Benutzerdokumentation auf dem EDPB Website Auditing Tool



Versionshistorie

|  |  |  |
| --- | --- | --- |
| Version 1.3 | 12 06 2024 | Aktualisierte Dokumentation für Version 1.2.4 |
| Version 1.2 | 04 08 2023 | Hinzufügung von Installationsinformationen |
| Version 1.1 | 10 01 2023 | Hinzufügung des testssl Addendums |
| Version 1.0 | 09 12 2022 | Veröffentlichung der ersten Version |

Copyright © Europäischer Datenschutzausschuss (EDPB), 2022-2024

Lizenziert unter der EUPL-1.2

Inhaltsverzeichnis

[1 Installation 4](#_Toc169703656)

[1.1 Vom Code Europa EU 4](#_Toc169703657)

[1.1.1 MAC 4](#_Toc169703658)

[1.1.2 Fenster 4](#_Toc169703659)

[1.1.3 GNU/Linux mit Snap 4](#_Toc169703660)

[1.2 TLS-Evaluierung in Reports aufnehmen 4](#_Toc169703661)

[1.2.1 Verwendung von testssl.sh mit von Shell 5](#_Toc169703662)

[1.2.2 Verwendung von testssl.sh mit Docker 5](#_Toc169703663)

[1.2.3 Testsl.sh Konfiguration testen 6](#_Toc169703664)

[2 Wie das Tool funktioniert 8](#_Toc169703665)

[**Analyse** 8](#_Toc169703666)

[**Sitzungen** 9](#_Toc169703667)

[**Redakteur** 9](#_Toc169703668)

[**Andere** 9](#_Toc169703669)

[3 Bereitstellung neuer Analysen 9](#_Toc169703670)

[**Informationen zur Website** 10](#_Toc169703671)

[**Erstes oder neues Szenario** 10](#_Toc169703672)

[4 Der interne Browser 11](#_Toc169703673)

[4.1 Die Symbolleiste 11](#_Toc169703674)

[4.2 Das Logger-Panel 12](#_Toc169703675)

[4.3 Analysekarten 12](#_Toc169703676)

[4.4 Das Detail-Panel 13](#_Toc169703677)

[5 Treffen einer Entscheidung über Compliance/Nicht-Compliance 14](#_Toc169703678)

[5.1 Analyse 15](#_Toc169703679)

[5.2 Auswertung 15](#_Toc169703680)

[5.3 Selektoren 16](#_Toc169703681)

[6 Wissensbasis 16](#_Toc169703682)

[6.1 Anzeigen und Bearbeiten einer Wissensdatenbank 17](#_Toc169703683)

[6.1.1 Cookie-Einträge 17](#_Toc169703684)

[6.1.2 Lokale Speichereinträge 18](#_Toc169703685)

[6.2 Aktualisieren einer Datenbank 19](#_Toc169703686)

[6.3 Wissensdatenbanknutzung 19](#_Toc169703687)

[7 Berichte erstellen 20](#_Toc169703688)

[7.1 Berichtsschnittstelle 20](#_Toc169703689)

[7.1.1 Werkzeugleiste bearbeiten/exportieren 21](#_Toc169703690)

[7.1.2 Werkzeugleiste zur Informationsfilterung 21](#_Toc169703691)

[7.2 Bearbeiten neuer Vorlagen 22](#_Toc169703692)

[7.3 Hinzufügung eines neuen Anhangs 22](#_Toc169703693)

Das **EDPB-Website-Auditing-Tool** sammelt Beweise, klassifiziert Daten und erstellt Berichte über Tracker, die von Websites verwendet werden. Es soll verwendet werden, um Website-Inspektionen zu erleichtern.

Auf dieser Seite finden Sie Informationen zur Verwendung der EDSA-Prüfungstools. Klicken Sie auf [**Wie das Tool funktioniert**](http://localhost:4200/#/helps/how_the_tool_works), um eine erste Einführung zu erhalten.

Sie können jederzeit auf diese Seite zurückkehren, indem Sie auf den HELP -Button in der linken Seitenleiste klicken.

# Installation

## Vom Code Europa EU

Laden Sie die letzte Version der für Ihr Betriebssystem geeigneten Software an der folgenden Stelle herunter:

<https://code.europa.eu/edpb/website-auditing-tool/-/releases>

### MAC

* Laden Sie website-audit-XXXX-mac.dmg herunter
* Ziehen/Ablegen des Werkzeugs in Ihren Anwendungsordner

### Fenster

* Laden Sie Website-audit Setup-XXX-win.exe herunter
* Doppelklick zum Installieren

### GNU/Linux mit Snap

* Download Website-audit\_ XXXX \_amd64.deb
* Sie können es in einem Terminal installieren mit:

sudo dpkg -i./website-audit\_ XXXX \_amd64.deb

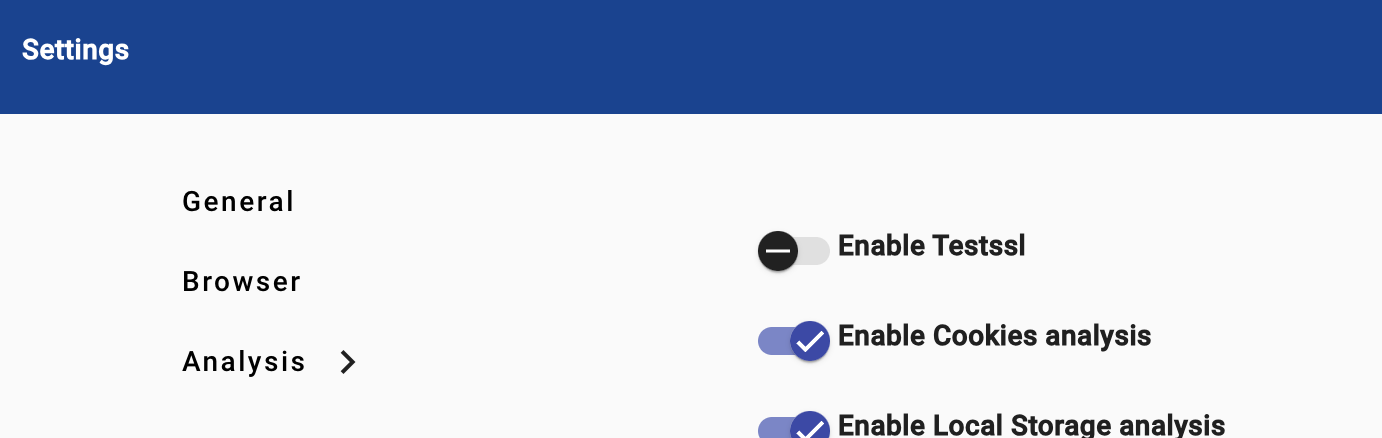
Dann können Sie die Anwendung im Terminal mit Website-Auditstarten

## TLS-Evaluierung in Reports aufnehmen

Die Software kann eine Auswertung der von der Website bereitgestellten TLS beinhalten. Dazu verwenden wir die Software testsl.sh, die [[1]](#footnote-1)die HTTPS-Konfiguration des Webservice-Hosts überprüft und erkannte Schwachstellen nach ihrem Schweregrad niedrig, mittel, hoch oder kritisch klassifiziert.

EDPB WAT ruft testsl.sh dynamisch [auf](https://testssl.sh/) und integriert die Ausgabe in das Tool. testssl.sh ist [[2]](#footnote-2) eine freie und quelloffene Software, die unter den Bedingungen von GPLv2 verfügbar ist.

