'Mixed Content' und Web-Security am Beispiel Firefox

'Mixed Content' und Web-Security am Beispiel Firefox

TL;DR "http"-Ressourcen innerhalb von "https://"-Seiten funktionieren nicht mehr (ab Firefox 127, Juni 2024) – gleiches gilt für Chrome und Derivate – Safari zeigt (noch) alle 'Daten' an.

„Version 127.0, first offered to Release channel users on June 11, 2024“

Abb. Firefox/ab Juni 2024, v127.0

"Mixed content" bezieht sich auf eine Situation, in der eine Webseite, die über eine sichere HTTP**S**-Verbindung bereitgestellt wird, auch Ressourcen wie Bilder, Videos, Stylesheets oder Skripte von einer unsicheren HTTP-Verbindung lädt.

"Mixed **Active** Content" (auch bekannt als Mixed Scripting) bezieht sich auf Inhalte, die auf den Inhalt des Dokuments zugreifen und diesen möglicherweise manipulieren oder Daten senden und empfangen können, z. B. Skripte, Stylesheets, Iframes und andere codebasierte Ressourcen. "Mixed **Active** Content" stellt ein **erhebliches Sicherheitsrisiko** bzgl. Vertraulichkeit und Integrität der Webseite dar. Angreifer könnten sensible Informationen auslesen.

„Mixed Passive Content“ (gemischter passiver Inhalt, auch bekannt als „Mixed Display Content“) bezieht sich auf Inhalte, die **nicht mit dem Inhalt** des Dokuments interagieren (zB. Daten senden/ empfangen). Beispiele: Bilder, Audiodateien, Videos.

Moderne Webbrowser **blockieren** in der Regel standardmäßig **gemischte aktive** Inhalte und zeigen möglicherweise **Warnungen** an oder blockieren auch **gemischte passive** Inhalte. Um Probleme mit gemischten Inhalten zu vermeiden, müssen alle Ressourcen auf einer Webseite über HTTPS bereitgestellt werden (Port 443), so die Seite selbst über HTTPS bereitgestellt wird.

Webseiten, die ausschließlich per „http://“-Protokoll Daten bereitstellen (non secure), sind von den Änderungen **nicht** betroffen.

*"Mixed content" refers to a situation where a web page served over a secure HTTP**S** connection also loads resources, such as images, stylesheets, or scripts, from an insecure HTTP connection.*

*Mixed **Active** Content (also known as Mixed Scripting): This refers to content that can access and potentially manipulate the document's content or send and receive data, such as scripts, stylesheets, iframes, and other code-based resources. Mixed active content poses a significant **security** risk, as it can compromise the confidentiality and integrity of a web page and expose sensitive information to attackers.*

*Mixed **Passive** Content (also known as Mixed Display Content): This refers to content that cannot interact with the document's content or send or receive data. Examples include images, audio files, and videos.*

*Modern web browsers typically **block mixed active** content by default and may display **warnings** or block **mixed passive** content as well. To avoid mixed content issues, it's recommended that all resources on a web page be served over HTTPS when the page itself is served over HTTP**S**.*

Vorweg: Darum sollte die Firefox-Standardeinstellung für **aktive** Inhalte **auf „true“ bleiben**:

„security.mixed_content.block_**active**_content → „true“

Re-Enable 'passive', not 'active'

Allgemein: Es wird **nun nicht mehr zwischen** "Mixed **active** content" (zB. ein Script, dass per "http" geladen würde und somit blockiert wird) und

"Mixed **passive**/display content" (zB. ein Bild das via "http" per <img src="htt**p**://example.com/img1.png"> eingebunden wurde) unterschieden.

Die Mixed-Content Regeln wurden **abgeschafft**, sprich das Einbinden von "htt**p**"-Ressourcen auf einer Webseite, die über http**s**:// aufgerufen wurde ist nicht mehr möglich.

