Security Analysis for:

https://google.com/

Report from Fri, 26 Jan 2024 17:04:36

50%
Connection Security

70%
Average Score

90%
Website Security

Report In-depth results

DOWNLOAD AS PDF

Content Security Policy Configuration

CSP

- CSP is not set

HttpOnly Flag cookie

HttpOnly

- HttpOnly flag is not set in the cookie : CONSENT

Connection

tls0

- Using TLS 1.0 could potentially allow attackers to decrypt and access sensitive data transmitted over supposedly secure connections due to susceptibility to cipher block chaining (CBC) attacks and issues related to its use of older, weaker cryptographic algorithms and hash functions. Relying on TLS 1.0 poses risks to data security and user privacy, potentially leading to data breaches and loss of trust. We highly recommend upgrading to TLS 1.3.

tls1

- Data transmitted using TLS 1.1 could potentially be compromised due to its reliance on older cryptographic algorithms and susceptibility to certain types of cryptographic attacks, such as padding oracle attacks. The protocol also lacks support for more robust and secure encryption methods available in later versions. Continued use of TLS 1.1 presents a considerable risk to the security and confidentiality of user data and communications. It is strongly recommended for website operators to upgrade to TLS 1.3, which offers enhanced security features, stronger encryption, and improved overall protection against modern cyber threats.

tls2

- Data transmitted using TLS 1.2 is considered reasonably secure and robust against various cyber threats. While TLS 1.2 remains a secure option, the evolution of cryptographic standards and the introduction of TLS 1.3, with even stronger security features and enhanced performance, make upgrading to the latest version a wise step for future-proofing website security.