Diese Auswertung kann in den Einstellungen über die Kategorie „Analyse“ aktiviert werden:



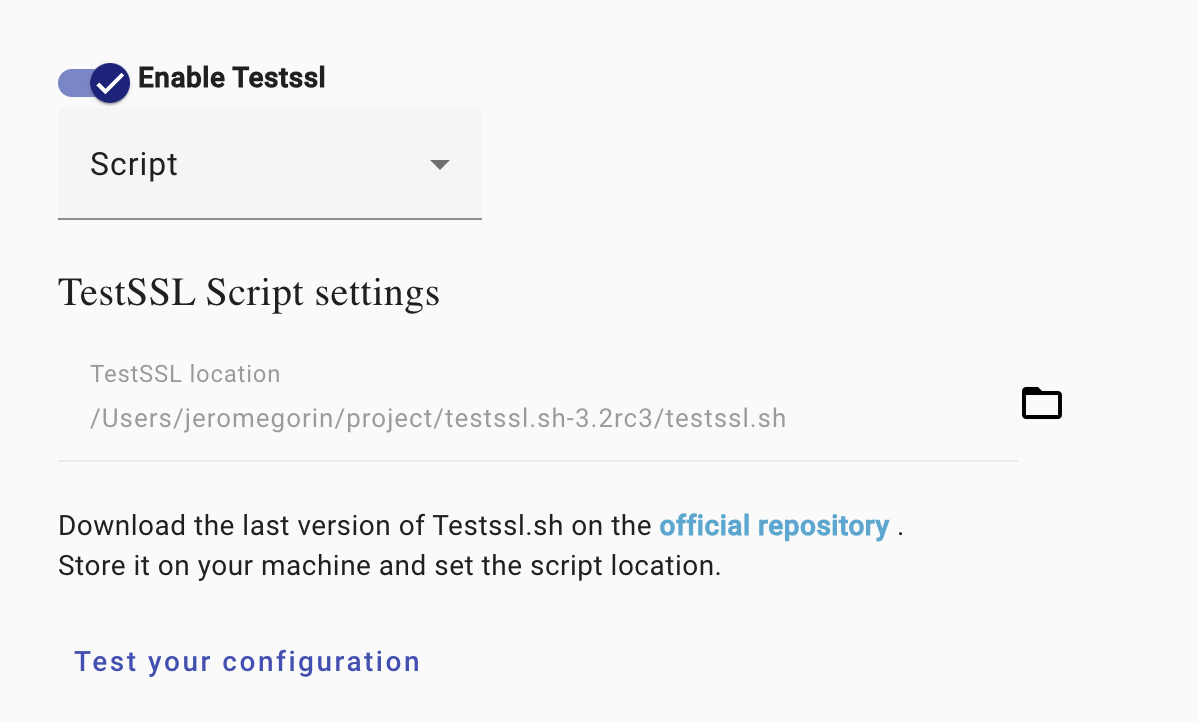
Die Verwendung von testssl.sh kann direkt oder über Docker (vorzugsweise unter Windows) mit dieser Einstellung erfolgen.

### Verwendung von testssl.sh mit von Shell

Das Skript testsl.sh sollte aus seinem offiziellen Repository abgerufen werden: <https://github.com/drwetter/testssl.sh>, entweder durch Klonen des Repository oder Herunterladen einer verpackten Version im Release-Bereich. Speichern Sie es auf Ihrem PC an Ihrem bevorzugten Standort.

Dieses Shell-Skript wird von einer Unix-Shell (Linux oder MacOS) ausgeführt. Es kann auch unter Windows mit der Funktion Windows Subsystem für Linux (WSL) durchgeführt werden.

Einmal gespeichert, geben Sie den Speicherort in den Einstellungen an.



### Verwendung von testssl.sh mit Docker

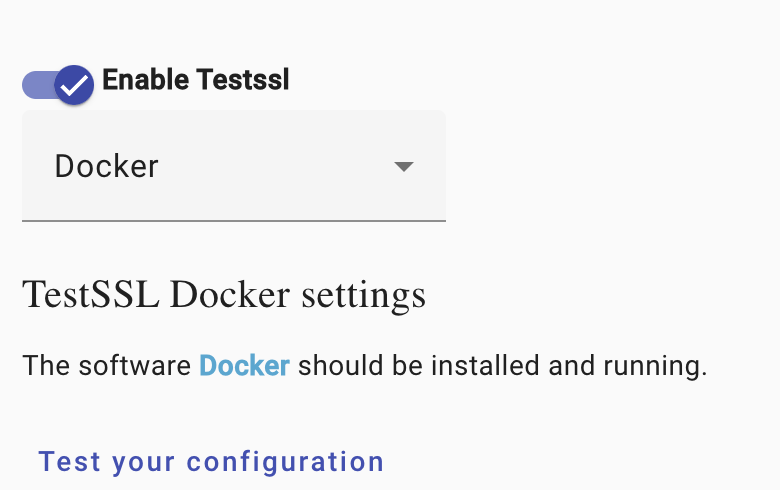
Docker bietet eine automatische Installation des Tools, eine bessere Portabilität des Skripts und reduziert mögliche Probleme mit Abhängigkeiten.

Stellen Sie sicher, dass Docker bereits installiert und auf Ihrem System aktiv ist. Wenn nicht, folgen Sie den Anweisungen, um Docker auf Ihrem System zu installieren:

* Windows: <https://docs.docker.com/desktop/install/windows-install/>
* Mac: <https://docs.docker.com/desktop/install/mac-install/>
* GNU/Linux: <https://docs.docker.com/desktop/install/linux-install/>

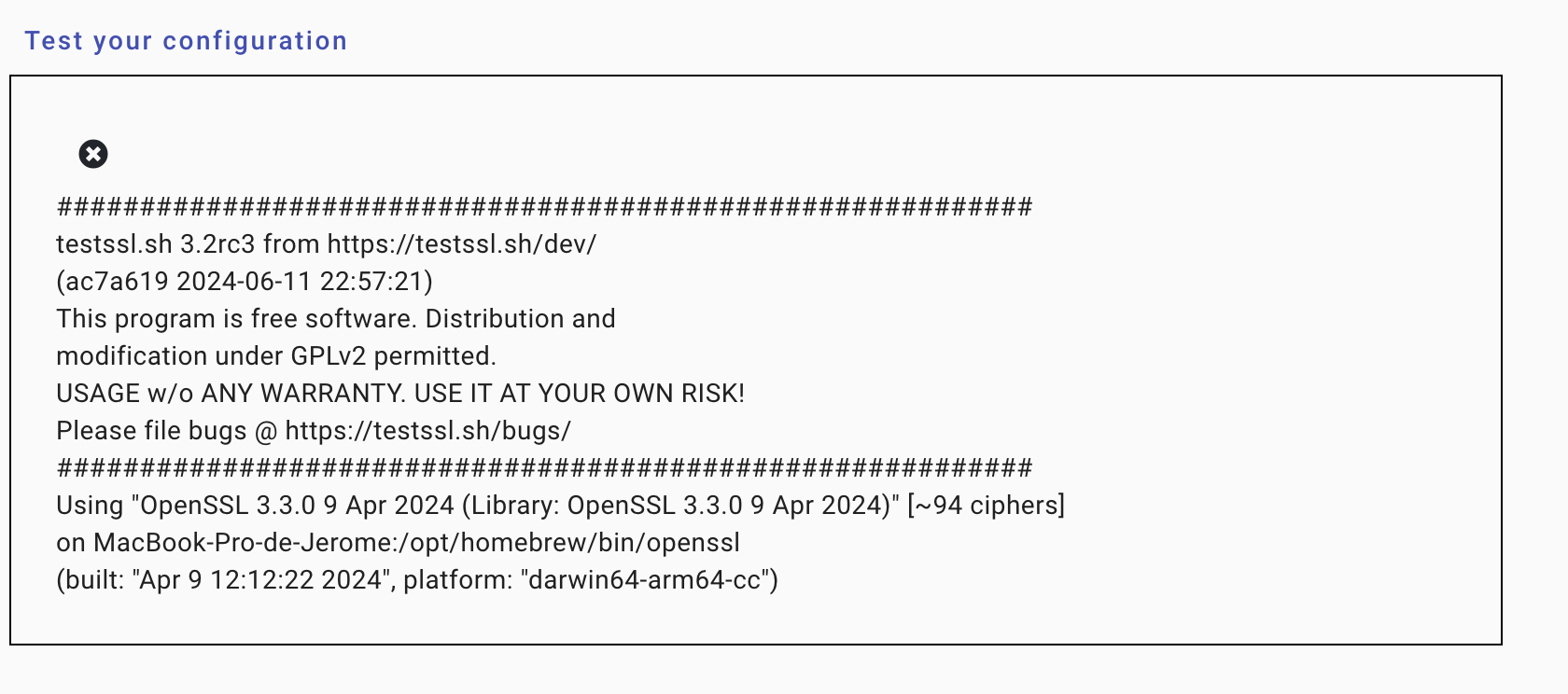
Öffnen Sie nach der Installation zum ersten Mal Docker (aus dem Systemfach oder aus dem Startmenü).

Dann können Sie testsl im WAT aktivieren, während Sie „Docker“ wählen.

