. verleitet werden, Formulardaten unverschlüsselt zu übertragen. Sobald die Umleitung stattgefunden hat, sollte der Browser per HSTS angewiesen werden, in Zukunft nur noch die verschlüsselte Verbindung zu benutzen. Dabei sollte die Umleitung nicht zu einer anderen Domain/Host führen (das würde HSTS aushebeln), sondern unmittelbar zur gleichen URL, aber mit HTTPS.

[9] Es ist zwar kein sehr großes Sicherheitsrisiko, keine Referrer-Policy festzulegen, aber auch nicht ideal. Die Browser verwenden dann eine eigene Policy, die möglicherweise etwas unsicherer ist als die empfohlene, das Verhalten ist aber auf jeden Fall unvorhersehbar.
Hintergrund: Der Referrer ist ein HTTP-Header, der bei einem Aufruf (auch an externe Ressourcen) die vorherige bzw. die aktuelle URL mitteilt. Da die URL sensitive Informationen enthalten kann, ist dies ein potentielles Sicherheitsrisiko. Eine Referrer-Policy legt deswegen fest, bei welchen Aufrufen dieser Header welchen Teil der URL enthält (oder leer ist). Als Best Practice gilt es, dass der Header die Policy *strict-origin-when-cross-origin* festlegt, dabei enthält dann der Referrer nur den eigenen Servernamen, wenn ein Aufruf an fremde Server stattfindet. Detaillierte Hinweise finden Sie hier.

[10] Es wurde ein *X-Content-Type-Options*-Header mit dem korrekten Wert *nosniff* gefunden.
Hintergrund: Der *X-Content-Type-Options*-Header mit dem Inhalt *nosniff* dient dazu, Cross-Site-Scripting-Attacken abzuwehren. Diese können auftreten, weil manche Browser (bspw. Internet Explorer) ein sog. "Content-Sniffing" durchführen. Dabei versucht der Browser selber herauszufinden, welchen Inhaltstyp eine Ressource hat, wenn der Content-Type-Header fehlt. Das ermöglicht es einem Angreifer, Javascript in eine Seite zu injizieren, etwa wenn er die Möglichkeit hat, selber Inhalte in ein Forum o.Ä. hochzuladen. Wenn andere Besucher die Seite öffnen, wird das Javascript ausgeführt, was eine Vielzahl von Angriffsmöglichkeiten bietet, etwa das Auslesen und Versenden von Passwörtern während der Eingabe. Es ist deshalb sinnvoll, diesen Header zu setzen.

[11] Es gilt als Best Practice, den *X-Frame-Options*-Header mit einem sicheren Wert wie *SAMEORIGIN* oder *DENY* zusammen mit der *frame-ancestors*-Direktive des *Content-Security-Policy*-Headers einzusetzen.
Hintergrund: Der *X-Frame-Options*-Header legt fest, ob die Website über ein iFrame auf einer anderen Website eingebettet werden kann. Letzteres kann ein Sicherheitsrisiko durch Clickjacking darstellen. Dabei werden Teile der eingebetteten Website durch Elemente des Angreifers überlagert, etwa um einem Besucher dazu zu bringen, auf scheinbar harmlose - aber tatsächlich gefährliche - Links zu klicken. Mit Hilfe des Headers kann derartiges Einbetten unterbunden werden. Alternativ ist der Content-Security-Policy-Header ebenfalls geeignet, ein Einbetten zu verhindern.