

Endpunktbericht

Seite 1 von 14

Übersicht

Verfügbarkeit

SSL/TLS

WTI

PortScan

HTTP-Headers

Endpunkt

https://www. 

Bericht erstellt am 21.05.2019 11:01 Uhr

Verfügbarkeit**A+**

Überprüfung der Erreichbarkeit Ihrer Website von verschiedenen Standpunkten aus.

SSL/TLS**C**

Überprüfung Ihres Webservers und Verschlüsselungen. Außerdem werden Chiffren, Protokolle und der aktuelle technische Stand bewertet.

WTI**A++**

Angriffsmöglichkeiten von außerhalb. Basierend auf installierter Software Ihres Servers.

Portscans**A++**

Überprüfung Ihres Servers hinsichtlich offener Ports.

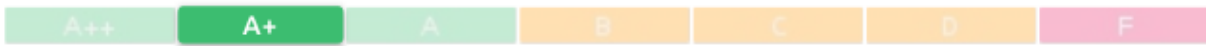
HTTP-Headers**F**

Überprüfung der gesetzten oder fehlenden HTTP-Headers, um potentielle Sicherheitslücken zu schließen.

Verfügbarkeit

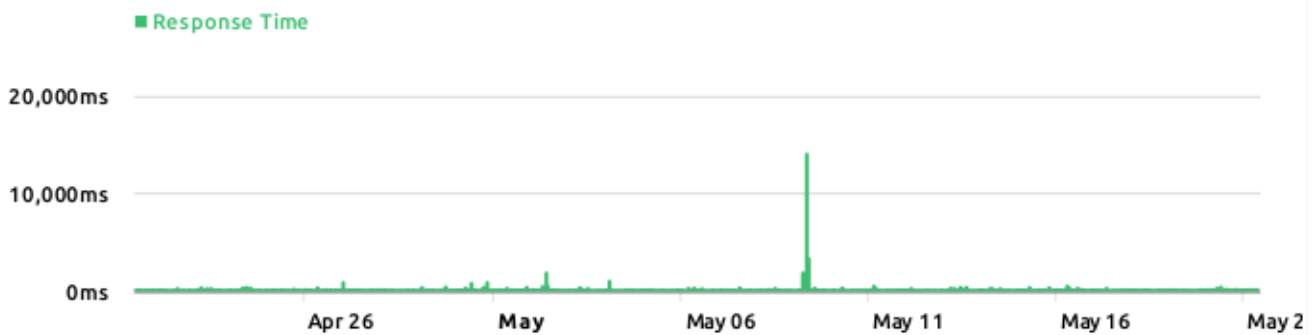
↳ <https://w>

Übersicht **Verfügbarkeit** SSL/TLS WTI PortScan HTTP-Headers



Verfügbarkeit (eu-central-frankfurt) Betrachteter Zeitraum: 21.04.2019 - 21.05.2019

99.87%



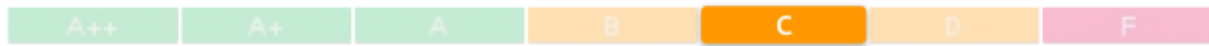
Ausfallzeit:

Dauer	Startzeitpunkt	Endzeitpunkt
5 Minuten	09.05.2019 10:10 Uhr	09.05.2019 10:15 Uhr
5 Minuten	09.05.2019 07:42 Uhr	09.05.2019 07:47 Uhr
10 Minuten	09.05.2019 07:15 Uhr	09.05.2019 07:26 Uhr

SSL/TLS

↗ <https://www.Enginsight.com>

- Übersicht
- Verfügbarkeit
- SSL/TLS**
- WTI
- PortScan
- HTTP-Headers



Ihr Webserver sowie die eingesetzte Verschlüsselung werden hinsichtlich bekannter Sicherheitslücken überprüft. Außerdem werden jedliche Chiffren, zugelassene Protokolle und der aktuelle technische Stand bewertet.

Zertifikat

Version:
Version.v3

Serial:
[REDACTED]


Fingerprint:
[REDACTED]

Gültig bis:
27.06.2019

Öffentlicher Schlüssel:
RSA 2048

Veröffentlicht von:
Let's Encrypt | US

Datenschutz



DSGVO / GDPR
Datenschutzgrundverordnung
Die Verschlüsselung erfolgt nach dem aktuellen Stand der Technik.



BSI
Bundesamt für Sicherheit in der Informationstechnik
Die Verschlüsselung erfolgt nicht nach Maßgabe und Empfehlung des BSI.