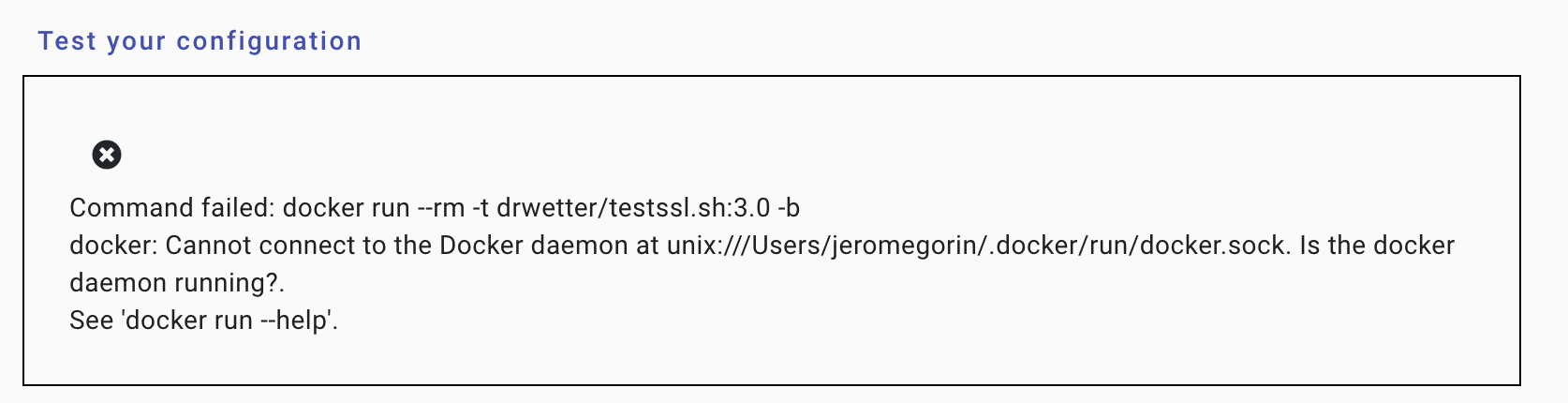


### Testsl.sh Konfiguration testen

Im Falle einer erfolgreichen Installation sollten Sie eine ähnliche Meldung wie die folgende erhalten, die die Version der verwendeten Software angibt:

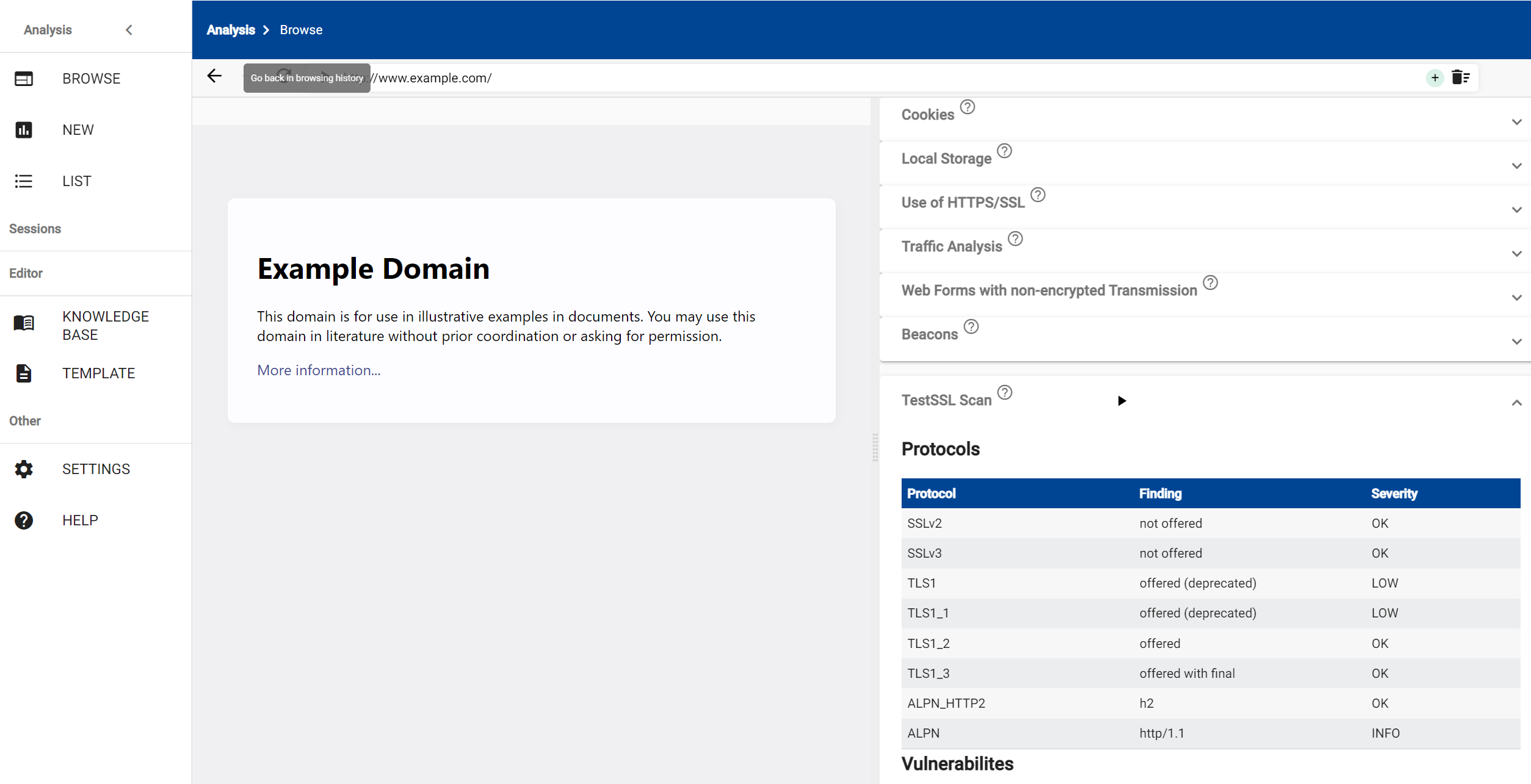


Andernfalls sollte die Meldung den Fehler während der Auswertung anzeigen.

**Fehlerbehebung:** Die folgende Meldung zeigt möglicherweise an, dass Sie versuchen, die Docker-Version zu verwenden, während Docker derzeit nicht auf Ihrem System ausgeführt wird. 

Abschließende Prüfung:

testsl.sh sollte nun direkt in der Karte „Testsl Scan“ im Durchsuchen des Tools verfügbar sein:



# Wie das Tool funktioniert

Das EDPB-Website-Auditing-Tool führt dem Chromium-Browser eine benutzerfreundliche Ebene ein, um sofort zu beurteilen, ob eine Website Informationen in einem Browser konform sammelt oder speichert (d. h.*durch*Unterrichtung und Einholung der Einwilligung des Nutzers, wenn dies erforderlich ist).

Alle Evidenzdaten können im Tool durch eine *Analyse* gespeichert werden, die verschiedene *Szenarien* sammelt und eine Interaktion (z.*B.* Einwilligung, Ablehnung usw.) mit der gegebenen Website darstellt.

Die Bewertung wird durch automatisierte Instrumente erleichtert, während die Entscheidung über die Einhaltung/Nichteinhaltung durch den Sachbearbeiter getroffen wird.

Die*Wissensdatenbank* kann dabei helfen, bekannte Tracker zu identifizieren.

Die*Vorlage* kann verwendet werden, um Berichte für ein bestimmtes Szenario zu personalisieren.