Beispiel: Daten die auf einer "http**s**://"-Seite via "http" eingebunden werden, werden nicht mehr angezeigt

https://moodle.ufg.at/test/

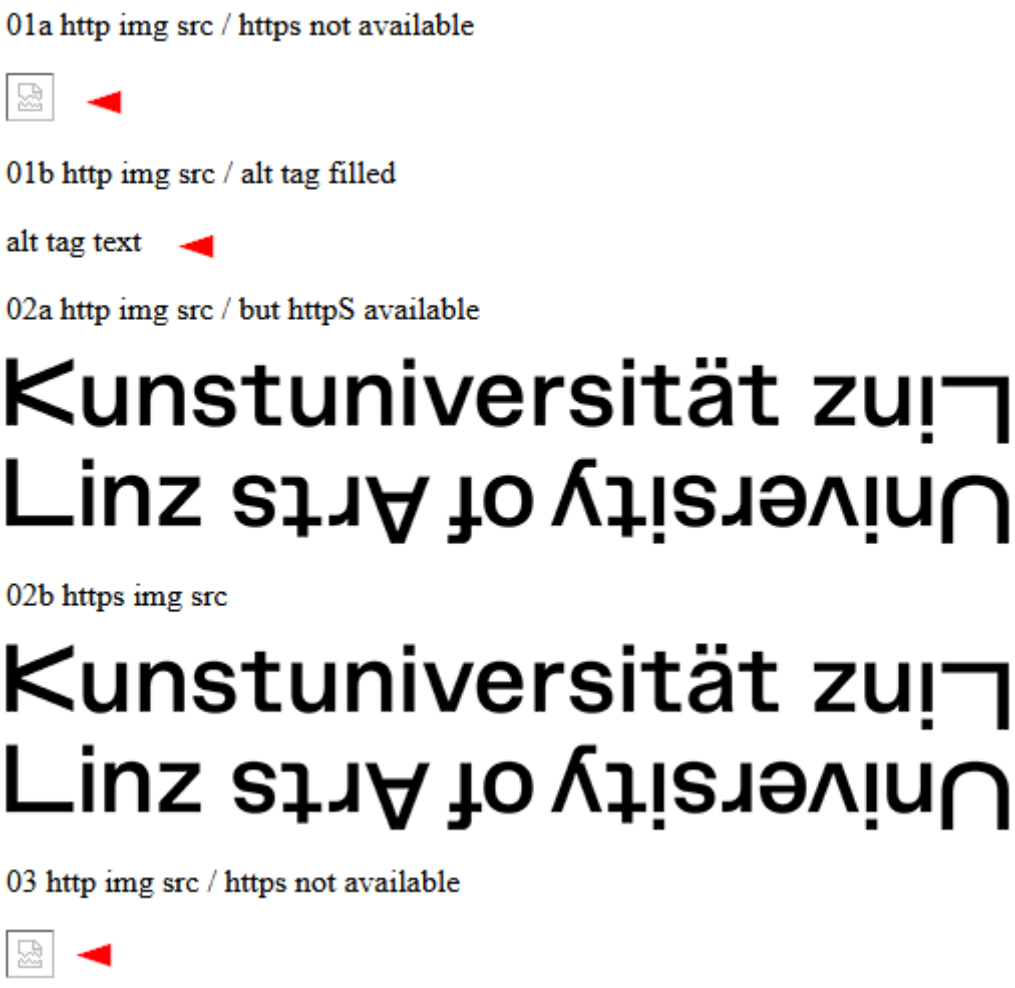


Abb. Einbindung von https- und http-Ressourcen auf einer per „http“ aufgerufenen Webseite

Beispiel-Code:

```
<p>01a http img src / https not available</p>
<p><img src="http://www.dma.ufg.ac.at/assets/7068/intern/h_fonts.gif"></p>
<p>01b http img src / alt tag filled</p>
<p><img src="http://www.dma.ufg.ac.at/assets/7068/intern/h_fonts.gif"
alt="alt tag text"></p>
<p>02a http img src / but httpS available</p>
<p><img src="http://www.kunstuni-
linz.at/assets/img/KunstUniversitaetLinzLogo.png"</p>
<p>02b https img src</p>
<p><img src="https://www.kunstuni-
linz.at/assets/img/KunstUniversitaetLinzLogo.png"</p>
<p>03 http img src / https not available</p>
<p><img
src="http://simon_bauer.public1.linz.at/www.plan9.at/simon_bauer_ambivalen
te-ambiente-1-6.png"</p>
```