SSL/TLS

↗ <https://w...>





















Übersicht Verfügbarkeit **SSL/TLS** WTI PortScan HTTP-Headers



Protokolle

Protokoll	Unterstützung
Secure Sockets Layer 2.0	
Secure Sockets Layer 3.0	
Transport Layer Security 1.0	
Transport Layer Security 1.1	
Transport Layer Security 1.2	
Transport Layer Security 1.3	

Chiffren

Name (OPENSSL)	Protokoll	Schlüsselstärke
 AES256-SHA	TLSv12	256
 DHE-RSA-AES256-SHA	TLSv12	256
 AES256-GCM-SHA384	TLSv12	256
 DHE-RSA-AES256-SHA256	TLSv12	256
 ECDHE-RSA-AES256-SHA	TLSv12	256
 AES256-SHA256	TLSv12	256
 ECDHE-RSA-AES256-GCM-SHA384	TLSv12	256
 ECDHE-RSA-AES256-SHA384	TLSv12	256
 ECDHE-RSA-CHACHA20-POLY1305	TLSv12	256
 DHE-RSA-AES256-GCM-SHA384	TLSv12	256
 DHE-RSA-AES128-SHA	TLSv12	128
 AES128-SHA	TLSv12	128
 AES128-GCM-SHA256	TLSv12	128
 AES128-SHA256	TLSv12	128
 ECDHE-RSA-AES128-SHA256	TLSv12	128
 ECDHE-RSA-AES128-SHA	TLSv12	128
 ECDHE-RSA-AES128-GCM-SHA256	TLSv12	128
 DHE-RSA-AES128-SHA256	TLSv12	128
 DHE-RSA-AES128-GCM-SHA256	TLSv12	128
 ECDHE-RSA-DES-CBC3-SHA	TLSv12	112

SSL/TLS

↗ <https://w>

Übersicht

Verfügbarkeit

SSL/TLS

WTI

PortScan

HTTP-Headers

A++

A+

A

B

C

D

F

CVEs

Sweet32 (CVE-2016-2183)

Dieser Kollisionsangriff beruht auf der veralteten Triple-DES Chiffre. Es wird empfohlen diese zu deaktivieren.

C

Beast (CVE-2011-3389)

Ein Angreifer kann unter bestimmten Voraussetzungen beispielsweise die Cookies einer verschlüsselten Verbindung auszuspähen. Die Serversicherheit ist von diesem Angriff nicht betroffen.

B

Supports Weak Protocols

Die Protokolle SSL2, SSL3 sowie TLS1.0 gelten als unsicher und sollten deaktiviert werden.

C

Supports Weak Ciphers

Die verwendeten Chiffren entsprechen nicht dem aktuellen Mindestsicherheitsstandard. Chiffren sollte mindestens eine Schlüssellänge von 128-bit aufweisen.

B

Supports Non-Compliant Encryption Standards (BSI)

Die Verschlüsselung entspricht nicht der Maßgabe und Empfehlung des BSI.

B

WTI

<https://w>

Seite 6 von 14

[Übersicht](#)[Verfügbarkeit](#)[SSL/TLS](#)**WTI**[PortScan](#)[HTTP-Headers](#)

A++

A+

A

B

C

D

F

Anwendung

Session Prediction



Diese Attacke untersucht Session-Ids auf wiederkehrende Muster.

Cross-Site-Scripting



Ermöglicht das Ausführen von Schadcode.

SQL Injection



Eine SQL-Injection kann über Eingabefehler einer Webseite Schadcode in Datenbankabfragen platzieren.

Fuzzy Redirects



Prüft die Webanwendung auf unvalidierte Weiterleitungen.

WTI

↗ <https://>

Seite 7 von 14

Übersicht

Verfügbarkeit

SSL/TLS

WTI

PortScan

HTTP-Headers

A++

A+

A

B

C

D

F

Webseite

Malware

Prüft die Anwendung auf potentielle Malware, Backdoors oder sonstigen Infizierungen.



externe iFrames

Prüft, ob auf Ihrer Seite externe iFrames eingebunden werden.



Veraltete Dateien

Prüft die Anwendung auf veraltete Dateien, die potentielle Angriffe ermöglichen.



Blacklisted

Prüft, ob die Domain (oder IP) auf einer Blacklist gelistet ist.



WTI

↗ <https://www.>

Seite 8 von 14

Übersicht

Verfügbarkeit

SSL/TLS

WTI

PortScan

HTTP-Headers

A++

A+

A

B

C

D

F

Server

Cross-Site-Tracing



Ermöglicht das Abfangen von sensiblen Benutzerinformationen.

HTTPS Unterstützung



Ermittelt, ob der Server eine gesicherte HTTPS-Verbindung aufbauen kann und ob diese vertrauenswürdig ist.

Directory Listing



Ermöglicht die automatische Auflistung von Dateien in einem bestimmten Verzeichnis.

WTI

↗ <https://www.>

Seite 9 von 14

Übersicht

Verfügbarkeit

SSL/TLS

WTI

PortScan

HTTP-Headers

A++

A+

A

B

C

D

F

Anfällige Software

Produkt

php
nginx

Hersteller

php
nginx

Version

Portscan

↗ <https://www.Enginsight.com>

Übersicht Verfügbarkeit SSL/TLS WTI **PortScan** HTTP-Headers



Status	Port	Service	Version	CVEs (Score)
OFFEN	80	HTTP	--	--
OFFEN	443	HTTPS	--	--

HTTP-Headers

<https://w>

Seite 11 von 14

Übersicht

Verfügbarkeit

SSL/TLS

WTI

PortScan

HTTP-Headers

A++

A+

A

B

C

D

F

Server

Der Server-Header beinhaltet Informationen über die Software, die von dem Ursprungsserver verwendet wurde. Diese Informationen sollten aus Sicherheitsgründen immer deaktiviert werden.