Über die linke Navigationsleiste können Sie auf alle diese Funktionen zugreifen:

|  |
| --- |
| **Analyse** |
| DURCHSTÖBERN | Verschaffen Sie sich einen schnellen Überblick über die im oder durch den Browser gespeicherten oder übertragenen personenbezogenen Daten. Die Ergebnisse werden nicht im Tool gespeichert. |
| NEU | Starten Sie eine neue Website-Analyse zum Sammeln von Beweisen. Nachweise werden im Tool für eine spätere Bewertung der Einhaltung der gesetzlichen Anforderungen gespeichert. |
| LISTE | Liste der Analysen, die im Tool mit ihrer Bewertung gespeichert sind. |
| **Sitzungen** |  |
| ANALYSE > SZENARIO | Aktuelle Sitzung an eine Analyse und ein Szenario in dieser Analyse angehängt. Nachweise können der referenzierten Analyse und dem Szenario beigefügt werden, bis diese Sitzung abgeschlossen ist. **Sobald diese Analyse und das Szenario abgeschlossen sind, können keine Beweise mehr beigefügt werden**. |
| **Redakteur** |  |
| WISSENSBASIS | Die Wissensdatenbank listet bekannte Tracker und deren entsprechende Zwecke auf. Diese Informationen können dynamisch während des Surfens oder der Bewertung der Einhaltung einer Website abgerufen werden.Die Wissensdatenbank kann mit neuen Informationen bearbeitet werden, die vom Sachbearbeiter gesammelt wurden. Es dient nur als Werkzeug, um die Analyse durch den Sachbearbeiter zu erleichtern. |
| SCHABLONE | Vorlagen werden für die Erstellung von Berichten verwendet, die auf spezifische Bedürfnisse zugeschnitten sind. |
| **Andere** |  |
| EINSTELLUNGEN | Passen Sie die angezeigten Informationen während des Surfens oder der Bewertung der Einhaltung eines bestimmten Szenarios an. |
| HILFE | Verweis auf die Dokumentation dieses Tools. |

Als erste Einführung, wie man eine Analyse durchführt, empfehlen wir Ihnen, sich den Abschnitt **Neue Analyse zur Verfügung zu stellen**.

# Bereitstellung neuer Analysen

Eine *Analyse* sammelt Informationen, die in einem Browser gespeichert wurden, wenn Sie Websites durch eine Reihe von *Szenarien* durchsuchen.

Es kann aus dem Abschnitt NEU oder über die Schaltfläche „+“ in der Symbolleiste des Abschnitts BROWSE initiiert werden.

Beide Symbole zeigen folgendes Formular:

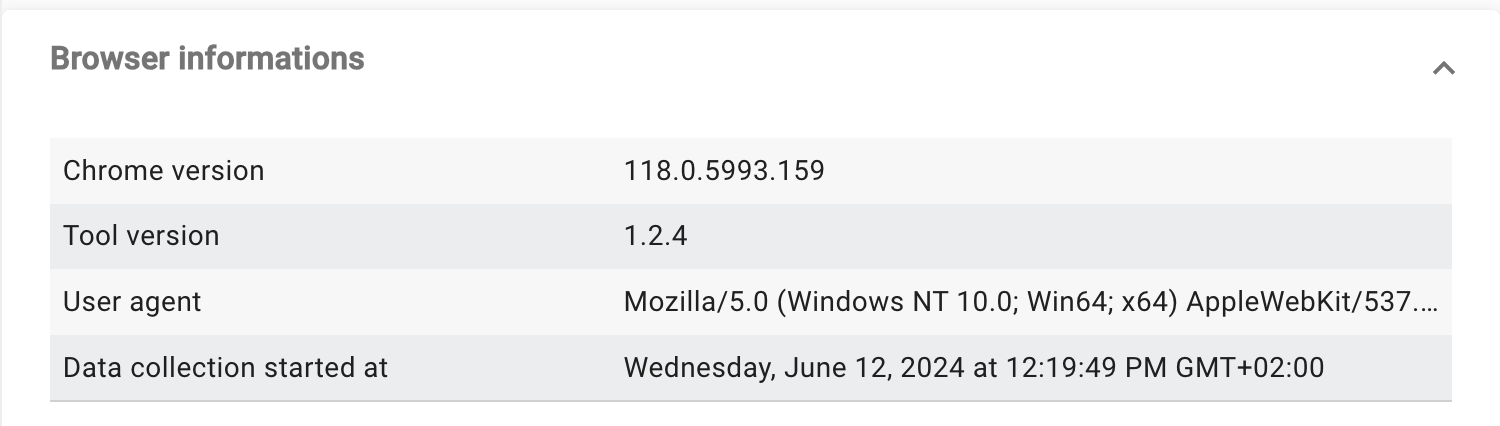
|  |
| --- |
| **Informationen zur Website** |
| \*Name der Website oder verantwortliche Stelle | Dieser Name ist nur informativ und hilft, diese Analyse aus der Liste zu identifizieren. |
| \*URL der Website | Dies ist der Ausgangspunkt der Analyse. Beachten Sie, dass eine Analyse nicht an eine URL gebunden ist und andere URLs beim Surfen enthalten sein können. |
| **Erstes oder neues Szenario** |  |
| \*Wählen Sie eine Quelle für dieses Szenario | Dies sind die Quellen, aus denen Datenerhebungsnachweise für die Durchführung ihrer rechtlichen Beurteilung entnommen werden können:   * *Interner Browser*: Verwenden Sie den Chromium-Browser, der in dieses Tool integriert ist und auch über den Abschnitt BROWSE zugänglich ist. * *HTTP-Archivformat (HAR)*: Verwenden Sie ein JSON-formatiertes Dateiformat, das Nachrichten speichert, die von einem Browser beim Surfen von Websites erzeugt werden. Diese Datei kann über den Inspektor aus allen allgemeinen öffentlichen Browsern generiert werden. * *Website Evidence Collector (WEC)*: Verwenden Sie Berichte, die vom [**Website Evidence Collector (WEC)**](https://edps.europa.eu/edps-inspection-software_en) erstellt wurden, der vom Europäischen Datenschutzbeauftragten (EDPS) für die Durchführung einer rechtlichen Bewertung mit diesem Tool entwickelt wurde.   Die **Verwendung des internen Browsers ist der empfohlene Weg, um eine Analyse durchzuführen**, da er**eine eingehende Analyse von Trackern auf einer Website erstellen kann,** einschließlich Tracking-Funktionen oder Anfragen, die tatsächlich Informationen im Browser speichern. |
| \*Setzen Sie ein Tag für dieses Szenario | Fügen Sie dem Szenario, das Sie auf der Website bewerten möchten (z. B.*vor* Zustimmung, nach Zustimmung, Verwaltung von Optionen usw.) einen Namen für ihre spätere Identifizierung und Bewertung zu. |
| Starten | Sobald alle Informationen korrekt eingegeben sind, erscheint die Starttaste, um die Zuordnung der Informationen mit dem gegebenen Szenario in der Analyse zu initiieren. |

Wenn die interne Browserquelle ausgewählt ist, wird in **Sessions** in der linken Navigationsleiste eine neue Sitzung ANALYSIS > SCENARIO angezeigt. Bis diese Sitzung abgeschlossen ist, wird das neu erstellte Szenario mit allen Informationen verknüpft, die durch diese Sitzung gesammelt werden.

# Der interne Browser

Der interne Browser des EDPB-Website-Auditing-Tools wird angezeigt, wenn Sie ein neues Szenario einer Analyse zuordnen, oder wenn Sie auf die BROWSE oder auf eine bestehende Sitzung in der linken Navigationsleiste klicken.

Es basiert auf einer Chrome-Version, die in der Karte angegeben ist Browser-Informationen:



Die Browseroberfläche besteht aus den folgenden drei Hauptkomponenten:

* die *Symbolleiste* im oberen Teil der Browseroberfläche ermöglicht die Verwaltung von Szenarien, Browsern und Daten, die über den Browser gesammelt werden.
* die auf der linken Seite des Browsers *angezeigten Informationen (Rendern)* zeigen den sichtbaren Teil der Website an, wie Einzelpersonen sie sehen,
* der *Logger* auf der rechten Seite des Browsers zeigt den versteckten Teil der Website an, d. h. alle Kommunikation und Speicherung durch die angegebene Website mit diesem Browser.

Der interne Browser kann einer Sitzung zugeordnet werden (oder nicht). Alle erhobenen Daten werden automatisch im Tool gespeichert und können im Handumdrehen über die Analyseschnittstelle ausgewertet werden.