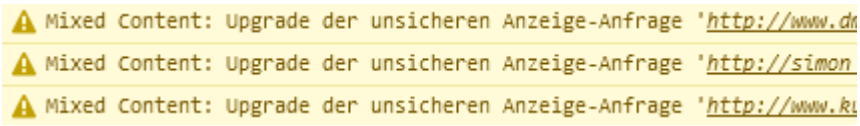
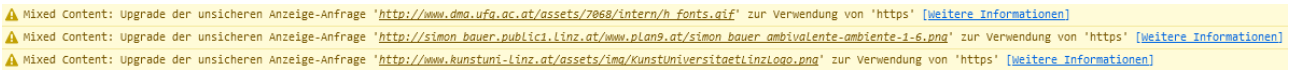


Abb. Firefox Web-Konsole (Shortcut: Strg-Shift-K oder F12)



Weitere Informationen: Web-Konsole:
https://firefox-source-docs.mozilla.org/devtools-user/web_console/

Beispiel „LMS Moodle“. Die Bilder wurden extern per „http://“ eingebunden.
Ein Bearbeiten der Seite ist schlecht möglich (das Setzen der Bildquelle auf https, statt http ist nötig).

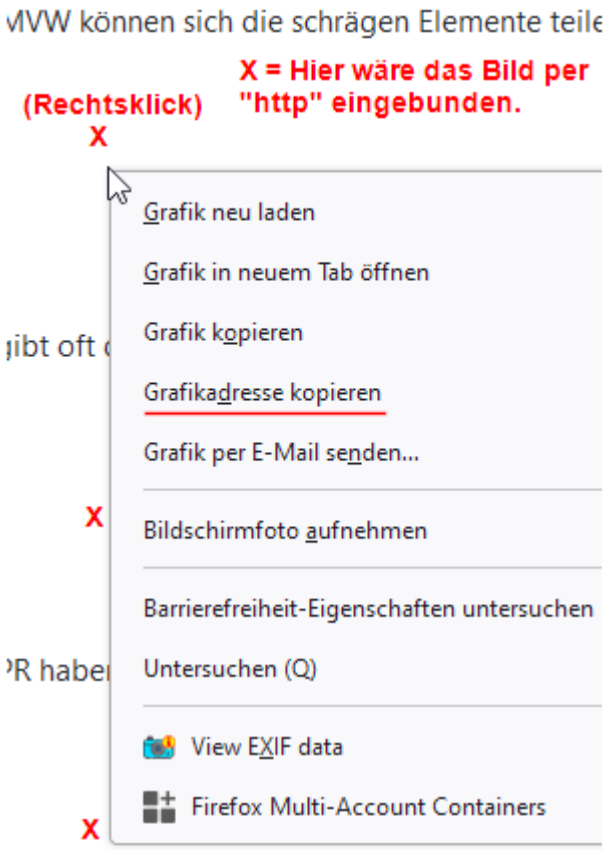


Abb. security.mixed_content.
upgrade_display_content.**image**
IST auf „TRUE “ gesetzt (Standard FF)