Gesetzter Wert: nginx

Date

Gesetzter Wert: Tue, 21 May 2019 10:25:49 GMT

Content-Type

Gesetzter Wert: text/html; charset=UTF-8

Transfer-Encoding

Gesetzter Wert: chunked

Connection

Gesetzter Wert: close

Vary

Gesetzter Wert: Accept-Encoding, Accept-Encoding

HTTP-Headers


↗ <https://...>

- Übersicht
- Verfügbarkeit
- SSL/TLS
- WTI
- PortScan
- HTTP-Headers**

A++ A+ A B C D **F**

Set-Cookie

F

Der Set-Cookie HTTP-Header wird verwendet, um Cookies vom Server zum Browser zu übertragen. Wird eine HTTPS-Verbindung verwendet, sollte der "Secure"-Flag zum Einsatz kommen.
Gesetzter Wert: PHPSESSID=klInuni5mh8vd95d03of6kivu2; 

Cache-Control

Gesetzter Wert: public s-max-age = 900

Content-Encoding

Gesetzter Wert: gzip

Feature-Policy

B

Die Feature-Policy bestimmt, welche Funktionen oder APIs eines Browsers verwendet werden dürfen.
Empfehlung: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; microphone 'none'; payment 'none'; usb 'none'
Gesetzter Wert: Nicht gesetzt.

X-Frame-Options

F

Die X-Frame-Options können verwendet werden, um zu bestimmen, ob ein aufrufender Browser die Zielseite in einem 'frame', 'iframe' oder 'object' rendern also einbetten darf.
Empfehlung: DENY
Gesetzter Wert: Nicht gesetzt.

X-Content-Type-Options

A

Der einzige definierte Wert "nosniff" untersagt dem Internet Explorer durch MIME-Sniffing einen anderen als den deklarierten Inhaltstyp zu bestimmen und anzuwenden.
Empfehlung: nosniff
Gesetzter Wert: Nicht gesetzt.

X-XSS-Protection

B

Die X-XSS-Protection kann Browsern untersagen eine Zielseite zu laden, sofern eine Cross-Site Scripting (XSS) Attacke erkannt wird.
Empfehlung: 1; mode=block
Gesetzter Wert: Nicht gesetzt.

Content-Security-Policy

B

Die HTTP Content-Security-Policy regelt welche Ressourcen in einer bestimmten Art und Weise im Browser geladen bzw. ausgeführt werden können.
Empfehlung: default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-src 'self'
Gesetzter Wert: Nicht gesetzt.

HTTP-Headers

<https://>

Seite 13 von 14

Übersicht

Verfügbarkeit

SSL/TLS

WTI

PortScan

HTTP-Headers

A++

A+

A

B

C

D

F

Referrer-Policy

Die Referrer-Policy stellt sicher, dass Referrer Informationen nur unter bestimmten Bedingungen gesendet werden dürfen.

Empfehlung: no-referrer-when-downgrade

Gesetzter Wert: Nicht gesetzt.

B

Strict-Transport-Security

Die HTTP Strict Transport Security (HSTS) ist ein Sicherheitsmechanismus für HTTPS-Verbindungen, der sowohl vor Aushebelung der Verbindungsverschlüsselung als auch vor Session Hijacking schützt.

Empfehlung: max-age=31536000; includeSubDomains

Gesetzter Wert: Nicht gesetzt.

F

Expect-CT

Der Expect-CT (Certificate Transparency) HTTP Header legt fest, wie die CT Policy angewandt werden soll.

Empfehlung: max-age=0

Gesetzter Wert: Nicht gesetzt.

B

Disclaimer

↳ <https://v>

Seite 14 von 14

Dieser Bericht wurde erstellt von

Enginsight GmbH
Hans-Knöll-Straße 6
07745 Jena

im folgenden 'Autor' genannt. Enginsight ist eine integrierte Lösung für alle wichtigen Belange des IT Monitorings. Überwachen Sie ganze IT- und Anwendungslandschaften von außen wie von innen hinsichtlich Verfügbarkeit, Stabilität sowie Sicherheit, ganzheitlich und autonom.

Der Autor übernimmt keinerlei Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität der bereitgestellten Informationen. Haftungsansprüche gegen den Autor, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen, sofern seitens des Autors kein nachweislich vorsätzliches oder grob fahrlässiges Verschulden vorliegt. Alle Angebote sind freibleibend und unverbindlich. Der Autor behält es sich ausdrücklich vor, Teile der Seiten oder das gesamte Angebot ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen.

Dieser Bericht enthält vertrauliche und/oder rechtlich geschützte Informationen. Wenn Sie nicht der richtige Adressat sind, oder dieser Bericht irrtümlich erhalten haben, informieren Sie bitte den Absender und löschen Sie diesen Bericht. Das unerlaubte Kopieren sowie die unbefugte Weitergabe dieses Berichtes und der darin enthaltenen Informationen sind nicht gestattet.