## Die Symbolleiste

Die Symbolleiste hilft, sowohl Browsersitzungen als auchvom Browser gesammelte Informationen zu verwalten:

|  |  |
| --- | --- |
|  | Navigationsschaltflächen, die es ermöglichen, im Browserverlauf rückwärts und vorwärts zu navigieren oder die aktuelle Seite neu zu laden. |
|  | Informationen, die in Echtzeit über das Logger-Panel angezeigt werden, anhalten oder fortsetzen. **Wenn sie angehalten werden, werden die Informationen immer noch von diesem Tool gesammelt, werden aber bis zur Wiederaufnahme nicht mehr aktualisiert.** |
|  | Wenn nicht ausgewählt, zeigt diese Eingabe den aktuellen Uniform Resource Locator (URL) der im Renderer-Panel angezeigten Webseite an. Wenn Sie ausgewählt sind, können Sie mit dieser Eingabe eine neue URL abrufen. Die http://protocol wird automatisch zu fehlerhaften URLs hinzugefügt. Nicht erreichbare URLs werden gelöscht. |
| Analyse > Szenario  + | Session-Management-Schaltflächen, die die Anzeige des Szenarios und der Analyse dieser Sitzung ermöglichen, sind derzeit (falls vorhanden) verknüpft. Ein Klick auf die aktuelle laufende Sitzung zeigt die Bewertungsansicht des zugehörigen Szenarios an. Als solche können Informationen, die bereits im Logger gesammelt wurden, als konform/nicht konform markiert werden, während die aktuelle laufende Sitzung am Leben bleibt und über **Sessions** in der linken Navigationsleiste zugänglich ist. |
|  | Schaltflächen zur Datenerfassungsverwaltung, die es ermöglichen, eine Momentaufnahme der im Browser angezeigten Website zu machen, alle Informationen sowohl vom Renderer als auch vom Logger zu löschen und die für das aktuelle Szenario gesammelten Daten zu stoppen und zu speichern. |
|  | Schaltflächen zur Browserverwaltung, die jeweils Entwicklertools für den aktuellen Inhalt öffnen, um die Textgröße des Inhalts zu reduzieren oder zu erhöhen |
|  | Das Logger-Panel ausblenden/zeigen. |

## Das Logger-Panel

Das Logger-Panel zeigt in Echtzeit alle Kommunikations- und Informationsspeicher an, die während der Navigation im Browser stattfinden.

Diese Informationen werden in eine Reihe von erweiterbaren *Karten* kategorisiert, die eine Liste von Informationen im Zusammenhang mit der gegebenen Analyse enthalten.

Die Kopfzeile dieser Tabellen in jeder Karte ist anklickbar, um identische Informationen für eine bestimmte Kategorie zu sortieren. Auf einigen Analystenes können Linien der Tabelle individuell ausgewählt werden, um weitere Details zu den ausgewählten Informationen zu erhalten.

## Analysekarten

Jede Karte ist eine Darstellung einer Analyse, die auf der aktuellen Website durchgeführt wurde. Kopfzeilen dieser Karten enthalten die Identifizierung der durchgeführten Analyse, ein Fragezeichen, das mehr Informationen über diese Analyse gibt, und einen Pfeil, um die enthaltenen Informationen zu erweitern oder zu kollabieren. Fragezeichen können über den Einstellungsbereich der linken Navigationsleiste ausgeblendet werden.

Die folgende Tabelle enthält Informationen über jede durchgeführte Analyse:

|  |  |
| --- | --- |
| Screenshot | Listen Sie alle Screenshots auf, die seit Beginn der Sitzung vom Renderer aufgezeichnet wurden. Der Titel jedes Screenshots kann durch den Edit-Button geändert werden, um seine spätere Identifizierung zu unterstützen. |
| Kekse | Führen Sie alle Cookies auf, die seit Beginn der Sitzung gespeichert wurden. Jedes Cookie wird als einzelne Zeile in der Tabelle dargestellt, die nach Domain, Name und potenziellem Zweck aus Wissensdatenbanken (falls vorhanden) klassifiziert ist. Ein Klick auf eine Zeile zeigt detaillierte Informationen zum Cookie an. |
| Lokale Lagerung | Führen Sie alle Schlüsselpaare/Wertpaare auf, die in jedem Frame auf der angezeigten Webseite gespeichert wurden. Jeder Schlüssel im lokalen Speicher wird als eine einzelne Zeile in der Tabelle dargestellt, die der URL des Frames zugeordnet ist, der den Speicher angefordert hat, den Schlüsselwert und den potenziellen Zweck aus Wissensdatenbanken (falls vorhanden). Ein Klick auf eine Zeile zeigt detaillierte Informationen über den lokalen Speicherzugriff an. |
| Verwendung von HTTPS/SSL | Prüfen Sie, ob die aktuelle Webseite eine sichere Kommunikation (SSL) nutzt. Es überprüft auch, ob ein unverschlüsselter Zugriff (HTTP) zu einem sicheren Zugriff (HTTPS) umleitet und den entsprechenden Speicherort angibt. |
| Verkehrsanalyse | Führen Sie alle Domains auf, die vom Renderer angefordert wurden, um die aktuelle Webseite anzuzeigen. |
| Webformulare mit unverschlüsselter Übertragung | Prüfen Sie, ob die gerenderte Seite ein Formular enthält, in dem Daten über eine ungesicherte Kommunikation (HTTP) übertragen werden. Jedes Formular wird als eine einzige Zeile in der Tabelle dargestellt, die mit seiner Identifizierung im Quellcode und der beim Absenden ausgeführten Aktion verknüpft ist. |
| Beacons | Listet alle bekannten Zählpixel (Web Beacons) auf, die in der gerenderten Seite gemäß [**EasyPrivacy und Fanboy’**](https://easylist.to/#easyprivacy) s [**Annoyance**](https://easylist.to/#fanboy-s-annoyance-list) -Liste enthalten sind. **Diese Liste ist nur informativ, sie kann unvollständig sein oder falsche Positive aufgrund ungenauer oder veralteter Signaturen enthalten.** |
| Testsl | Wenn Sie im Abschnitt Einstellungen konfiguriert sind, kann das Befehlszeilenwerkzeug testsl.sh auf der aktuellen URL durchgeführt werden, indem Sie auf die Wiedergabe-Schaltfläche klicken. Dieses Tool überprüft die Unterstützung von TLS/SSL-Chiffren, Protokollen sowie aktuellen kryptografischen Fehlern auf dem aktuellen URL-Server. Beachten Sie, dass dieser Test mehrere Minuten dauert. |
| Browser-Informationen | Alle Informationen zum Kontext der Analyse anzeigen: die Version des Tools und des Browsers, der User Agent und der Startzeitpunkt der Datenerfassung. |

## Das Detail-Panel

Detaillierte Informationen, die während der aktuellen Sitzungen über Cookies, lokale Speicherung und Web Beacons gespeichert oder übertragen werden, sind über ein Fenster zugänglich, das am bo ttom erscheint, wenn eine Zeile in Tabellen ausgewählt wird.

Diese detaillierten Informationen sind in drei Kategorien unterteilt:

|  |  |
| --- | --- |
| Details | Liste vollständige Informationen über einen bestimmten Cookie, Schlüssel im lokalen Speicher oder ein Web Beacon. |
| Protokolle | Zeigen Sie die Rohinformationen und den Call-Stack-Baum oder die Anforderung an, die zur Ablage des angegebenen Cookies, zum Eintrag des Schlüssels im lokalen Speicher oder zur Einleitung der Anfrage aus dem Webbeacon führt. |
| Wissen | Wenn der aktuelle Eintrag in einer Wissensdatenbank gefunden wurde, listet diese Registerkarte die passende Wissensdatenbank und den passenden Eintrag in dieser entsprechend ihrer Kategorie auf.  Wenn es sich um ein Cookie handelt, werden diese Einträge wie folgt kategorisiert:   * *Exakte Übereinstimmung*: mindestens ein Eintrag entspricht dem Namen und der Domain des Cookies, * *Name* des Spiels: mindestens ein Eintrag entspricht dem Namen des Cookies mit einer Wildcard-Domain (*\**), * *Match Domain*: mindestens ein Eintrag entspricht der Domain dieses Cookies.   Wenn es sich um einen Schlüssel im lokalen Speicher handelt, entspricht mindestens ein Eintrag dem Schlüssel oder dem Skript, das für diesen Eintrag verantwortlich ist. |
| Details schließen | Klicken Sie auf diesen Button oben im Loggerbedienfeld, um das aktuelle Detailfenster zu schließen. |

# Treffen einer Entscheidung über Compliance/Nicht-Compliance

Um bei der Beurteilung der Einhaltung der Website-Compliance zu helfen, können Analysen, Szenarien und Karten als konform, nicht konform oder definiert werden.

Diese Bewertungsschnittstelle kann jederzeit erreicht werden, indem Sie während einer Sitzung auf die Symbolleistenschaltfläche Analyse > Szenario klicken oder nach der Erfassung von Beweisen durch die Liste in der linken Seitenleistennavigation.