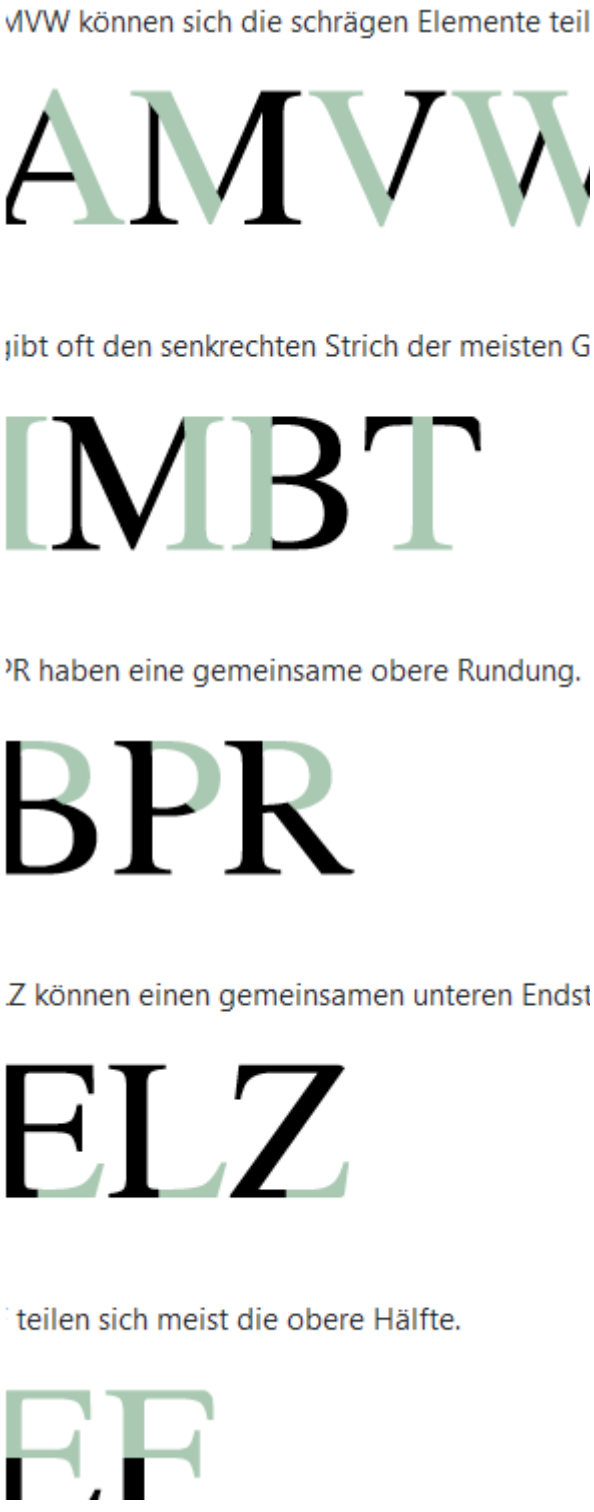


Abb. security.mixed_content.
upgrade_display_content.**image**
IST auf „FALSE“ gesetzt

Zum Energieverbrauch: Jedes Element wird nun ver- und entschlüsselt.
Dies wäre zB für Bilder, Videos etc. die offen auf Webseiten zu finden sind eigentlich nicht nötig.
Dazu kommen die "unnötigen" Versuche des Webbrowsers "doch noch" an das Material per „https“ zu kommen.

"TLS-Handshake mit <website ohne https> …"

(Dadurch wird momentan auch das „Fertigladen“ der Seite verzögert.)

„Starting with version 127, Firefox is going to automatically upgrade audio, video, and image subresources from HTTP to HTTPS."

https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content

https://web.archive.org/web/2/https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content

Weitere Informationen:

https://support.mozilla.org/en-US/kb/mixed-content-blocking-firefox
https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content#developer_console
https://w3c.github.io/webappsec-mixed-content/

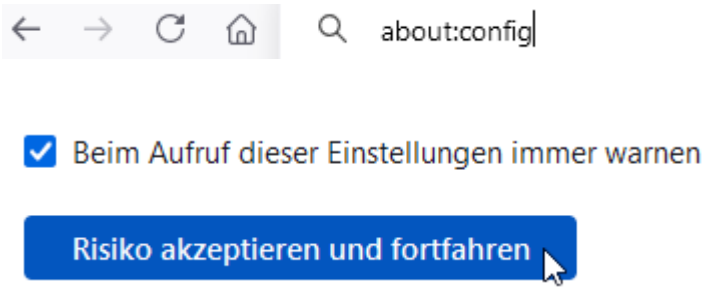
Anmerkung „fake resources“: *"There is a risk of introducing a security or privacy issue in a webpage by loading a resource that the developer did not intend. For example, suppose that a website includes an innocuous image from htt**p**://www.example.com/image.jpg, and for some reason https://www.example.com/**image.jpg redirects** to a tracking site. The browser will now have introduced a privacy issue without the developer's or user's explicit consent. However, these cases are expected to be exceedingly rare."*

Möchte man diese Bilder doch wieder sehen:

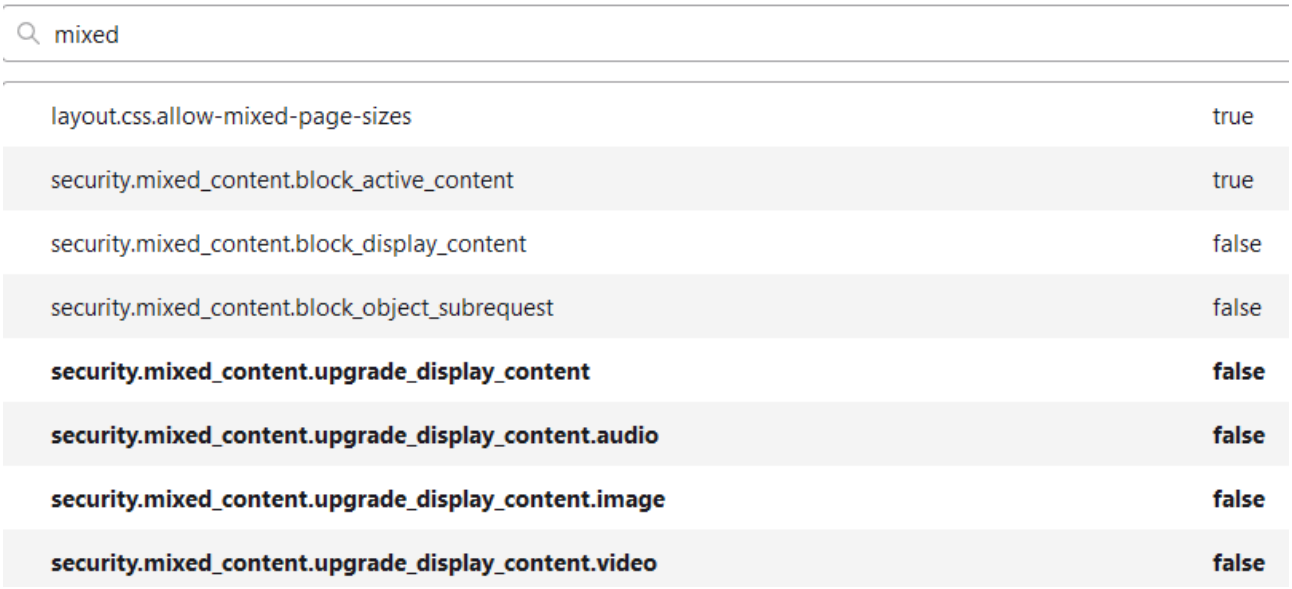
„**Enabling mixed content in your browser**“

https://experienceleague.adobe.com/en/docs/target/using/experiences/vec/troubleshoot-composer/mixed-content

Für Firefox ist in der URL-Leiste "about:config" einzugeben.



Gesucht wird nach dem Begriff „***mixed***“.
Werte werden durch einen Doppelklick auf die jeweilige Zeile geändert (hier ist nur der Wechsel „true“/„false“ nötig).



security.mixed_content.block_**active**_content	true (! *belassen*)
security.mixed_content.**block_display**_content	false (Standard)
security.mixed_content.block_object_subrequest	false
security.mixed_content.**upgrade_display**_content	**false**
security.mixed_content.**upgrade_display**_content.**audio**	**false**
security.mixed_content.**upgrade_display**_content.**image**	**false**
security.mixed_content.**upgrade_display**_content.**video**	**false**

Die Seite sieht nun wie folgt aus:

01a http img src / https not available

01b http img src / alt tag filled

02a http img src / but httpS available

02b https img src

03 http img src / https not available

Um NUR Bilder zuzulassen langt die Einstellung:
security.mixed_content.**upgrade_display**_content.**image** **false**

security.mixed_content.block_active_content	true
security.mixed_content.block_display_content	false
security.mixed_content.block_object_subrequest	false
security.mixed_content.upgrade_display_content	true
security.mixed_content.upgrade_display_content.audio	true
security.mixed_content.upgrade_display_content.image	**false**
security.mixed_content.upgrade_display_content.video	true

Weitere sicherheitsrelevante Themen

Unabhängig davon für "https" gilt:

CORS Regeln https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS

https://cors-test.codehappy.dev/

Beispiel:
https://cors-test.codehappy.dev/?url=https%3A%2F%2Fwww.moodle.ufg.at%2Ftest%2F&origin=http%3A%2F%2Fwww.dma.ufg.ac.at&method=get

Header (Webserver)