Diese Liste gibt einen Überblick über alle im Website-Auditing-Tool gespeicherten Analysen und deren aktuelle Bewertung.

Jeder Eintrag hat folgende Form:

|  |  |
| --- | --- |
| Analyse Konform  Nicht konform  Zu definieren | Das Unternehmen, das mit dieser Analyse und seiner aktuellen Bewertung verbunden ist. |
|  | Aktionsschaltflächen für die aktuelle Analyse, um diesen Eintrag anzuzeigen bzw. zu bewerten, einen Bericht über diese Analyse zu erstellen und den Eintrag zu löschen. |
| Szenario 1  Szenario 2  Szenario 3 | Die Szenarien, die für die gegebene Analyse aufgezeichnet wurden. Die Farbe entspricht ihrer jeweiligen aktuellen Bewertung (**konform,** **nicht konform** oder **zu definieren**). |
| Link www.(...).com Datum\_Bereich 10/01/2022 | Andere Metadaten, die mit dieser Analyse verbunden sind, d. h. der Link, der bei der Erstellung der Analyse und dem Datum dieser Erstellung angegeben wurde. |

Das rechte Panel ermöglicht es, diese Analysen nach ihrer Identifikation oder ihrer aktuellen Bewertung zu filtern.

## Auswertung

Die Auswahl des Buttons durch eine Analyse, ein Szenario oder eine Karte ermöglicht das Navigieren im angegebenen Element und erhält detaillierte Informationen.

Jedes dieser Elemente kann markiert werden, um die globale Bewertung der Website wie folgt durchzuführen:

|  |  |
| --- | --- |
| Konform  Nicht konform  Zu definieren | Markieren Sie eine Analyse als konform, nicht konform und nach den gesetzlichen Anforderungen zu bewerten. |
| Schließen  Schreiben Sie einen Kommentar | Öffnen und schließen Sie einen Texteditor, um einen Kommentar über die gegebene Bewertung zu schreiben. |
| fertig | Einzelne Zeilen dieser Karten:   * **Cookies**, * **Lokale Lagerung**, * **Web Beacons** und * Testsl   kann auch als konform gekennzeichnet, nicht konform oder definiert werden, um die Bewertung zu unterstützen. |
| *Bewertung am 25. November 2022* | Datum der letzten Bewertung. |

Die erste Karte der Analyse oder des Szenarios gibt einen Überblick über jedes Szenario oder jede Karte mit ihrer aktuellen Auswertung. Es ermöglicht auch eine globale Auswertung für die aktuelle Analyse oder das Szenario entsprechend diesen Elementen.

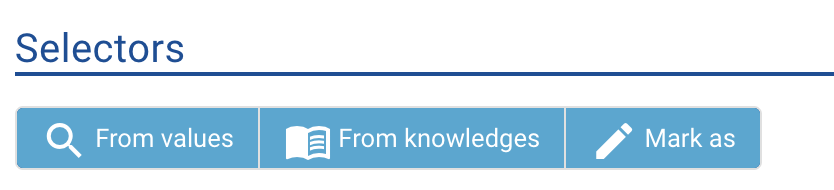
Jede einzelne Zeile in der Tabelle dieser Karten (Cookies**,** **lokale Speicherung** und **Web Beacons**) kann ausgewählt werden, um detailliertere Informationen auf der rechten Seite zu erhalten **Weitere Details**. Auf Cookie- und lokalen Speicherlinien bietet der Wissens- Tab einfachen Zugriff auf passende Einträge aus der entsprechenden Wissensdatenbank oder um diesen Eintrag in eine Wissensdatenbank aufzunehmen. Klicken Sie auf [**Wissensdatenbank**](http://localhost:4200/#/helps/knowledge_base), um weitere Informationen über die Verwaltung zu erhalten.

Jederzeit kann ein neues Szenario an die Analyse angehängt werden, indem Sie auf + im linken **Szenario** -Panel klicken.

Nach der Auswertung der Analyse können Sie Berichte generieren, die gesammelte Daten, Auswertungen und Kommentare in einem übertragbaren Format enthalten. Klicken Sie auf [**Berichte erstellen**](http://localhost:4200/#/helps/create_reports), um Anleitungen zu erhalten.

## Selektoren

Die Karten Cookies**, Local Storage und Web Beacons bieten eine Reihe von Selektoren, die eine Reihe gemeinsamer Attribute zwischen den Kartenzeilen auswählen und markieren:**



Die Auswahl kann auf einer Kombination der Attribute der Zeile (z. B. Domain und Name des Cookies), ihrer aktuellen Bewertung (kompliant, nicht konform, zu definieren) oder Übereinstimmungen in Wissensdatenbanken basieren, einschließlich ihrer Kategorisierung unter allen Wissensdatenbanken. Das Ergebnis wird im Inhaltsbereich dynamisch aktualisiert. Schließlich ermöglicht die Funktion „mark as“ die Auswertung der resultierenden Auswahl.

# Wissensbasis

Informationen, die in Browsern von einer Website gespeichert werden, können mehrere Zwecke haben, entweder für das ordnungsgemäße Funktionieren der Website oder für Nebenzwecke, wie z. B. das Tracking des Surfens der Nutzer zur Bereitstellung gezielter Werbung. Daher kann es sein, dass einige vor ihrer Nutzung durch die Website oder Dritte ihre Zustimmung benötigen, um den gesetzlichen Anforderungen zu entsprechen, während andere davon ausgenommen werden könnten.

Viele dieser Tracker werden über externe SDK gespeichert, die von Drittanbietern entwickelt wurden, da sie gemeinsame Eigenschaften zwischen Websites wie der Domain, dem Schlüsselnamen oder Skripten teilen. Wissensdatenbanken können helfen, diese Tracker zu identifizieren und Wissen im Laufe der Zeit mit Fall-zu-Fall-Analysen zu konsolidieren.

Die Identifizierung bekannter Tracker aus allen aktivierten Wissensdatenbanken erfolgt kontinuierlich während des Surfens. Die Auswahl eines Cookies oder der Schlüsselzeile eines lokalen Speichers aus Karten des Logger-Panels zeigt Details zu passenden Einträgen in allen Datenbanken an.

Diese Informationen sind auch unter **Weitere Details** bei der Bewertung der rechtlichen Übereinstimmung einer Analyse zugänglich. Das Erweiterungspanel **Hinzufügen dieses Elements zu einer Wissensdatenbank** ermöglicht auch das Hinzufügen noch unbekannter Tracker für ihre spätere Bewertung.

Schließlich ist der vollständige Inhalt des Wissens über KNOWLEDGE BASE in der Kategorie **Editor** in der linken Navigationsleiste zugänglich.

## Anzeigen und Bearbeiten einer Wissensdatenbank

Jede Wissensdatenbank wird durch einen Namen und einen Autor identifiziert. Es ist mit einem Vertrauensniveau verbunden und besteht aus einer Reihe von Einträgen, die entweder auf Cookies oder Schlüssel in der lokalen Speicherung abzielen können. Es kann verwendet werden oder nicht für die Identifizierung von übereinstimmenden Einträgen während des Surfens und der Analyse.

In der folgenden Tabelle ist der Zweck jedes Elements im Abschnitt KNOWLEDGE BASE aufgeführt:

|  |  |
| --- | --- |
| Neue Datenbank | Standardmäßig enthält das Website-Auditing-Tool keine Wissensdatenbank. Benutzer können entweder einen neuen erstellen, einen Namen und die entsprechende Kategorie (*Cookie* oder *Local Storage*) auswählen. |
| Importieren | Sie können auch bestehende Datenbanken im json-Format importieren, die bereits von anderen über das Website-Auditing-Tool erstellt wurden. |
| Exportieren Sie alle | Schließlich können sie alle Datenbanken, die in diesem Tool enthalten sind, über eine json-Formatdatei exportieren, zum Teilen oder Archivieren. |

Datenbank- und Datenbankeinträge können individuell über eine Reihe von Schaltflächen verwaltet werden, die das Betrachten, Herunterladen, Duplizieren oder Entfernen des ausgewählten Eintrags ermöglichen.

Datenbanken sind einem Grad an Sicherheit (Validated/zuverlässig/informativ) und einer Farbe zugeordnet, die bei der Bewertung für jeden Tracker helfen kann.

### Cookie-Einträge

Die Schaltfläche „Ansicht“ in einer Cookie-Wissensdatenbank bietet eine vollständige Ansicht aller darin enthaltenen Einträge, kategorisiert nach ihrer Domain, ihrem Namen und ihrer Kategorie.

Ein Klick auf einen Cookie-Wissenseintrag gibt detailliertere Informationen zu diesem Eintrag:

|  |  |
| --- | --- |
| Kategorie | Der identifizierte Zweck des Cookies. Mögliche Einträge sind: *Gezielte Werbung*, *Non-Targeted Advertising*, *Technical*, *Analytics (ausgenommen)*, *Analytik (nicht ausgenommen)*, *Social Media*, *Social Media*, *Content Customization* oder*? (Unbekannt*) |
| Domänen | Die URL-Domain, von der aus Cookies gespeichert wurden. Seine Syntax umfasst Wildcards (\*). Wenn also ein Cookie von der URL der Drittanbieter-Domains wie „server1.adcompany.com“ und „server2.adcompany.com“ hinterlegt wird, lautet der erwartete Eintrag „\*.adcompany.com“. Wenn ein Cookie notwendigerweise von der besuchten Website-URL (*Erste Partei*) hinterlegt wird und die Domain keine relevanten Informationen ist, dann ist der erwartete Eintrag „\*“. |
| Namen | Der vom Cookie verwendete Identifikationsschlüssel. Die Verwendung von Wildcards (\*) wird ebenfalls akzeptiert. Wenn ein Cookie als „RTB\_1234“ und „RTB\_5678“ bezeichnet wird, lautet die erwartete Eingabe „RTB\_\*“. Wenn eine Domain notwendigerweise mit einem Zweck verbunden ist und der Name des Cookies nicht relevant ist, ist der erwartete Eintrag „\*“. |
| Quelle | Herkunft oder Herkunft der Identifizierung. |
| Datenkontroller | Der identifizierte Datenverantwortliche für die identifizierte Datenverarbeitung. Verwenden Sie „? wenn es unbekannt ist. |
| Datenschutzerklärung | Die URL der Datenschutzerklärung, falls vorhanden. |
| Referenztyp | Wenn es Fälle gibt (z.*B.* bestehende Sanktionen), die sich auf dieses Cookie beziehen. |
| Bemerkung | Kommentare können verwendet werden, um kontextbezogene Informationen zum Cookie hinzuzufügen. |

Jeder Eintrag des angezeigten Formulars kann mit einem Klick bearbeitet werden. Schließlich können neue Einträge mit Neuer Cookie-Eingabe hinzugefügt werden.

### Lokale Speichereinträge

Die Schaltfläche „Ansicht“ in einer lokalen Speicher-Wissensdatenbank gibt einen vollständigen Überblick über alle darin enthaltenen Einträge. Diese Einträge funktionieren in ähnlicher Weise wie Cookies. Diese Einzahlung kann jedoch nur durch Skripte erfolgen.

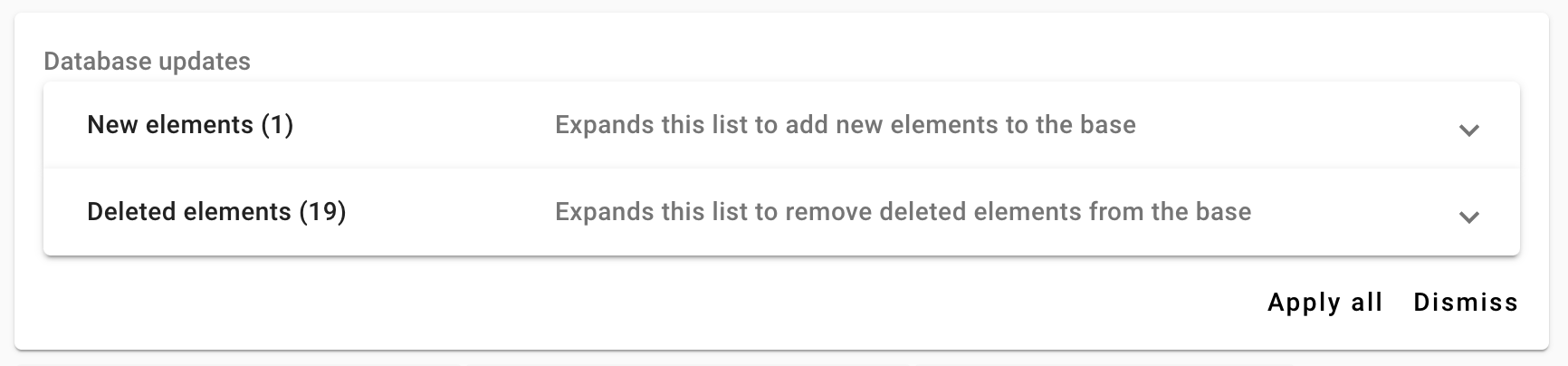
Ein Klick auf einen Schlüssel eines lokalen Speichers gibt detailliertere Informationen zu diesem Eintrag:

|  |  |
| --- | --- |
| Kategorie | Der identifizierte Zweck des Cookies. Mögliche Einträge sind: *Gezielte Werbung*, *Non-Targeted Advertising*, *Technical*, *Analytics (ausgenommen)*, *Analytik (nicht ausgenommen)*, *Social Media*, *Social Media*, *Content Customization* oder*? (Unbekannt*) |
| Schlüssel | Der Schlüsselwert dieses Eintrags. Die Verwendung von Wildcards (\*) wird ebenfalls akzeptiert. Wenn ein Cookie „RTB\_1234“ und „RTB\_5678“ genannt wird, lautet die erwartete Eingabe „RTB\_\*“. |
| Script | Die URL des Skripts, die verwendet wird, um diesen ausgewählten Schlüssel zu verwalten. Das Call-Stack-Protokoll am Ursprung der Ablage des angegebenen Schlüssels wird analysiert, um das passende Skript zu finden. |
| Quelle | Herkunft oder Herkunft der Identifizierung. |
| Datenkontroller | Der identifizierte Datenverantwortliche für die identifizierte Datenverarbeitung. Verwenden Sie „? wenn es unbekannt ist. |
| Datenschutzerklärung | Die URL der Datenschutzerklärung, falls vorhanden. |
| Referenztyp | Wenn es Fälle gibt (z.*B.* bestehende Sanktionen), die sich auf diesen Eintrag beziehen. |
| Bemerkung | Kommentare können verwendet werden, um kontextbezogene Informationen zum Cookie hinzuzufügen. |

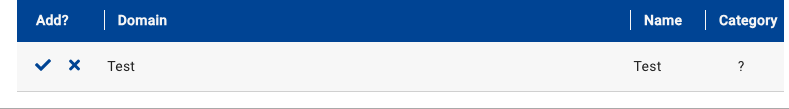
Jeder Eintrag des angezeigten Formulars kann auch mit einem Klick auf die Informationen bearbeitet werden. Neue Einträge können mit Neuem lokalen Speichereintrag hinzugefügt werden.

## Aktualisieren einer Datenbank

Jede einzelne Datenbank kann über die *Update-Datenbankfunktion in der Ansichtsschnittstelle* mit anderen exportierten Datenbanken zusammengeführt werden. Durch die Auswahl einer.json-Datei aus einer exportierten Datenbank kann das Tool neue oder fehlende Einträge in der aktuellen Datenbank über die folgende Schnittstelle identifizieren:



Jede Änderung kann einzeln akzeptiert oder abgelehnt werden, indem die neuen oder gelöschten Elemente erweitert werden:



Sie können alle mit der Schaltfläche „Alle anwenden“ angenommen und jederzeit mit dem Abschalten-Button gestoppt werden.

## Wissensdatenbanknutzung

Jeder Cookie oder Eintrag im lokalen Speicher, der während einer Browsersitzung gespeichert wird, wird automatisch auf die Suche nach passenden Einträgen in der Wissensdatenbank gescannt.

Identifizierte Zwecke der Übereinstimmung von Einträgen sind in der *Kategorie* -Zeile in Tabellen von Cookie- und lokalen Speicherkarten sowie in der folgenden Registerkarte aus dem Detailfenster bei der Auswahl einer Zeile in Tabellen verfügbar.

Wenn der aktuelle Eintrag in einer Wissensdatenbank gefunden wird, listet dieser Reiter den passenden Eintrag in der Wissensdatenbank entsprechend seiner Kategorie auf.