HTTP/2301
date: Tue, 18 Jun 2024 21:48:33 GMT
server: Apache
location: https://moodle.ufg.at/test/
content-type: text/html; charset=iso-8859-1
access-control-allow-origin: *
access-control-allow-headers: Origin, X-Requested-With, Content-Type, Accept, Authorization, JSNLog-RequestId, activityId, applicationId, applicationUserId, channelId, senderId, sessionId
access-control-max-age: 3628800
access-control-allow-methods: GET, DELETE, OPTIONS, POST, PUT

HSTS

HTTP Strict-Transport-Security

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

Weitere Informationen: Topic "HTTP security"
https://developer.mozilla.org/en-US/docs/Web/HTTP

Checking HTTP Headers

https://www.w3.org/International/questions/qa-headers-charset.en

https://tools.keycdn.com/curl

HTTP/2200
date: Tue, 18 Jun 2024 21:18:28 GMT
server: Apache
last-modified: Tue, 18 Jun 2024 10:50:34 GMT
etag: "192-64b27d9f11a68"
accept-ranges: bytes
content-length: 658
vary: Accept-Encoding
content-type: text/html

https://www.rexswain.com/httpview.html

CSP – Content Security Policy

CSP: upgrade-insecure-requests (Meta-Tags/Header)

`<meta http-equiv="Content-Security-Policy" content="upgrade-insecure-requests" />`

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Upgrade-Insecure-Requests

CSP via Header

HTTP-Header: `Content-Security-Policy: upgrade-insecure-requests;`

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/upgrade-insecure-requests

Weitere Informationen:
https://w3c.github.io/webappsec-upgrade-insecure-requests/#delivery

https://en.wikipedia.org/wiki/Content_Security_Policy
https://de.wikipedia.org/wiki/Content_Security_Policy

Übersicht Content-Security-Policy
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Siehe auch:

"Permissions Policy provides mechanisms for web developers to explicitly declare what functionality can and cannot be used on a website."

https://developer.mozilla.org/en-US/docs/Web/HTTP/Permissions_Policy

Firefox-Einstellungen bezüglich Webseiten http/https:

„**Nur-HTTPS-Modus**“ erzwingt "https"-Zugriff auf die Webseite (HTTPS-Only Mode in Firefox)

https://support.mozilla.org/en-US/kb/https-only-prefs
https://support.mozilla.org/de/kb/nur-https-modus-in-firefox

All in all. Etwas absurd werden die „html“-Specs schon. Alleine das „Bild-/Webseitenvorladen“, weil man unter Umständen einem Link auf der Seite folgt ist Bandbreiten- und Stromverschwendung durch die Folgeseite.

Nun lässt sich auch „DNS“ prefetchen – no comment.

„We completed work to optimize and enable DNS prefetching for HTTPS documents via the rel="dns-prefetch" link hint. This standard allows web developers to specify domain names for important assets that should be resolved preemptively.“

Der eingebaute PDF-Editor mag nützlich sein:
https://www.mozilla.org/en-US/firefox/features/pdf-editor

Alle Release-Notes von **Firefox 127** sind unter:
https://www.mozilla.org/en-US/firefox/127.0/releasenote zu finden.

Und hier befindet sich auch der „mixed“ Eintrag – „try“ klang kurz noch gut. „Firefox will now automatically **TRY to upgrade <img>, <audio>, and <video>** elements **from HTTP to HTTPS** if they are embedded **within an HTTPS page**. If these so-called mixed content elements **do not support HTTPS**, they will **NO longer load.**“

Wobei „It is now possible to close all duplicate tabs in a window with the Close duplicate tabs command available from the List all tabs widget in the tab bar or a tab context menu.“ doch hilfreich sein kann, so eine „Tab“-Recherchier-Orgie wieder etwas aufgeräumter sein soll.

Firefox Download:
https://www.mozilla.org/firefox/download/

oT: Firefox-Userin arbeitet mit 7500 geöffneten Tabs – und verliert alle auf einmal (*vorübergehend*) (05/2024)
https://www.spiegel.de/netzwelt/web/firefox-nutzerin-verliert-7500-geoeffnete-tabs-a-d72b9ff2-7986-457f-b73f-0cdbd3882718