Wenn es sich um ein Cookie handelt, werden diese Einträge wie folgt kategorisiert:

* *Exakte Übereinstimmung*: mindestens ein Eintrag entspricht dem Namen und der Domain des Cookies,
* *Name* des Spiels: mindestens ein Eintrag entspricht dem Namen des Cookies mit einer Wildcard-Domain (*\**),
* *Match Domain*: mindestens ein Eintrag entspricht der Domain dieses Cookies.

Wenn es sich um einen Schlüssel im lokalen Speicher handelt, entspricht mindestens ein Eintrag dem Schlüssel oder dem Skript, das für diesen Eintrag verantwortlich ist.

Alle Datenbanken sind einem Vertrauensgrad (Validated/zuverlässig/informativ) und einer Farbe zugeordnet, die dazu beiträgt, Fälle zu identifizieren, in denen die Bewertung der Zwecke zwischen den Wissensdatenbanken unterschiedlich ist.

Sie können auf [**Bereitstellung neuer Analysen**](http://localhost:4200/#/helps/new_analysis) für die Verwendung dieser Informationen verweisen, um Compliance/Nichtkonformität von Websites gemäß den gesetzlichen Anforderungen zu bewerten.

# Berichte erstellen

Berichte sind formatierte Dokumente, entsprechend einer bestimmten *Informationsvorlage*, die in einer *Analyse*, einem *Szenario* oder einer gegebenen *Karte* enthalten ist.

Die Schnittstellenbearbeitungsberichte sind in jeder Zeile der Tabelle **Zusammenfassung der Auswertungen** in einer bestimmten Analyse oder einem bestimmten Szenario zugänglich.

## Berichtsschnittstelle

Die Berichtsschnittstelle besteht aus den folgenden drei Hauptkomponenten:

Werkzeugleiste bearbeiten/exportieren

Werkzeugleiste zur Informationsfilterung

Vorschau des Berichts

* die *Werkzeugleiste Bearbeiten/Export* im oberen Teil der Schnittstelle ermöglicht die Bearbeitung des Berichts und die Auswahl eines Formats für seine Exporte (*json*, *XLSX*, *PDF* oder *DOCX*),
* die *Symbolleiste zur Informationsfilterung* ermöglicht die Auswahl von Informationen, die gemäß ihrer Identifizierung oder Bewertung gemeldet werden können.
* der *Vorschaurahmen* gibt einen Überblick über die in den Abschlussberichten enthaltenen Informationen. Es bietet auch einen einfachen Editor zum Hinzufügen oder Entfernen von Informationen im Bericht. Beachten Sie, dass sich das endgültige Rendering je nach ausgewähltem Exportformat unterscheiden kann.

### Werkzeugleiste bearbeiten/exportieren

Die Werkzeugleiste Bearbeiten/Export zum Bearbeiten von Informationen der Berichte und zum Exportieren in jedem Format:

|  |  |
| --- | --- |
| Bearbeiten | Öffnen Sie einen einfachen Editor im Vorschaurahmen zum Hinzufügen oder Entfernen von Informationen im generierten Bericht. Beachten Sie, dass geänderte Informationen nur beim Export in PDF oder Docx sichtbar sind. Wenn Sie neue Filter aus der *Symbolleiste „Informationsfilter“* auswählen, löschen Sie alle aktuellen Änderungen. |
| Speichern als JSON | Exportieren Sie Rohinformationen einer bestimmten *Analyse*, *Szenario* oder *Karte* mit dem JavaScript Object Notation (JSON) Format. |
| Speichern als XLSX | Exportieren Sie Rohinformationen einer bestimmten *Analyse*, *Szenario* oder *Karte* in Tabellenkalkulationen mit Office Open XML (XLXS) Format. |
| Als PDF speichern | Exportieren Sie formatierte Informationen einer bestimmten *Analyse*, eines *Szenarios* oder einer *Karte* im Portable Document Format (PDF). |
| Speichern als Docx | Exportieren Sie formatierte Informationen einer bestimmten *Analyse*, eines *Szenarios* oder einer *Karte* in einem bearbeitbaren Office Open XML (DOCX). |

Formatierte Informationen entsprechen der Generierung von HTML-Darstellung eines Berichts basierend auf einer Vorlage im PUG-Format. Neue Vorlagen können im Abschnitt TEMPLATE in der linken Navigationsleiste importiert und in der *Symbolleiste „Informationsfilter“* ausgewählt werden.

### Werkzeugleiste zur Informationsfilterung

Die Werkzeugleiste zur Informationsfilterung ermöglicht die Auswahl von Analysen, Szenarien und Karten je nach ihrer Identifikation oder ihrer jeweiligen Bewertung nach Optionen oder einer Vorlage:

|  |  |
| --- | --- |
| Wählen Sie eine Vorlage aus | Verwenden Sie eine PUG-Vorlage wurde aus dem Abschnitt BeschreibungTEMPLATE in der linken Navigationsleiste importiert. |
| Tags auswählen, um zu melden | Wenn Sie eine vollständige Analyse melden, können Sie eine Reihe von Szenarien oder alle Szenarien auswählen, die in den Bericht aufgenommen werden sollen. |
| Wählen Sie Karten aus, um zu melden | Wenn Sie eine Analyse oder ein Szenario melden, können Sie einen Satz von Karten oder alle Karten auswählen, die in den Bericht aufgenommen werden sollen. |
| Auswertungen auswählen, um Bericht zu erstatten | Wenn Sie eine Analyse, ein Szenario oder eine Karte melden, können Bewertungen oder Kommentare in den Bericht aufgenommen werden. Beachten Sie, dass diese Option auch für Zeilen in Cookies, lokale Speicherung, Beacons und testssl gilt. |
| Wählen Sie einen Anhang aus | Bei der Meldung einer Analyse, eines Szenarios oder einer Karte kann ein Untersuchungsanhang hinzugefügt werden, um beispielsweise zu erläutern, wie die Untersuchung durchgeführt wurde. |

Vorlagen- und Filteroptionen sind gegenseitig inklusiv. Als solche können Vorlagen vollständige Informationen über Analysen, Szenarien und Karten sein, die später durch die Filteroptionen ausgewählt werden könnten.

## Bearbeiten neuer Vorlagen

Neue Vorlagen können im Template-Bereich mit der Schaltfläche *Neue Vorlage* hinzugefügt werden.

Die einzige unterstützte Syntax für Templates ist jedoch [**PUG**](https://github.com/pugjs/pug). Der generierte Bericht aus einer Vorlage entspricht den Daten, die im json einer Analyse, einem Szenario oder einer Karte den entsprechenden *Locals* in der Mops-Syntax enthalten sind.

Sie können den Abschnitt „ *Sprachreferenz*“ der [**offiziellen Website**](https://pugjs.org/api/getting-started.html) lesen, um vollständige Informationen in der Syntax zu erhalten.

Der TEMPLATE bietet eine Reihe von Aktionen zum Importieren, Bearbeiten oder Duplizieren vorhandener Vorlagen:

|  |  |
| --- | --- |
| Neue Vorlage | Importieren Sie eine Vorlage in PUG-Syntax mit einem Namen und einem Autor für die spätere Verwendung in Berichten. |
|  | Bzw. importierte Vorlagen herunterladen und löschen |

Als erste Einführung zum Generieren neuer Vorlagen empfehlen wir, eine Analyse, ein Szenario oder ein Tag aus der *Werkzeugleiste Bearbeiten/Export* im JSON-Rohformat herunterzuladen, um passende Einträge zu finden.

Viele Online-Online-Pug-Testing-Tool ermöglicht das Kopieren/Einfügen von PUG-Vorlagen und JSON-Informationen, um das endgültige HTML zu rendern. *Die Standardvorlage* kann auch als Referenz exportiert werden.

## Hinzufügung eines neuen Anhangs

Anhang kann auch im Muster-Abschnitt mit der Schaltfläche „ *Neuer Anhang*“ hinzugefügt werden.

Die einzige unterstützte Syntax für Anhang ist HTML. Viele Software unterstützt den Export eines Formats (z. B. DOCx oder PDF) in HTML. Dieser Anhang wird automatisch an der Stelle { *annex} in der* Mops-Syntax der Mopsvorlage hinzugefügt*.* In der Standard-Pug-Vorlage wird dieser Anhang wie am Ende des Berichts beigefügt*.*

1. <https://testssl.sh/> [↑](#footnote-ref-1)
2. Quelle und Entwicklung sind auf GitHub unter <https://github.com/drwetter/testssl.sh>. [↑](#footnote-ref-2)